Public Comments to
Full Draft of
Revised *Privacy of Consumer Financial and Health Information Act (*672)

TABLE OF CONTENTS

Regulator Comments 2

Michigan Department of Insurance and Financial Services (DIFS) 2
Virginia Bureau of Insurance (VBOI) 74

Industry Comments 133

American Council of Life Insurers (ACLI) 133
American Land Title Association (ALTA) 208
American Property Casualty Insurance Association (APCIA) 280
America's Health Insurance Plans (AHIP) 296
Blue Cross Blue Shield Association (BCBSA) 298
Coalition Against Insurance Fraud (CAIF) 304
Committee of Annuity Insurers (CAI) 363
Council of Insurance Agents and Brokers (CIAB) 430
Independent Insurance Agents and Brokers of America (IIABA) 434
Insured Retirement Institute (IRI) 441
InsurTech Coalition 445
International Underwriting Association (IUA) 450
Joint Trades 454
Lloyd's America, Inc. 457
National Association of Mutual Insurance Companies (NAMIC) 462
National Insurance Crime Bureau (NICB) 536
Verisk 538

Consumer Comments 543

Chris Dion 543
Chuck Bell 679
Harry Ting, on behalf of Adam Fox, Amy Bach, Anna Hyde, Anna Schwamlein Howard, Brenda Cude, Brendan Bridgeland, Brent Walker, Bonnie Burns, Carl Schmid, Deborah Darcy, Deborah Steinberg, Elizabeth Hagan, Eric Ellsworth, Erica Eversman, Kellan Baker, Kenneth Klein, Laura Colbert, Marguerite Herman, Michael DeLong, Milo Vieland, Peter Kochenburger, Richard Weber, Shamus Durac, Silvia Yee, Stephanie Hengst, and Wayne Turner 691

Regulator Comments:

Michigan:

PRIVACY OF CONSUMER ~~FINANCIAL AND HEALTH~~ INFORMATION ~~REGULATION~~ACT

Table of Contents

ARTICLE I. GENERAL PROVISIONS

Section 1. ~~Authority~~ Purpose
Section 2. ~~Purpose and~~ Scope and Compliance
Section 3. Rule of Construction
Section 4. Definitions

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS~~PRIVACY AND OPT OUT NOTICES FOR FINANCIAL INFORMATION~~

Section 5. Third-Party Service Provider Arrangements~~Initial Privacy Notice to Consumers Required~~

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7~~6~~. ~~Annual Privacy~~ Initial and Subsequent Delivery Notice of Information Practices to ~~Customers~~ Consumers Required
Section 8~~7~~. ~~Information to be Included in Privacy Notices~~Annual Notice of Information Practices to ~~Customers~~Consumers Required
Section 9~~8~~. ~~Form of Opt Out Notice to Consumers and Opt Out Methods~~Information to be Included in Notices of Information Practices
Section 10~~9~~. ~~Revised Privacy Notices~~Short Form Initial Notice of Information Practices
Section 11~~0~~. Form of Opt-In Notice to Consumers and Opt-In Methods~~Privacy Notices to Group Policyholders~~
Section 12~~1~~. ~~Delivery~~Form of Opt-Out Notice to Consumers and Opt-Out Methods
Section 13. Revised Notice of Information Practices
Section 14. Notice of Information Practices to Group Policyholders
Section 15. Delivery

ARTICLE ~~VIII~~V. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL ~~FINANCIAL~~ INFORMATION

Section 16~~2~~. General Rules for Use and Disclosure of Nonpublic Personal Information~~Limitation on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties~~

Section 17~~3~~. Limits on Redisclosure and Reuse of Nonpublic Personal ~~Financial~~ Information
Section 18~~4~~. Limits on Sharing Access ~~Account~~ Number or Access Code Information for Marketing Purposes
Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted Advertising
Section 20. Limits on Sale of Nonpublic Personal Information
Section 21. Limits on Disclosure of Sensitive Personal Information

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL ~~FINANCIAL~~ INFORMATION

Section 22~~15~~. Exception to Opt Out Requirements for Disclosure of Nonpublic Personal ~~Financial~~ Information for Service Providers and Joint Marketing
Section 23~~16~~. Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal ~~Financial~~ Information for Processing and Servicing Transactions
Section 24~~17~~. Other Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Information

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 25~~18~~. When Authorization Required for Disclosure of Nonpublic Personal Health Information
Section 26~~19~~. Authorizations
Section 27~~0~~. Authorization Request Delivery
Section 28~~1~~. Relationship to Federal Rules
Section 29~~2~~. Relationship to State Laws

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 30~~23~~. Protection of Fair Credit Reporting Act
Section 31~~24~~. Nondiscrimination
Section 32~~25~~. Violation
Section 33~~26~~. Severability
Section 34. Individual Remedies
Section 35~~27~~. Effective Date
~~Appendix A Sample Clauses~~
~~Appendix B Federal Model Privacy Form~~

APPENDICES

Appendix A Sample Clauses
Appendix B Federal Model Privacy Form
Model Law Forms

© 202617 National Association of Insurance Commissioners

ARTICLE I. GENERAL PROVISIONS

~~**Section 1. Authority**~~

~~This regulation is promulgated pursuant to the authority granted by Sections [insert applicable sections] of the Insurance Law.~~

Section ~~2~~1. Purpose ~~and Scope~~

~~A.~~ Purpose. This Act~~regulation~~ governs the treatment of nonpublic personal health information and nonpublic personal ~~financial~~ information about individuals by all licensees of the state insurance department. This Act~~regulation~~:

A. ~~A.~~(1) Requires a licensee to provide notice to individuals about its privacy policies and practices;

B. ~~B.~~(2) Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal ~~financial~~ information about individuals to affiliates and nonaffiliated third parties; and

C. ~~C.~~(3) Provides methods for individuals to prevent a licensee from disclosing that information.

Drafting Note: Whether this model is adopted as an Act or Regulation will depend upon individual state law. If a state adopts the model as an Act, reference to the model as an Act should be updated throughout the model.

Section 2. Scope and Compliance

A. ~~A.B.~~Scope. This Act~~regulation~~ applies to:

(1) Nonpublic personal ~~financial~~ information about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. This ~~regulation~~ Act does not apply to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes; and

(2) All nonpublic personal health information.

B. ~~B.C.~~Compliance. A licensee domiciled in this state that is in compliance with this Act ~~regulation~~ in a state that has not enacted laws or regulations that meet the requirements of Title V of the Gramm-Leach-Bliley Act (PL 102-106) may nonetheless be deemed to be in compliance with Title V of the Gramm-Leach-Bliley Act in the other state.

Drafting Note: Subsection B~~C~~ is intended to give licensees some guidance for complying with Title V of the Gramm-Leach-Bliley Act in those states that do not have laws or regulations that meet GLBA's privacy requirements.

© 2026~~17~~ National Association of Insurance Commissioners

Section 3. Rule of Construction

The examples in this Act~~regulation~~, the sample clauses in Appendix A, and the Federal Model Privacy Form in Appendix B of this Act~~regulation~~ are not exclusive. Compliance with an example, use of a sample clause, or the Federal Privacy Model Form, to the extent applicable, constitutes compliance with this Act~~regulation~~.

Licensees may rely on use of the Federal Privacy Form in Appendix B, consistent with the attached instructions, as a safe harbor of compliance with the Notice of Information Practices~~privacy notice~~ content requirements of this ~~regulation~~Act.

Use of the Federal Model Privacy Form is not required. Licensees may continue to use other types of privacy notices, including notices that contain the examples in this ~~regulation~~ Act and/or the sample clauses in Appendix A, provided that such notices accurately describe the Licensee's privacy practices and otherwise meet the notice content requirements of this ~~regulation~~Act. ~~However, while Licensees may continue to use privacy notices that contain the examples in this regulation and/or the sample clauses in Appendix A, Licensees may not rely on use of privacy notices with the sample clauses in Appendix A as a safe harbor of compliance with the notice content requirements of this regulation after July 1, 2019.~~

~~**Drafting Note:** Safe harbor of compliance with this regulation Act for use of sample clauses in Appendix A sunsets on July 1, 2019.~~

Section 4. Definitions

As used in this Act~~regulation~~, unless the context requires otherwise:

A. "Affiliate" means a company that controls, is controlled by or is under common control with another company.

B. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

C~~B~~. (1) "Clear and conspicuous" means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) Examples.

(a) Reasonably understandable. A licensee makes its notice reasonably understandable if it:

(i) Presents the information in the notice in clear, concise sentences, paragraphs and sections;

(ii) Uses short explanatory sentences or bullet lists whenever possible;

(iii) Uses definite, concrete, everyday words and active voice whenever possible;

(iv) Avoids multiple negatives;

(v) Avoids legal and highly technical business terminology whenever possible; and

(vi) Avoids explanations that are imprecise and readily subject to different interpretations.

(b) Designed to call attention. A licensee designs its notice to call attention to the nature and significance of the information in it if the licensee:

(i) Uses a plain-language heading to call attention to the notice;

(ii) Uses a typeface and type size that are easy to read;

(iii) Provides wide margins and ample line spacing;

(iv) Uses boldface or italics for key words; and

(v) In a form that combines the licensee's notice with other information, uses distinctive type size, style, and graphic devices, such as shading or sidebars.

(c) Notices on web sites. If a licensee provides a notice on a web page, the licensee designs its notice to call attention to the nature and significance of the information in it if the licensee uses text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks or sound) do not distract attention from the notice, and the licensee either:

(i) Places the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(ii) Places a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

D~~C~~. "Collect" means to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other ~~identifying~~ identifier particular assigned to the individual, irrespective of the source of the underlying information.

E~~D~~. "Commissioner" means the chief insurance regulatory official ~~commissioner~~ of the state.

Drafting Note: Use the title of the chief insurance regulatory official wherever the term "commissioner" appears. If the jurisdiction of certain health licensees, such as health maintenance organizations, lies with some state agency other than the insurance department, or if there is dual regulation, a state should add language referencing that agency to ensure the appropriate coordination of responsibilities.

F~~E~~. "Company" means a corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.

G~~F~~. (1) "Consumer" means an individual who seeks to obtain, obtains or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, and about whom the licensee has nonpublic personal information, or that individual's legal representative.

(2) Examples.

(a) An individual who provides nonpublic personal information to a licensee in connection with obtaining or seeking to obtain financial, investment or economic advisory services relating to an insurance product or service is a consumer regardless of whether the licensee establishes an ongoing advisory relationship.

(b) An applicant for insurance prior to the inception of insurance coverage is a licensee's consumer.

(c) An individual who is a consumer of another financial institution is not a licensee's consumer solely because the licensee is acting as agent for, or provides processing or other services to, that financial institution.

(d) An individual is a licensee's consumer if:

(i) (I) The individual is a beneficiary of a life insurance policy underwritten by the licensee;

(II) The individual is a claimant under an insurance policy issued by the licensee;

(III) The individual is an insured or an annuitant under an insurance policy or an annuity, respectively, issued by the licensee; or

(IV) The individual is a mortgagor of a mortgage covered under a mortgage insurance policy; and

(ii) The licensee discloses nonpublic personal ~~financial~~ information about the individual to a nonaffiliated third party other than as permitted under Sections ~~15, 16 and 17~~22, 23, and 24 of this ~~regulation~~Act.

(e) Provided that the licensee provides the initial, annual and revised notices under Sections ~~10~~ 7, 8, and 13 of this ~~regulation~~ Act to the plan sponsor, group or blanket insurance policyholder or group annuity contractholder, or workers' compensation policyholder, and further provided that the licensee does not disclose to a nonaffiliated third party nonpublic personal financial information about an individual described in Item (i), (ii) or (iii), other than as permitted under Sections ~~15, 16 and 17~~22, 23, or 24 of this ~~regulation~~Act, such an individual is not the consumer of the licensee solely because he or she is:

Commented [A1]: Recommendation to remove gendered language, e.g., "such an individual is not the consumer of the licensee soley because **the individual** is:" or "...because **they** are"

(i) A participant or a beneficiary of an employee benefit plan that the licensee administers or sponsors or for which the licensee acts as a trustee, insurer or fiduciary;

(ii) Covered under a group or blanket insurance policy or group annuity contract issued by the licensee; or

(iii) A claimant covered by a workers' compensation plan.

Drafting Note: In states where the workers' compensation self-insurance or workers' compensation state fund coverage is outside the commissioner's jurisdiction, regulators may wish to urge the applicable agency or agencies to promulgate a regulation similar to this ~~regulation~~ Act in order to ensure parity in treatment of workers' compensation plans and to ensure that all workers covered by such plans have privacy protections.

(f) (i) The individuals described in Subparagraph (e)(i) through (iii) of this paragraph are consumers of a licensee if the licensee does not meet all the conditions of Subparagraph (e).

(ii) In no event shall the individuals, solely by virtue of the status described in Subparagraph (e)(i) through (iii) above, be deemed to be ~~customers~~ consumers for purposes of this ~~regulation~~Act.

(g) An individual is not a licensee's consumer solely because he or she is a beneficiary of a trust for which the licensee is a trustee.

Commented [A2]: Same recommendation re: gendered language.

(h) An individual is not a licensee's consumer solely because he or she has designated the licensee as trustee for a trust.

Commented [A3]: Same recommendation re: gendered language.

H~~G~~. "Consumer reporting agency" has the same meaning as in Section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

I~~H~~. "Control" means:

(1) Ownership, control or power to vote twenty-five percent (25%) or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

(2) Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or

(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the commissioner determines.

~~I. "Customer" means a consumer who has a customer relationship with a licensee.~~

~~J. (1) "Customer relationship" means a continuing relationship between a consumer and a licensee under which the licensee provides one or more insurance products or services to the consumer that are to be used primarily for personal, family or household purposes.~~

~~(2) Examples.~~

~~(a) A consumer has a continuing relationship with a licensee if:~~

~~(i) The consumer is a current policyholder of an insurance product issued by or through the licensee; or~~

~~(ii) The consumer obtains financial, investment or economic advisory services relating to an insurance product or service from the licensee for a fee.~~

~~(b) A consumer does not have a continuing relationship with a licensee if:~~

~~(i) The consumer applies for insurance but does not purchase the insurance;~~

~~(ii) The licensee sells the consumer airline travel insurance in an isolated transaction;~~

~~(iii) The individual is no longer a current policyholder of an insurance product or no longer obtains insurance services with or through the licensee;~~

~~(iv) The consumer is a beneficiary or claimant under a policy and has submitted a claim under a policy choosing a settlement option involving an ongoing relationship with the licensee;~~

~~(v) The consumer is a beneficiary or a claimant under a policy and has submitted a claim under that policy choosing a lump sum settlement option;~~

~~(vi) The customer's policy is lapsed, expired or otherwise inactive or dormant under the licensee's business practices, and the licensee has not communicated with the customer about the relationship for a period of twelve (12) consecutive months, other than annual privacy notices, material required by law or regulation, communication at the direction of a state or federal authority, or promotional materials;~~

~~(vii) The individual is an insured or an annuitant under an insurance policy or annuity, respectively, but is not the policyholder or owner of the insurance policy or annuity; or~~

~~(viii) For the purposes of this regulation, the individual's last known address according to the licensee's records is deemed invalid. An address of record is deemed invalid if mail sent to that address by the licensee has been returned by the postal authorities as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.~~

J. "De-identified data" means information that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual.

K. (1) "Financial institution" means any institution the business of which is engaging in activities

that are financial in nature or incidental to such financial activities as described in Section 1843(k)(4)(B) ~~4(k)~~ of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial institution does not include:

(a) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 *et seq.*);

(b) The Federal Agricultural Mortgage Corporation or any entity charged and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*); or

(c) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as the institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

L. (1) "Financial product or service" means a product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 1843(k)(4)(B) ~~4(k)~~ of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.

~~M. "Health care" means:~~

~~(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, services, procedures, tests or counseling that:~~

~~(a) Relates to the physical, mental or behavioral condition of an individual; or~~

~~(b) Affects the structure or function of the human body or any part of the human body, including the banking of blood, sperm, organs or any other tissue; or~~

~~(2) Prescribing, dispensing or furnishing to an individual drugs or biologicals, or medical devices or health care equipment and supplies.~~

~~N. "Health care provider" means a physician or other health care practitioner licensed, accredited or certified to perform specified health services consistent with state law, or a health care facility.~~

M~~P~~. ~~(1)~~ "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.

~~(2) Insurance service includes a licensee's evaluation, brokerage or distribution of information that the licensee collects in connection with a request or an application from a consumer for a insurance product or service.~~

~~Q~~N. (1) "Licensee" means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Insurance Law of this state, [and health maintenance organizations holding a certificate of authority pursuant to Section [insert section] of this state's Public Health Law].

Drafting Note: Add bracketed language if HMOs are licensed under other than insurance statutes and cite appropriate state law.

(2) A licensee is not subject to the notice and opt out requirements for nonpublic personal ~~financial~~ information set forth in Articles I, II, III and IV of this ~~regulation~~ Act if the licensee is an employee, agent or other representative of another licensee ("the principal") and:

(a) The principal otherwise complies with, and provides the notices required by, the provisions of this ~~regulation~~Act; and

(b) The licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates in a manner permitted by this ~~regulation~~Act.

(3) (a) Subject to Subparagraph (b), "licensee" shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only in regard to the excess lines placements placed pursuant to Section [insert section] of this state's laws.

(b) An excess lines broker or excess lines insurer shall be deemed to be in compliance with the notice and opt out requirements for nonpublic personal ~~financial~~ information set forth in Articles I, II, III and IV of this ~~regulation~~ Act provided:

(i) The broker or insurer does not disclose nonpublic personal information of a consumer ~~or a customer~~ to nonaffiliated third parties for any purpose, including joint servicing or marketing under Section 22~~15~~ of this ~~regulation~~Act, except as permitted by Section 23~~16~~ or 24~~17~~ of this ~~regulation~~Act; and

(ii) The broker or insurer delivers a notice to the consumer at the time a ~~customer~~ consumer relationship is established on which the following is printed in 16-point type:

NOTICE OF INFORMATION PRACTICES~~PRIVACY NOTICE~~

"Neither the U.S. brokers that handled this insurance nor the insurers that have underwritten this insurance will disclose nonpublic personal information concerning the buyer to nonaffiliates of the brokers or insurers except as permitted by law."

Drafting Note: References to "excess lines broker" and "excess lines insurer" should be changed as necessary to correspond with the applicable terms used in each state.

~~R~~O. (1) "Nonaffiliated third party" means any person except:

(a) A licensee's affiliate; or

(b) A person employed jointly by a licensee and any company that is not the licensee's affiliate (but nonaffiliated third party includes the other company that jointly employs the person).

(2) Nonaffiliated third party includes any company that is an affiliate solely by virtue of the direct or indirect ownership or control of the company by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

P. "Nonpublic personal h~~H~~ealth information" means any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of an individual;

(2) The provision of health care to an individual; or

(3) Payment for the provision of health care to an individual.

Commented [A4]: Although age is not treated as nonpublic personal health information under this Act, note that under HIPAA Privacy Rule's Safe Harbor de-identification standard (45 C.F.R. §164.514(b)(2)(i)(C)), age is treated differently depending on the value. 0-89 can be reported in years, but 90 and above must be reported as '90 or older' as the more advanced the age, the rarer. Therefore, with ages above 90, there is increased ability to uniquely identify individuals based on that data element.

Q~~S~~. "Nonpublic personal information" means ~~nonpublic personal financial information and nonpublic personal health information.~~any personally identifiable information that is linked or reasonably linkable to an identified natural person. Nonpublic personal information does not include de-identified data or publicly available information.

~~T. (1) "Nonpublic personal financial information" means:~~

~~(a) Personally identifiable financial information; and~~

~~(b) Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.~~

~~(2) Nonpublic personal financial information does not include:~~

~~(a) Health information;~~

~~(b) Publicly available information, except as included on a list described in Subsection T(1)(b) of this section; or~~

~~(c) Any list, description or other grouping of consumers (and publicly available~~

~~information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.~~

~~(3) Examples of lists.~~

~~(a) Nonpublic personal financial information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information that is not publicly available, such as account numbers.~~

~~(b) Nonpublic personal financial information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived in whole or in part using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.~~

~~U. "Nonpublic personal health information" means health information:~~

~~(1) That identifies an individual who is the subject of the information; or~~

~~(2) With respect to which there is a reasonable basis to believe that the information could be used to identify an individual.~~

RV. (1) "Personally identifiable ~~financial~~ information" means any information:

(a) A consumer provides to a licensee to obtain an insurance product or service from the licensee;

(b) About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

(c) The licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.

(2) Examples.

(a) Information included. Personally identifiable ~~financial~~ information includes:

(i) Information a consumer provides to a licensee on an application to obtain an insurance product or service;

(ii) Account balance information and payment history;

(iii) The fact that an individual is or has been one of the licensee's consumers~~ustomers~~ or has obtained an insurance product or service from the licensee;

(iv) Any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer;

(v) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;

(vi) Any information the licensee collects through an Internet cookie (an information-collecting device from a web server); and

(vii) Information from a consumer report.

(b) Information not included. Personally identifiable ~~financial~~ information does not include:

~~(i) Health information;~~

(i~~i~~) A list of names and addresses of customers of an entity that is not a financial institution; and

(ii~~i~~) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.

S~~X~~. "Opt in" means an affirmative direction by a consumer that authorizes a licensee to disclose the consumer's information.

T~~X~~. "Opt out" means a direction by a consumer that the licensee may not disclose nonpublic personal information about the consumer to a nonaffiliated third party, except as permitted under Sections 22,23, or 24 ~~15, 16, 17, and 18~~.

U~~W~~. (1) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

(a) Federal, state or local government records;

(b) Widely distributed media; or

(c) Disclosures to the general public that are required to be made by federal, state or local law.

(2) Reasonable basis. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

(a) That the information is of the type that is available to the general public; and

(b) Whether an individual can direct that the information not be made available to the general public and, if so, that the licensee's consumer has not done so.

(3) Examples.

(a) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(b) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(c) Reasonable basis.

(i) A licensee has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(ii) A licensee has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the licensee has located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

V. "Reasonable opportunity" means any of the following:

(1) ~~(a)~~ The licensee mails the notices required to the consumer and allows the consumer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within sixty (60) days from the date the licensee mailed the notices;

(2) ~~(b)~~ Where a consumer agrees to receive the notices required by this Act electronically in accordance with UETA [insert state electronic transactions act statute], the licensee allows the consumer to opt out by any reasonable means at any time; or

(3) ~~(c)~~ For an isolated transaction, such as providing the consumer with an insurance quote, the licensee provides the notices required by this Act at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction.

X. "Sale" or "selling" means the exchange of nonpublic personal information for monetary or other valuable consideration. A licensee does not sell nonpublic personal information when:

(1) The disclosure is to a third party for the purpose of or in support of providing a product or service requested by the consumer.

~~(1)~~(2) A licensee provides information to or receives anything of value from an insurance

support organization, statistical agent, or reinsurer;

~~(2)~~(3) A licensee provides nonpublic personal information to an affiliate or to a financial institution with which the licensee performs joint marketing;

~~(3)~~(4) The business transfers to a third party the nonpublic personal information as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction in which the party assumes control of all or part of the licensee's assets; or

(5) A consumer uses or directs the business to (i) disclose nonpublic personal information; or (ii) interact with one or more third parties including but not limited to referrals to other licensees.

Y. "Sensitive Personal Information" means personally identifiable "nonpublic personal information" about a consumer that includes:

(1) Racial or ethnic origin, religious beliefs, sexual orientation, or citizenship or citizenship status; or

(2) Genetic information or biometric data that may be processed for the purpose of uniquely identifying an individual.

Z. (1) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests.

(2) "Targeted advertising" does not include:

(a) Online advertisements based on activities within a Licensee's own websites or online applications;

(b) Online advertisements based on the context of a consumer's current search query, visit to a website, or online application;

(c) Online advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(d) Processing Nonpublic Personal Information solely for measuring or reporting advertising performance, reach, or frequency.

AA. "Third party service provider" or "third party" means a person or entity not otherwise defined as a licensee or affiliate of a licensee that:

(1) Provides services to the licensee; and

(2) Maintains, processes or otherwise is permitted access to nonpublic personal information through its provisions of services to the licensee.

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS
~~**PRIVACY AND OPT_OUT NOTICES FOR FINANCIAL INFORMATION**~~

Section 5. Third-Party Service Provider Arrangements

A. Contract Requirements.

A licensee that discloses a consumer's nonpublic personal information to a third-party service provider shall enter into a written contract with the third-party service provider that:

(1) Prohibits the third-party service provider from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless processing is necessary to comply with the law or a valid and binding order of a governmental body, in which case the third-party service provider must notify the licensee within 48 hours unless prohibited by law;

(2) Requires the third-party service provider to delete, destroy, de-identify or return all nonpublic personal information to the licensee when requested by the licensee; or to delete nonpublic personal information after it is no longer necessary to fulfill a legal requirement or to meet the record retention requirements of the licensee or third-party service provider, and to notify the licensee of the action taken;

(3) Requires the third-party service provider to notify the licensee if it can no longer comply with its obligations under this contract and provides the licensee with a right to terminate the contract;

(4) Requires that any contract between a third-party service provider and a subcontractor with access to a consumer's nonpublic personal information must contain provisions no less protective of nonpublic personal information than those contained in the third-party service provider's agreement with the licensee;

(5) Requires the third-party service provider to provide assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act;

(6) Requires the third-party service provider to implement and maintain administrative, technical, and physical data security practices to protect the nonpublic personal information from unauthorized access, destruction, use, modification, or disclosure;

(7) Requires the third-party service provider to notify the licensee of a failure to meet the obligations of Subsections (1) to (6) above within 48 hours of discovery by the third-party service provider.

B. A licensee that discloses a consumer's nonpublic personal information to a third-party service provider remains fully responsible for compliance with this Act and the handling of nonpublic personal information.

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

A. A consumer may file the following requests with a licensee, which shall be processed in accordance with the following standards:

(1) Within 45 days of receiving an authenticated request from a consumer for their nonpublic personal information, a licensee shall disclose:

(a) All nonpublic personal information about the consumer that is maintained by the licensee or any contracted third-party service provider; and

(b) A list of all third-party service providers to whom the licensee disclosed the consumer's nonpublic personal information.

(2) A licensee shall not be required to disclose the following:

(a) A consumer's Social Security Number, driver's license number or other government-issued identification number, financial account number(s), any health insurance or medical identification number, any account password(s), security questions and answers, unique biometric data or other information that could create a high risk of identity theft. The licensee may instead disclose the types of nonpublic personal information maintained by listing each type of nonpublic personal information it has about the consumer;

(b) Duplicative nonpublic personal information, if it is described in a manner reasonably understandable by the consumer and the consumer is offered an opportunity to review the nonpublic personal information for inconsistencies; or

(c) Information that is outside the scope of the request, if the consumer has requested only specified items or categories of information.

B. Correction of nonpublic personal information.

(1) A consumer may make an authenticated request for the correction of their nonpublic personal information by filing a request with the licensee that:

(a) Identifies the specific nonpublic personal information the consumer wishes to correct; and

(b) Provides an explanation of why the nonpublic personal information is incorrect.

(2) Within 45 days of receipt of the request under this subsection, a licensee shall take one of the following actions and notify the consumer:

(a) Correct the nonpublic personal information in dispute as requested by the consumer;

(b) Delete the nonpublic personal information in dispute; or

(~~b~~c) Deny the request and provide:

(i) The basis for refusal to correct the nonpublic personal information as requested;

(ii) Information about how the consumer may appeal the denial; and

(iii) An explanation of how the appeal will be reviewed and how the consumer will be notified of the decision on appeal.

Commented [A5]: 1) Should the Act specify minimum standards for the appeal process (timelines, required content, documentation expectations), rather than leaving it entirely to licensees?

2) Should the Act require licensees to maintain records of appeals for market conduct examinations?
3) Should consumers receive written notice that an appeal decision is final or whether there is a further escalation path (e.g., DOI complaint process)?

(3) A licensee may deny a request for correction if:

(a) The nonpublic personal information is accurate and complete and if the licensee provides a process for appeal of the decision; or

(b) The nonpublic personal information that is the subject of the request was not created by the licensee, unless there is a reasonable basis to believe that the originator of the nonpublic personal information is no longer available to act on the requested correction, and the consumer has independently demonstrated the information is incorrect.

C. Deletion of nonpublic personal information.

(1) Within 45 days of an authenticated request from a consumer, a licensee shall delete the nonpublic personal information about the consumer that is maintained by the licensee or direct a third-party service provider to delete the nonpublic personal information on the licensee's behalf.

(2) The licensee is not required to delete nonpublic personal information if:

(a) The licensee is required by law or regulation to retain the nonpublic personal information;

(b) The nonpublic personal information may be necessary to perform the contract or service requested by or benefiting the consumer;

(c) The information is necessary to comply with a legal obligation; or

(d) The information is maintained in reasonable anticipation of a claim or civil or criminal proceeding.

(3) A licensee may delay fulfilling a consumer's request, up to 45 days, to delete nonpublic personal information stored on an archived or backup system. A licensee must notify the consumer of such delay.

D. Request and Response Procedures

(1) Except as provided in Subsection D(1)(b), a licensee shall respond to requests submitted under this section within 45 days in the following manner:

(a) A licensee may use its secure communications portal to authenticate requests from consumers holding current accounts with the licensee, unless the licensee has reason to believe the request has been submitted through an account that has been compromised. Otherwise, the licensee may use methods that are commercially reasonable, but not unduly burdensome, to authenticate the identity of the person making the request and to verify that this person is either:

(i) The consumer;

(ii) A person acting with the consumer's written authorization, including but not limited to a valid power of attorney;

(iii) The parent or legal guardian of a consumer who is a minor, except where the information relates to health insurance claims in circumstances where the child has a legal right to obtain the services in question without the parent's or guardian's consent;

(iv) The legal guardian or other person authorized by law to act on behalf of an incapacitated consumer; or

(v) The personal representative or other person authorized by law to act on behalf of a deceased consumer.

(b) A licensee is required to notify the consumer if either of the following prevents the licensee from complying with the request:

Commented [A6]: Should there be guidance on how licensees handle fraudulent requests?

(i) The specific nonpublic personal information at issue is not locatable or retrievable by the licensee; or

Drafting Note: Examiners should review licensees' notifications to consumers regarding nonpublic personal information that is not locatable or retrievable by the licensee and its justifications for irretrievability during Market Conduct and/or IT Exams.

(ii) The licensee is unable to verify the request after requesting that the consumer provide additional information necessary to authenticate the identity of the consumer and authenticate the consumer's request.

(c) If a licensee declines the consumer's request, the licensee shall inform the consumer of the basis for declining the request and provide instructions for how to request review of the decision.

(2) There shall be no cap on the number of requests to correct or delete nonpublic personal information.

(3) If a consumer disagrees with a licensee's refusal to correct or delete nonpublic personal information per the consumer's request, the consumer shall be permitted to file with the licensee:

(a) A concise statement setting forth why the consumer disagrees with the licensee's refusal and what the consumer thinks is the correct, relevant or fair information; and

(b) The licensee shall maintain the statement with the disputed nonpublic personal information and allow anyone reviewing the disputed nonpublic personal information to be made aware of the dispute and have access to the consumer's statement.

ARTICLE IV.——— NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7~~85~~. Initial and Subsequent Delivery Notice of Information Practices~~Privacy Notice~~ to Consumers Required

Commented [A7]: For Sections 7-9, how do DOIs get the notices? Should we add that copies must be provided for review by the department upon request (or add a drafting note to address this)?

A. Initial Delivery of Notice~~notice requirement~~. A licensee shall provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to~~:~~ all consumers no later than when the licensee obtains access to the consumer's nonpublic personal information, except that a licensee may provide the initial notice within a reasonable time after access to the consumer's nonpublic personal information if:

(1) Obtaining access to the consumer's nonpublic personal information is not at the consumer's election and the licensee follows the Notice of Information Practices previously sent to the consumer; or

(2) Providing notice when the licensee obtains access to the consumer's nonpublic personal i~~n~~formation would substantially delay the consumer's transaction and the consumer agrees to receive the notice at a later time.

B. Subsequent Delivery of Notice

When a consumer with an existing relationship with a licensee obtains a new insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, the licensee satisfies the initial notice requirements of Subsection A of this section as follows:

(1) The licensee may provide a revised notice, under Section 13~~.~~, that covers the consumer's new insurance product or service; or

(2) If the initial, revised or annual notice that the licensee most recently provided to that consumer was accurate with respect to the new insurance product or service, the licensee does not need to provide a new notice of information practices under Subsection A of this section.

C. For purposes of this section:

(1) "Not at consumer's election" includes the scenario where a licensee acquires or is assigned a consumer's policy from another financial institution or residual market mechanism and the consumer does not have a choice about the licensee's acquisition or assignment.

(2) "Substantially delay the consumer's transaction" includes the scenario where the licensee and the individual agree over the telephone or electronically to enter into a consumer relationship involving prompt delivery of the insurance product or service but does not include the scenario where the relationship is initiated in person at the licensee's office or through other means by which the consumer may view the notice, such as on a website.

~~(1) Customer. An individual who becomes the licensee's customer, not later than when the licensee establishes a customer relationship, except as provided in Subsection E of this section; and~~

(2) Consumer. A consumer, before the licensee discloses any nonpublic personal financial information about the consumer to any nonaffiliated third party, if the licensee makes a disclosure other than as authorized by Sections 16 and 17.

B. When initial notice to a consumer is not required. A licensee is not required to provide an initial notice to a consumer under Subsection A(2) of this section if:

(1) The licensee does not disclose any nonpublic personal financial information about the consumer to any nonaffiliated third party, other than as authorized by Sections 16 and 17, and the licensee does not have a customer relationship with the consumer; or

(2) A notice has been provided by an affiliated licensee, as long as the notice clearly identifies all licensees to whom the notice applies and is accurate with respect to the licensee and the other institutions.

C. When the licensee establishes a customer relationship.

(1) General rule. A licensee establishes a customer relationship at the time the licensee and the consumer enter into a continuing relationship.

(2) Examples of establishing customer relationship. A licensee establishes a customer relationship when the consumer:

(a) Becomes a policyholder of a licensee that is an insurer when the insurer delivers an insurance policy or contract to the consumer, or in the case of a licensee that is an insurance producer or insurance broker, obtains insurance through that licensee; or

(b) Agrees to obtain financial, economic or investment advisory services relating to insurance products or services for a fee from the licensee.

D. Existing customers. When an existing customer obtains a new insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, the licensee satisfies the initial notice requirements of Subsection A of this section as follows:

(1) The licensee may provide a revised policy notice, under Section 9, that covers the customer's new insurance product or service; or

(2) If the initial, revised or annual notice that the licensee most recently provided to that customer was accurate with respect to the new insurance product or service, the licensee does not need to provide a new privacy notice under Subsection A of this section.

E. Exceptions to allow subsequent delivery of notice.

(1) A licensee may provide the initial notice required by Subsection A(1) of this section within a reasonable time after the licensee establishes a customer relationship if:

(a) Establishing the customer relationship is not at the customer's election; or
(b) Providing notice not later than when the licensee establishes a customer

~~relationship would substantially delay the customer's transaction and the customer agrees to receive the notice at a later time.~~

~~(2) Examples of exceptions.~~

~~(a) Not at customer's election. Establishing a customer relationship is not at the customer's election if a licensee acquires or is assigned a customer's policy from another financial institution or residual market mechanism and the customer does not have a choice about the licensee's acquisition or assignment.~~

~~(b) Substantial delay of customer's transaction. Providing notice not later than when a licensee establishes a customer relationship would substantially delay the customer's transaction when the licensee and the individual agree over the telephone to enter into a customer relationship involving prompt delivery of the insurance product or service.~~

~~(c) No substantial delay of customer's transaction. Providing notice not later than when a licensee establishes a customer relationship would not substantially delay the customer's transaction when the relationship is initiated in person at the licensee's office or through other means by which the customer may view the notice, such as on a web site.~~

~~F. Delivery. When a licensee is required to deliver an initial privacy notice by this section, the licensee shall deliver it according to Section 11. If the licensee uses a short-form initial notice for non-customers according to Section 7D, the licensee may deliver its privacy notice according to Section 7D(3).~~

Section ~~6~~8. Annual ~~Privacy~~ Notice of Information Practices to ~~Customers~~ Consumers Required

~~A. (1)~~ General rule. A licensee shall provide a clear and conspicuous notice to consumers~~ustomers~~ that accurately reflects its privacy policies and practices ~~not less than annually during the continuation of the customer relationship. Annually means~~ at least once in any period of twelve (12) consecutive months. ~~during which that relationship exists.~~ A licensee may define the twelve-consecutive-month period, but the licensee shall apply it to the consumer~~ustomer~~ on a consistent basis.

A.~~(2)~~ Example. A licensee provides a notice annually if it defines the twelve-consecutive-month period as a calendar year and provides the annual notice to the consumer~~ustomer~~ once in each calendar year following the calendar year in which the licensee provided the initial notice. For example, if a consumer~~ustomer~~ opens an account on any day of year 1, the licensee shall provide an annual notice to that consumer~~ustomer~~ by December 31 of year 2.

(1) Exceptions. ~~to general rule.~~

(1) A licensee that provides nonpublic personal information to nonaffiliated third parties only in accordance with Sections ~~15, 16, or 17~~22, 23, or 24 and has not changed its policies and practices with regard to disclosing ~~n~~Nonpublic P~~p~~ersonal ~~i~~information from the policies and practices that were disclosed in the most recent disclosure sent to consumers in accordance with this section or Section 7~~5~~ shall not be required to provide an annual disclosure under this section until such time as the licensee fails to comply with any

criteria described in this paragraph.

(2) A licensee is not required to provide notice if the licensee no longer has access to the consumer's nonpublic personal information.

(2) For the purposes of this Act, a licensee no longer has an obligation to continue to notify a consumer if the licensee's records do not contain a valid address. An address is deemed invalid if electronic or regular mail sent to that address by the licensee has been returned as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.

~~C. (1) Termination of customer relationship. A licensee is not required to provide an annual notice to a former customer. A former customer is an individual with whom a licensee no longer has a continuing relationship.~~

~~(2) Examples.~~

~~(a) A licensee no longer has a continuing relationship with an individual if the individual no longer is a current policyholder of an insurance product or no longer obtains insurance services with or through the licensee.~~

~~(b) A licensee no longer has a continuing relationship with an individual if the individual's policy is lapsed, expired or otherwise inactive or dormant under the licensee's business practices, and the licensee has not communicated with the customer about the relationship for a period of twelve (12) consecutive months, other than to provide annual privacy notices, material required by law or regulation, or promotional materials.~~

~~(c) For the purposes of this regulation, a licensee no longer has a continuing relationship with an individual if the individual's last known address according to the licensee's records is deemed invalid. An address of record is deemed invalid if mail sent to that address by the licensee has been returned by the postal authorities as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.~~

~~(d) A licensee no longer has a continuing relationship with a customer in the case of providing real estate settlement services, at the time the customer completes execution of all documents related to the real estate closing, payment for those services has been received, or the licensee has completed all of its responsibilities with respect to the settlement, including filing documents on the public record, whichever is later.~~

~~D. Delivery. When a licensee is required by this section to deliver an annual privacy notice, the licensee shall deliver it according to Section 11.~~

Section 9~~7~~. Information to be Included in ~~Privacy~~ Notices of Information Practices

A. General rule. The initial, annual and revised ~~privacy notices~~ Notice of Information Practices that a licensee provides under Sections ~~5~~7, ~~, 68~~8, and ~~3~~13~~9~~ shall include each of the following items of information, in addition to any other information the licensee wishes to provide, that applies to the licensee and to the consumers to whom the licensee sends its ~~privacy notice:~~ Notice of Information Practices:

~~(1) The categories of nonpublic personal financial information that the licensee collects;~~

~~(2) The categories of nonpublic personal financial information that the licensee discloses;~~

~~(3) The categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information, other than those parties to whom the licensee discloses information under Sections 16 and 17;~~

~~(4) The categories of nonpublic personal financial information about the licensee's former customers that the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information about the licensee's former customers, other than those parties to whom the licensee discloses information under Sections 16 and 17;~~

~~(5) If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under Section 15 (and no other exception in Sections 16 and 17 applies to that disclosure), a separate description of the categories of information the licensee discloses and the categories of third parties with whom the licensee has contracted;~~

(1) The categories of nonpublic personal information that the licensee collects, including, but not limited to, whether information is collected from the consumer, through the consumer's transactions with affiliates or nonaffiliated third parties, or consumer reporting agencies;

(2) The categories of nonpublic personal information that the licensee discloses, including at least one example in each category. Categories may include, but are not limited to, application information, transaction information, or consumer reports;

(3) The categories of affiliates and nonaffiliated third parties, and the types of business in which they engage, to whom the licensee discloses nonpublic personal information, other than those parties to whom the licensee discloses information under Sections ~~20 and 21~~22, 23, and 24. The types of businesses may be described in general terms only if the licensee uses illustrative examples of each significant line of business;

(~~4~~6) An explanation of the consumer's right under Section 12~~A~~ to opt out of the disclosure of nonpublic personal ~~financial~~ information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;

(5) An explanation of the consumer's rights with regard to the sale of nonpublic personal information and disclosure of sensitive personal information pursuant to Sections 20 and 21;

(6) A description of the consumer's options to request access, correction, or deletion of

nonpublic personal information about the consumer as established under this Act and the instructions for exercising such options;

(7) Any disclosures that the licensee makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);

(8) The licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; by~~and~~

(a) Describing in general terms who is authorized to have access to the information; and

(b) Stating whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance with the licensee's policy. The licensee is not required to describe technical information about the safeguards it uses; and

~~(9)~~(c) Any disclosure that the licensee makes ~~under Subsection B of this section.~~ as authorized under Section 22, 23, or 24~~21~~, except that the licensee is not required to list those exceptions in the initial or annual Notice of Information Practices required by Sections ~~9~~7 and ~~10~~8. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.

~~B. Description of parties subject to exceptions. If a licensee discloses nonpublic personal financial information as authorized under Sections 16 and 17, the licensee is not required to list those exceptions in the initial or annual privacy notices required by Sections 5 and 6. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.~~

B. The licensee's notice may include:

(1) Categories of nonpublic personal information that the licensee reserves the right to disclose in the future, but does not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the right in the future to disclose, but to whom the licensee does not currently disclose, nonpublic personal information.

C. Exceptions:~~Examples.~~

If a licensee does not disclose, and does not reserve the right to disclose, nonpublic personal information about consumers to affiliates or nonaffiliated third parties except as authorized under Sections ~~20 and 21~~22, 23, or 24, the licensee shall state that in its notice, in addition to the information it shall provide under Subsections A(1) and A(8) and Subsection B of this section.

D. Sample Clauses and Federal Model Privacy Form.

(1) Licensees are not required to use any prescribed clauses or model form.

(2) The commissioner may determine that a Licensee's use of any of the following constitutes compliance with this Act:

(a) Sample clauses illustrating some of the notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner;

(b) Model forms illustrating notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner; or

(c) The Federal Model Privacy Forms are included in Appendix A and Appendix B, of this Act.

~~(1) Categories of nonpublic personal financial information that the licensee collects. A licensee satisfies the requirement to categorize the nonpublic personal financial information it collects if the licensee categorizes it according to the source of the information, as applicable:~~

~~(a) Information from the consumer;~~

~~(b) Information about the consumer's transactions with the licensee or its affiliates;~~

~~(c) Information about the consumer's transactions with nonaffiliated third parties; and~~

~~(d) Information from a consumer reporting agency.~~

~~(2) Categories of nonpublic personal financial information a licensee discloses.~~

~~(a) A licensee satisfies the requirement to categorize nonpublic personal financial information it discloses if the licensee categorizes the information according to source, as described in Paragraph (1), as applicable, and provides a few examples to illustrate the types of information in each category. These might include:~~

~~(i) Information from the consumer, including application information, such as assets and income and identifying information, such as name, address and social security number;~~

~~(ii) Transaction information, such as information about balances, payment history and parties to the transaction; and~~

~~(iii) Information from consumer reports, such as a consumer's creditworthiness and credit history.~~

~~(b) A licensee does not adequately categorize the information that it discloses if the~~

licensee uses only general terms, such as transaction information about the consumer.

(c) If a licensee reserves the right to disclose all of the nonpublic personal financial information about consumers that it collects, the licensee may simply state that fact without describing the categories or examples of nonpublic personal information that the licensee discloses.

(3) Categories of affiliates and nonaffiliated third parties to whom the licensee discloses.

(a) A licensee satisfies the requirement to categorize the affiliates and nonaffiliated third parties to which the licensee discloses nonpublic personal financial information about consumers if the licensee identifies the types of businesses in which they engage.

(b) Types of businesses may be described by general terms only if the licensee uses a few illustrative examples of significant lines of business. For example, a licensee may use the term financial products or services if it includes appropriate examples of significant lines of businesses, such as life insurer, automobile insurer, consumer banking or securities brokerage.

(c) A licensee also may categorize the affiliates and nonaffiliated third parties to which it discloses nonpublic personal financial information about consumers using more detailed categories.

(4) Disclosures under exception for service providers and joint marketers. If a licensee discloses nonpublic personal financial information under the exception in Section 15 to a nonaffiliated third party to market products or services that it offers alone or jointly with another financial institution, the licensee satisfies the disclosure requirement of Subsection A(5) of this section if it:

(a) Lists the categories of nonpublic personal financial information it discloses, using the same categories and examples the licensee used to meet the requirements of Subsection A(2) of this section, as applicable; and

(b) States whether the third party is:

(i) A service provider that performs marketing services on the licensee's behalf or on behalf of the licensee and another financial institution; or

(ii) A financial institution with whom the licensee has a joint marketing agreement.

(5) Simplified notices. If a licensee does not disclose, and does not wish to reserve the right to disclose, nonpublic personal financial information about customers or former customers to affiliates or nonaffiliated third parties except as authorized under Sections 16 and 17, the licensee may simply state that fact, in addition to the information it shall provide under Subsections A(1), A(8), A(9) and Subsection B of this section.

(6) Confidentiality and security. A licensee describes its policies and practices with respect to

protecting the confidentiality and security of nonpublic personal financial information if it does both of the following:

(a) Describes in general terms who is authorized to have access to the information; and

(b) States whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance with the licensee's policy. The licensee is not required to describe technical information about the safeguards it uses.

D. Short-form initial notice with opt-out notice for non-customers.

(1) A licensee may satisfy the initial notice requirements in Sections 5A(2) and 8C for a consumer who is not a customer by providing a short-form initial notice at the same time as the licensee delivers an opt-out notice as required in Section 8.

(2) A short-form initial notice shall:

(a) Be clear and conspicuous;

(b) State that the licensee's privacy notice is available upon request; and

(c) Explain a reasonable means by which the consumer may obtain that notice.

(3) The licensee shall deliver its short-form initial notice according to Section 10. The licensee is not required to deliver its privacy notice with its short-form initial notice. The licensee instead may simply provide the consumer a reasonable means to obtain its privacy notice. If a consumer who receives the licensee's short-form notice requests the licensee's privacy notice, the licensee shall deliver its privacy notice according to Section 11.

(4) Examples of obtaining privacy notice. The licensee provides a reasonable means by which a consumer may obtain a copy of its privacy notice if the licensee:

(a) Provides a toll-free telephone number that the consumer may call to request the notice; or

(b) For a consumer who conducts business in person at the licensee's office, maintains copies of the notice on hand that the licensee provides to the consumer immediately upon request.

E. Future disclosures. The licensee's notice may include:

(1) Categories of nonpublic personal financial information that the licensee reserves the right to disclose in the future, but does not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the right in the future to disclose, but to whom the licensee does not currently disclose, nonpublic personal financial information.

~~F. Sample Clauses and Federal Model Privacy Form. Sample clauses illustrating some of the notice content required by this section and the Federal Model Privacy Form are included in Appendix A and Appendix B, respectively, of this regulation.~~

Section 10. Short Form Initial Notice of Information Practices

A. A licensee may satisfy the initial notice requirements in Sections 7A and 13A by providing a Short Form Initial Notice of Information Practices at the same time the licensee delivers an opt-out notice as required in Section 12 if:

(1) The licensee provides the consumer a reasonable means to obtain its Notice of Information Practices; and

(2) The licensee provides the Notice of Information Practices upon request.

B. A Short Form Initial Notice of Information Practices shall meet all of the following requirements.

(1) Be clear and conspicuous;

(2) State that the licensee's Notice of Information Practices is available upon request;

(3) Explain the reasonable means to obtain the licensee's Notice of Information Practices;

(4) Contain contact information for the commissioner; and

(5) Describe how the consumer can request access to or correction of their nonpublic personal information.

C. For purposes of this section "reasonable means to obtain the licensee's Notice of Information Practices" includes:

(1) Providing a toll-free telephone number that the consumer may call to request the notice;

(2) Providing a website or other electronic medium that is easily accessible by the consumer; or

(3) Maintaining copies of the notice at the licensee's place of business to be provided upon request.

Section 11~~8~~. Form of Opt-In~~Out~~ Notice to Consumers and Opt-In~~Out~~ Methods

A. ~~(1) Form of opt-out notice.~~ If a licensee is required to provide an opt-in ~~-out~~ notice under Sections ~~12A22~~20 or ~~23~~21, it shall provide a clear and conspicuous notice to each of its consumers that accurately explains the ~~right~~ information proposed to be disclosed, the use of that information, and the consumer's option to opt in to that use.~~out under that section.~~ The notice shall state:

(1)~~a~~) ~~That T~~the licensee discloses or reserves the right to disclose nonpublic personal ~~financial~~ information about its consumer to a nonaffiliated third party;

(2~~b~~) ~~That T~~the consumer has the ~~right~~ option to opt in to ~~out of~~ that disclosure; and

(3) A reasonable means by which the consumer may exercise the option to opt inout right.

B. The licensee shall not disclose that information to a nonaffiliated third party unless the consumer has affirmatively opted in to the use.

C. The opt-in must be an affirmative act by the consumer. The licensee cannot deem a failure to respond as an opt-in or use pre-checked boxes.

D. The opt-in should be obtained separately from any other communication or consent.

E. The opt-in may be revoked at any time by the consumer.

~~(2) Examples.~~

~~(a) Adequate opt out notice. A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal financial information to a nonaffiliated third party if the licensee:~~

~~(i) Identifies all of the categories of nonpublic personal financial information that it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to which the licensee discloses the information, as described in Section 7A(2) and (3), and states that the consumer can opt out of the disclosure of that information; and~~

~~(ii) Identifies the insurance products or services that the consumer obtains from the licensee, either singly or jointly, to which the opt out direction would apply.~~

~~(b) Reasonable opt out means. A licensee provides a reasonable means to exercise an opt out right if it:~~

~~(i) Designates check-off boxes in a prominent position on the relevant forms with the opt out notice;~~

~~(ii) Includes a reply form together with the opt out notice;~~

~~(iii) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the licensee's web site, if the consumer agrees to the electronic delivery of information; or~~

~~(iv) Provides a toll-free telephone number that consumers may call to opt out.~~

~~(c) Unreasonable opt out means. A licensee does not provide a reasonable means of opting out if:~~

~~(i) The only means of opting out is for the consumer to write his or her own letter to exercise that opt out right; or~~

~~(ii) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the licensee provided with~~

the initial notice but did not include with the subsequent notice.

(d) Specific opt out means. A licensee may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

B. Same form as initial notice permitted. A licensee may provide the opt out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 5.

C. Initial notice required when opt out notice delivered subsequent to initial notice. If a licensee provides the opt out notice later than required for the initial notice in accordance with Section 5, the licensee shall also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.

D. Joint relationships.

(1) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt out notice. The licensee's opt out notice shall explain how the licensee will treat an opt out direction by a joint consumer (as explained in Paragraph (5) of this subsection).

(2) Any of the joint consumers may exercise the right to opt out. The licensee may either:

(a) Treat an opt out direction by a joint consumer as applying to all of the associated joint consumers; or

(b) Permit each joint consumer to opt out separately.

(3) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all of the joint consumers.

(4) A licensee may not require all joint consumers to opt out before it implements any opt out direction.

(5) Example. If John and Mary are both named policyholders on a homeowner's insurance policy issued by a licensee and the licensee sends policy statements to John's address, the licensee may do any of the following, but it shall explain in its opt out notice which opt out policy the licensee will follow:

(a) Send a single opt out notice to John's address, but the licensee shall accept an opt out direction from either John or Mary.

(b) Treat an opt out direction by either John or Mary as applying to the entire policy. If the licensee does so and John opts out, the licensee may not require Mary to opt out as well before implementing John's opt out direction.

(c) Permit John and Mary to make different opt out directions. If the licensee does so:

(i) It shall permit John and Mary to opt out for each other;

~~(ii) If both opt out, the licensee shall permit both of them to notify it in a single response (such as on a form or through a telephone call); and~~

~~(iii) If John opts out and Mary does not, the licensee may only disclose nonpublic personal financial information about Mary, but not about John and not about John and Mary jointly.~~

~~E. Time to comply with opt out. A licensee shall comply with a consumer's opt out direction as soon as reasonably practicable after the licensee receives it.~~

~~F. Continuing right to opt out. A consumer may exercise the right to opt out at any time.~~

~~G. Duration of consumer's opt out direction.~~

~~(1) A consumer's direction to opt out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.~~

~~(2) When a customer relationship terminates, the customer's opt out direction continues to apply to the nonpublic personal financial information that the licensee collected during or related to that relationship. If the individual subsequently establishes a new customer relationship with the licensee, the opt out direction that applied to the former relationship does not apply to the new relationship.~~

~~H. Delivery. When a licensee is required to deliver an opt out notice by this section, the licensee shall deliver it according to Section 11.~~

Section 12. Form of Opt-Out Notice to Consumers and Opt-Out Methods

A. (1) If a licensee is required to provide an opt-out notice, it shall provide a clear and conspicuous notice to each consumer that accurately explains the right to opt out under that section. To the extent applicable, the notice shall state:

(a) That the licensee discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;

(b) That the consumer has the right to opt out of that disclosure; and

(c) A reasonable means by which the consumer may exercise the opt-out right.

(2) Requirements

(a) A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if the licensee:

(i) Identifies all of the categories of nonpublic personal information it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to whom the licensee discloses the information, as described in Section ~~11~~9A(2) and (3), and states the consumer can opt out of the disclosure of that information; and

(ii) Identifies the insurance products or services the consumer obtains from the licensee, either singly or jointly, to which the opt-out would apply.

(b) A licensee provides a reasonable means to exercise an opt-out right if it:

(i) Designates check-off boxes in a prominent position on the relevant forms with the opt-out notice;

(ii) Includes a reply form together with the opt–out notice;

(iii) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the licensee's website, if the consumer agrees to the electronic delivery of information; or

(iv) Provides a toll-free telephone number that consumers may call to opt out.

(c) A licensee does not provide a reasonable means of opting out if:

(i) The only means of opting out is for the consumer to write a letter to the licensee to exercise their opt-out right; or

(ii) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the licensee provided with the initial notice but did not include with the subsequent notice.

(d) A licensee may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

B. A licensee may provide the opt-out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 7.

C. If a licensee provides the opt-out notice after it provides the initial notice, the licensee shall include a copy of the initial notice with the opt-out notice in writing or, if the consumer agrees, electronically.

D. Joint relationships.

(1) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt-out notice. The licensee's opt-out notice shall explain how the licensee will treat an opt-out direction by a joint consumer (as explained in Paragraph (2) of this subsection).

(2) Any of the joint consumers may exercise the right to opt out. The licensee may either:

(a) Treat an opt-out direction by a joint consumer as applying to all of the associated joint consumers; or

(b) Permit each joint consumer to opt out separately.

(3) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all the joint consumers.

(4) A licensee may not require all joint consumers to opt out before it implements any opt-out direction.

E. A licensee shall comply with a consumer's opt-out direction as soon as reasonably practicable but no later than 10 days after the licensee receives it.

F. A consumer may exercise the right to opt out at any time. A consumer's direction to opt-out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.

Section 139. Revised ~~Privacy~~ Notice of Information Practices~~s~~

A. ~~General rule.~~Except as otherwise authorized in this Act~~regulation~~, a licensee shall not, directly or through an affiliate, disclose any nonpublic personal ~~financial~~ information about a consumer to a nonaffiliated third party other than as described in the initial notice that the licensee provided to that consumer under Section ~~5~~7, unless:

(1) The licensee has provided to the consumer a clear and conspicuous revised notice that accurately describes its policies and practices;

(2) The licensee has provided to the consumer a new opt-out notice;

(3) The licensee has given the consumer a reasonable opportunity, before the licensee discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(4) The consumer does not opt out.

B. Examples.

(1) Except as otherwise permitted by Sections 1~~9~~5, 20~~16~~ and 21~~17~~, a licensee shall provide a revised notice before it:

(a) Discloses a new category of nonpublic personal ~~financial~~ information to any nonaffiliated third party; or

(b) Discloses nonpublic personal ~~financial~~ information to a new category of nonaffiliated third party.~~; or~~

~~(c) Discloses nonpublic personal financial information about a former customer to a nonaffiliated third party, if that former customer has not had the opportunity to exercise an opt out right regarding that disclosure.~~

(2) A revised notice is not required if the licensee discloses nonpublic personal ~~financial~~ information to a new nonaffiliated third party that the licensee adequately described in its prior notice.

~~C. Delivery. When a licensee is required to deliver a revised privacy notice by this section, the licensee shall deliver it according to Section 11.~~

Section 14~~0~~. ~~Privacy~~ Notice~~s~~ of Information Practices to Group Policyholders

Unless a licensee is providing notices of information practices~~privacy notices~~ directly to covered individuals described in Section 4~~F~~(G)2)(e)(i), (ii) or (iii), a licensee shall provide initial, annual and revised notices to the plan sponsor, group or blanket insurance policyholder or group annuity contract holder, or workers' compensation policyholder, in the manner described in Sections ~~9~~7~~5~~ through 13~~9~~ of this Act~~regulation~~, describing the licensee's privacy practices with respect to nonpublic personal information about individuals covered under the policies, contracts or plans. Compliance with this section satisfies the licensees initial, annual and renewal Notice of Information Practices as required by Sections 7 and 8 and delivery provisions of Section 15.

Section 15~~1~~. Delivery

Commented [A8]: Should there be a requirement to maintain notices for a specific or minimum record retention period?

A. ~~How to provide notices.~~ A licensee shall provide any notices that this Act~~regulation~~ requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer interacts with the licensee online or in some other electronic fashion, ~~agrees,~~ electronically.

B. (1) ~~Examples of reasonable expectation of actual notice.~~ A licensee may reasonably expect that a consumer will receive actual notice if the licensee:

(a) Hand-delivers a printed copy of the notice to the consumer;

(b) Mails a printed copy of the notice to the last known address of the consumer separately, or in a policy, billing or other written communication;

(c) For a consumer who conducts transactions electronically, in accordance with UETA (insert state electronic transactions act statute), posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service;

(i) The notice should be posted in a manner that enables a consumer to print or save it using programs or apps that are widely available and free of charge.

(ii) Notice is available electronically as long as it is in force.

(d) For an isolated transaction with a consumer, such as the licensee providing an insurance quote or selling the consumer travel insurance, posts the notice and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular insurance product or service.

(e) Provides the notice by any other means authorized by the commissioner.

(2) Examples of unreasonable expectation of actual notice. A licensee may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:

(a) Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or

(b) Sends the notice via electronic mail to a consumer who does not otherwise

© 202617 National Association of Insurance Commissioners

communicate with ~~obtain an insurance product or service from~~ the licensee electronically.

C. ~~Annual notices only.~~ A licensee may reasonably expect that a consumer~~ustomer~~ will receive actual notice of the licensee's ~~annual privacy n~~Notice ~~if.~~ of Information Practices if:

(1) The consumer~~ustomer~~ uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or

(2) The consumer~~ustomer~~ has requested that the licensee refrain from sending any information regarding the consumer~~ustomer~~ relationship, and the licensee's current privacy notice remains available to the consumer~~ustomer~~ upon request.

D. A licensee may not provide any notice required by this Act solely by orally explaining the notice, either in person or over the telephone.

E. A licensee may provide a joint notice from the licensee and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the licensee and the other institutions. A licensee also may provide a notice on behalf of another financial institution.

F. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of Sections 7A, 8A and 13A, respectively, by providing one notice to those consumers jointly.

~~D. Oral description of notice insufficient. A licensee may not provide any notice required by this regulation solely by orally explaining the notice, either in person or over the telephone.~~

~~E. Retention or accessibility of notices for customers.~~

~~(1) For customers only, a licensee shall provide the initial notice required by Section 5A(1), the annual notice required by Section 6A, and the revised notice required by Section 9 so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.~~

~~(2) Examples of retention or accessibility. A licensee provides a privacy notice to the customer so that the customer can retain it or obtain it later if the licensee:~~

~~(a) Hand delivers a printed copy of the notice to the customer;~~

~~(b) Mails a printed copy of the notice to the last known address of the customer; or~~

~~(c) Makes its current privacy notice available on a web site (or a link to another web site) for the customer who obtains an insurance product or service electronically and agrees to receive the notice at the web site.~~

~~F. Joint notice with other financial institutions. A licensee may provide a joint notice from the licensee and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the licensee and the other institutions. A licensee~~

~~also may provide a notice on behalf of another financial institution.~~

~~G. Joint relationships. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of Sections 5A, 6A and 9A, respectively, by providing one notice to those consumers jointly.~~

ARTICLE V~~III~~. LIMITS ON DISCLOSURES OF NONPUBLIC~~FINANCIAL~~ PERSONAL INFORMATION

Section 16. General Rules for Use and Disclosure of Nonpublic Personal Information

A. Use and Disclosure

(1) A licensee may use and disclose nonpublic personal information about a consumer for purposes of processing a business transaction requested or authorized by the consumer.

(2) A licensee may disclose nonpublic personal information with affiliates, provided the affiliates' use and disclosure comply with this Act.

(3) A licensee shall not disclose nonpublic personal information to a nonaffiliated third party except as permitted by this Act.

(4) This section applies to nonpublic personal information collected before and after a consumer exercises an opt-out right under Section 19 or an opt-in right under Sections 20 and 21.

(5) If a consumer submits an opt-out request during a transaction and the requested information is necessary to complete that transaction, the licensee shall:

(a) Inform the consumer that the transaction cannot be completed without the information; and

(b) Confirm whether the consumer wishes to proceed.

B. Limits on Disclosure. Except as provided by Section 16A(1), before disclosing a consumer's nonpublic personal information to a nonaffiliated third party, whether directly or through an affiliate, a licensee shall:

(1) Provide the initial notice required by Section 7;

(2) Provide a clear and conspicuous notice to the consumer that details:

(a) The consumer's right to opt out of disclosure for targeted advertising under Section 19;

(b) The consumer's option to opt in to the sale of nonpublic personal information under Section 20; or

(c) The consumer's option to opt in to the disclosure of sensitive personal information Section 21.

(3) Provide a reasonable opportunity for the consumer to exercise any applicable opt-out right before disclosure; and

(4) Obtain and document the consumer's opt-in or opt-out election, as applicable.

~~**Section 12. Limits on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties**~~

A. (1) Conditions for disclosure. Except as otherwise authorized in this regulation, a licensee may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party unless:

(a) The licensee has provided to the consumer an initial notice as required under Section 5;

(b) The licensee has provided to the consumer an opt out notice as required in Section 8;

(c) The licensee has given the consumer a reasonable opportunity, before it discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(d) The consumer does not opt out.

(2) Opt out definition. Opt out means a direction by the consumer that the licensee not disclose nonpublic personal financial information about that consumer to a nonaffiliated third party, other than as permitted by Sections 15, 16 and 17.

(3) Examples of reasonable opportunity to opt out. A licensee provides a consumer with a reasonable opportunity to opt out if:

(a) By mail. The licensee mails the notices required in Paragraph (1) of this subsection to the consumer and allows the consumer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within thirty (30) days from the date the licensee mailed the notices.

(b) By electronic means. A customer opens an on-line account with a licensee and agrees to receive the notices required in Paragraph (1) of this subsection electronically, and the licensee allows the customer to opt out by any reasonable means within thirty (30) days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.

(c) Isolated transaction with consumer. For an isolated transaction such as providing the consumer with an insurance quote, a licensee provides the consumer with a reasonable opportunity to opt out if the licensee provides the notices required in Paragraph (1) of this subsection at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

B. Application of opt out to all consumers and all nonpublic personal financial information.

(1) A licensee shall comply with this section, regardless of whether the licensee and the consumer have established a customer relationship.

(2) Unless a licensee complies with this section, the licensee may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer that the licensee has collected, regardless of whether the licensee collected it before or after receiving the direction to opt out from the consumer.

~~C. Partial opt-out. A licensee may allow a consumer to select certain nonpublic personal financial information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out.~~

Section 1~~7~~3. Limits on Redisclosure and Reuse of Nonpublic Personal ~~Financial~~ Information

A. ~~(1) Information the licensee receives under an exception.~~ If a licensee receives nonpublic personal ~~financial~~ information from a nonaffiliated third-party service provider~~financial institution~~ under an exception in ~~Sections 20~~16 ~~or 17 or~~ Article VI of this Act~~regulation~~, ~~the licensee's disclosure and use of that information is limited as follows:~~

~~(a) The licensee may disclose the information to the affiliates of the financial institution from which the licensee received the information;~~

~~(b) The licensee may disclose the information to its affiliates, but the licensee's affiliates may, in turn, disclose and use the information only to the extent that the licensee may disclose and use the information; and~~

~~(a~~c~~)~~ t~~T~~he licensee may use and disclose the information ~~pursuant to an exception in Sections 16 or 17 of this regulation,~~ in the ordinary course of business to carry out the activity covered by the exception under which the licensee received the information.

~~(2) Example. If a licensee receives information from a nonaffiliated financial institution for claims settlement purposes, the licensee may disclose the information for fraud prevention, or in response to a properly authorized subpoena. The licensee may not disclose that information to a third party for marketing purposes or use that information for its own marketing purposes.~~

B. (1) ~~Information a licensee receives outside of an exception.~~ If a licensee receives nonpublic personal ~~financial~~ information from a nonaffiliated third-party service provider~~financial institution~~ other than under an exception in ~~Sections 20 or~~ Article VI~~16 or 17~~ of this Act~~regulation~~, the licensee may disclose the information only to the following, provided the disclosure is consistent with this Act:

(a) ~~To the A~~affiliates of the third party-service provider~~financial institution~~ from which the licensee received the information; and

(b) ~~To its A~~affiliates of the licensee who may~~, but its affiliates may, in turn,~~ disclose the information only to the extent that the ~~licensee may disclose the information;~~disclosure would be permissible by the licensee pursuant to this Act. ~~and~~

~~(c) To any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which the licensee received the information.~~

(2) Example. If a licensee obtains a customer list from a nonaffiliated third-party service provider~~financial institution~~ outside of the exceptions in ~~Sections 16 or 17:~~20 ~~or~~ Article VI:

(a) The licensee may use that list for its own purposes~~; and~~ consistent with this Act; and

(b) The licensee may disclose that list to another nonaffiliated third-party service provider only as permitted by this Act.~~if the financial institution from which the licensee purchased the list could have lawfully disclosed the list to that third party. That is, the licensee may disclose the list in accordance with the privacy policy of the financial institution from which the licensee received the list, as limited by the opt-out direction of each consumer whose nonpublic personal financial information the licensee intends to disclose, and the licensee may disclose the list in accordance with an exception in Sections 16 or 17, such as to the licensee's attorneys or accountants.~~

C. ~~Information a licensee discloses under an exception.~~ If a licensee discloses nonpublic personal ~~financial~~ information to a nonaffiliated third-party service provider under an exception in S~~ections 16 or 17 20 or~~ Article VI of this Act~~of this regulation~~, the third party-service provider:~~ may disclose and use that information only as follows:~~

(1) ~~The third party~~ M~~m~~ay disclose the information to the licensee's affiliates; and

~~(2) The third party may disclose the information to its affiliates, but its affiliates may, in turn, disclose and use the information only to the extent that the third party may disclose and use the information; and~~

(2~~3~~) ~~The third party~~ M~~m~~ay disclose and use the information ~~pursuant to an exception in Sections 16 or 17~~ in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

D. ~~Information a licensee discloses outside of an exception.~~ If a licensee discloses nonpublic personal ~~financial~~ information to a nonaffiliated third-party service provider other than under an exception in ~~Sections 20 16 or 17 or~~ Article VI of this Act~~regulation~~, the third-party service provider may disclose the information only:

(1) To the licensee's affiliates~~;~~ who may disclose the information only to the extent that it would be permissible for the licensee to disclose the information pursuant to this Act;~~:~~ and

~~(2) To the third party's affiliates, but the third party's affiliates, in turn, may disclose the information only to the extent the third party can disclose the information; and~~

(2~~3~~) To any other person, if the disclosure would be lawful if the licensee made it directly to that person.

Commented [A9]: I don't understand this reference, "S Article VI"

Section 18~~14~~. Limits on Sharing Access Number or Access Code~~Account Number~~ Information for Marketing Purposes

A. ~~General prohibition on disclosure of account numbers.~~ A licensee shall not, directly or through an affiliate, disclose, other than to a consumer reporting agency, a policy number or similar form of access number or access code for a consumer's policy or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

B. Exceptions. Subsection A of this section does not apply if a licensee discloses a policy number or similar form of access number or access code:

(1) To the licensee's service provider solely in order to perform marketing for the licensee's own products or services, as long as the service provider is not authorized to directly initiate charges to the account;

(2) To a licensee who is a producer solely in order to perform marketing for the licensee's own products or services; or

(3) To a participant in an affinity or similar program where the participants in the program are identified to the consumer~~ustomer~~ when the consumer~~ustomer~~ enters into the program.

(4) Where the policy number, or similar form of access number or access code, is in an encrypted form, as long as the licensee does not provide a means to decode the access number or access code.

~~C. Examples.~~

~~(1) Policy number. A policy number, or similar form of access number or access code, does not include a number or code in an encrypted form, as long as the licensee does not provide the recipient with a means to decode the number or code.~~

~~(2) Policy or transaction account. For the purposes of this section, a policy or transaction account is an account other than a deposit account or a credit card account. A policy or transaction account does not include an account to which third parties cannot initiate charges.~~

Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted ~~Marketing~~ Advertising

A. Except as otherwise authorized in this Act, a licensee may not, directly or through any affiliate, disclose for the purpose of targeted advertising any nonpublic personal information about a consumer to a nonaffiliated third party unless the consumer has been provided clear and conspicuous notice and a reasonable opportunity to opt out of targeted advertising in accordance with the requirements of Section 12 of this Act.

B. A licensee shall act on a consumer's request to opt out within 15 days of receipt.

C. A licensee is under no obligation to obtain additional information to execute the opt-out request.

D. A licensee may not solicit the consumer to change their election to opt -out for twelve months.

E. A consumer has the right to opt out at any time.

Section 20. Limits on Sale of Nonpublic Personal Information

Before a licensee may sell nonpublic personal information:

A. The licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

B. The consumer must affirmatively opt in to the sale of their nonpublic personal information.

Section 21. Limits on Disclosure of Sensitive Personal Information

A. Except as provided by Subsection B below, a licensee may disclose a consumer's sensitive personal information only for those purposes and uses identified in Article VI and as expressly permitted or required by Article VI or other provisions of this Act.

B. Before a licensee may disclose a consumer's sensitive personal information for purposes other than those specified in subsection A of this section:

(1) A licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

(2) The consumer must affirmatively opt in to disclosure of their sensitive personal information.

© 20261~~7~~ National Association of Insurance Commissioners

ARTICLE ~~I~~V[I]. EXCEPTIONS TO LIMITS ON DISCLOSURES OF ~~FINANCIAL~~ NONPUBLIC PERSONAL INFORMATION

Section 22~~5~~. Exception to Opt-Out Requirements for Disclosure of Nonpublic Personal ~~Financial~~ Information for Service Providers and Joint Marketing

A. General rule.

(1) The opt-out requirements in Sections 12~~-8~~ and ~~16~~219 do not apply when a licensee provides nonpublic personal ~~financial~~ information to a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf, if the licensee:

(a) Provides the initial notice in accordance with Section ~~-95~~7; and

(b) Enters into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in Sections ~~2516 or 2617~~23 or 24 in the ordinary course of business to carry out those purposes.

(2) Example. If a licensee discloses nonpublic personal ~~financial~~ information under this section to a financial institution with which the licensee performs joint marketing, the licensee's contractual agreement with that institution meets the requirements of Paragraph (1)(b) of this subsection if it prohibits the institution from disclosing or using the nonpublic personal ~~financial~~ information except as necessary to carry out the joint marketing or under an exception in Sections ~~2516 or 2617~~23 or 24 in the ordinary course of business to carry out that joint marketing.

B. Service may include joint marketing. The services a nonaffiliated third party performs for a licensee under Subsection A of this section may include marketing of the licensee's own products or services or marketing of financial products or services offered pursuant to joint agreements between the licensee and one or more financial institutions.

C. Definition of "joint agreement." For purposes of this section, "joint agreement" means a written contract pursuant to which a licensee and one or more financial institutions jointly offer, endorse or sponsor a financial product or service.

Section 23~~16~~. Exceptions to Notice and Opt-Out Requirements for Disclosure of Nonpublic Personal ~~Financial~~ Information for Processing and Servicing Transactions

A. Exceptions for processing transactions at consumer's request. The requirements for initial notice in Section ~~9~~75A(2), the opt-out in Sections 12~~8~~ and ~~16~~219, and service providers and joint marketing in Section ~~24~~1522 do not apply if the licensee discloses nonpublic personal ~~financial~~ information as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Servicing or processing an insurance product or service that a consumer requests or authorizes;

(2) Maintaining or servicing the consumer's account with a licensee, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity;

(3) A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer; or

(4) Reinsurance or stop loss or excess loss insurance.

B. "Necessary to effect, administer or enforce a transaction" means that the disclosure is:

(1) Required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or

(2) Required, or is a usual, appropriate or acceptable method:

(a) To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer's account in the ordinary course of providing the insurance product or service;

(b) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

(c) To provide a confirmation, statement or other record of the transaction, or information on the status or value of the insurance product or service to the consumer or the consumer's agent or broker;

(d) To accrue or recognize incentives or bonuses associated with the transaction that are provided by a licensee or any other party;

(e) To underwrite insurance at the consumer's request or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects or as otherwise required or specifically permitted by federal or state law; or

(f) In connection with:

(i) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited or otherwise paid using a debit, credit or other payment card, check or account number, or by other payment means;

(ii) The transfer of receivables, accounts or interests therein; or

(iii) The audit of debit, credit or other payment information.

© 2026~~17~~ National Association of Insurance Commissioners

Section 2417. Other Exceptions to Notice and Opt-Out Requirements for Disclosure of Nonpublic Personal ~~Financial~~ Information

A. Exceptions to opt-out requirements. The requirements for initial notice to consumers in Section 957A(2), the opt-out in Sections 128 and 1692, and service providers and joint marketing in Section 24195 22 do not apply when a licensee discloses nonpublic personal ~~financial~~ information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

(2) (a) To protect the confidentiality or security of a licensee's records pertaining to the consumer, service, product or transaction;

(b) To protect against or prevent actual or potential fraud or unauthorized transactions;

(c) For required institutional risk control or for resolving consumer disputes or inquiries;

(d) To persons holding a legal or beneficial interest relating to the consumer; or

(e) To persons acting in a fiduciary or representative capacity on behalf of the consumer;

(f) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted nonpublic personal information.

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating a licensee, persons that are assessing the licensee's compliance with industry standards, and the licensee's attorneys, accountants and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the federal Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, the Securities and Exchange Commission, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance authority, and the Federal Trade Commission), self-regulatory organizations or for an investigation on a matter related to public safety;

(5) (a) To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or

(b) From a consumer report reported by a consumer reporting agency;

(6) In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal ~~financial~~ information concerns solely consumers of the business or unit;

(7) (a) To comply with federal, state or local laws, rules and other applicable legal requirements;

(b) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities; or

(c) To respond to judicial process or government regulatory authorities having jurisdiction over a licensee for examination, compliance or other purposes as authorized by law; or

(8) For purposes related to the replacement of a group benefit plan, a group health plan, a group welfare plan or a workers' compensation plan.

B. Example of revocation of consent. A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under Section ~~12~~8F.~~.~~12F.

Drafting Note: Because the notice requirements of this Act ~~regulation~~ could be a financial burden on a company in liquidation or receivership and negatively impact the ability of the liquidator or receiver to pay claims, regulators may want to consider adding an additional exception providing that licensees in liquidation or receivership are not subject to the notice provisions of this ~~.~~ Act~~regulation~~.

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 2518. When Authorization Required for Disclosure of Nonpublic Personal Health Information

A. A licensee shall not disclose nonpublic personal health information about a consumer ~~or customer~~ unless an authorization is obtained from the consumer ~~or customer~~ whose nonpublic personal health information is sought to be disclosed.

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee: ~~claims administration; claims adjustment and management; detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity; underwriting; policy placement or issuance; loss control; ratemaking and guaranty fund functions; reinsurance and excess loss insurance; risk management; case management; disease management; quality assurance; quality improvement; performance evaluation; provider credentialing verification; utilization review; peer review activities; actuarial, scientific, medical or public policy research; grievance procedures; internal administration of compliance, managerial, and information systems; policyholder service functions; auditing; reporting; database security; administration of consumer disputes and inquiries; external accreditation standards; the replacement of a group benefit plan or workers compensation policy or program; activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit; any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services; disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes; and any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.~~

(1) Claims administration ~~,~~ and~~y~~ processing~~claims~~;

(2) Claims adjustment and management;

(3) Detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity;

(4) Underwriting;

(5) Policy placement or issuance;

(6) Loss control;

(7) Ratemaking and guaranty fund functions;

(8) Reinsurance and excess loss insurance;

(9) Risk management;

(10) Case management;

(11) Disease management;

(12) Quality assurance;

(13) Quality improvement;

(14) Performance evaluation;

(15) Provider credentialing verification;

(16) Utilization review;

(17) Peer review activities;

(18) Actuarial, scientific, medical or public policy research;

(19) Grievance procedures;

(20) Internal administration of compliance, managerial, and information systems;

(21) Policyholder service functions;

(22) Auditing;

(23) Reporting;

(24) Database security;

(25) Administration of consumer disputes and inquiries;

(26) External accreditation standards;

(27) The replacement of a group benefit plan or workers' compensation policy or program;

(28) Activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit;

(29) Any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services or other applicable laws;

(30) Disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes including subrogation, and

(31) Any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with the legal process.

C. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable

Section ~~19~~26. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article VII shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer ~~or customer~~ who is the subject of the nonpublic personal health information;

(2) A general description of the types of nonpublic personal health information to be disclosed;

(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

~~–~~(4) The signature, including electronic signatures, of the consumer ~~or customer~~ who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer ~~or customer~~ may revoke the authorization at any time and the procedure for making a revocation.

(6) Any additional information necessary to comply with HIPAA or any other applicable law.

B. An authorization for the purposes of this Article VII shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer ~~or customer~~ who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article VII at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

E. A signed copy of the authorization shall be provided to the consumer.

© 2026~~17~~ National Association of Insurance Commissioners

Section 27.0. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer ~~or a customer~~ as part of an opt-out notice pursuant to Section ~~15~~12, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer ~~or customer~~ or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section ~~18~~25A.

Section 28~~1~~. Relationship to Federal Rules

A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

This Act shall not apply to nonprofits, such as the National Association of Insurance Commissioners or the National Insurance Crime Bureau, when processing or sharing information solely for investigating criminal or fraudulent insurance acts. ~~Irrespective of whether a licensee is subject to the federal Health Insurance Portability and Accountability Act privacy rule as promulgated by the U.S. Department of Health and Human Services [insert cite] (the "federal rule"), if a licensee complies with all requirements of the federal rule except for its effective date provision, the licensee shall not be subject to the provisions of this Article V.~~

~~**Drafting Note:** The drafters note that the effective date of this Act regulation is July 1, 2001. The HHS regulation is anticipated to be promulgated in late 2000, thereby becoming effective in late 2002. As of July 1, 2001, if the licensee is in compliance with all requirements of the HHS regulation except its effective date provision, the licensee is not subject to the provisions of this articlethis Article. If the licensee comes into compliance with the HHS regulation after that date, the licensee is no longer subject to the provisions of this aArticle as of the date the licensee comes into compliance with the HHS regulation.~~

Section 29~~2~~. Relationship to State Laws

Nothing in ~~this article~~this Article shall preempt or supersede ~~supercede~~ existing state law related to medical records, consumer data privacy, health or insurance information privacy.

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 3023. Protection of Fair Credit Reporting Act

Nothing in this regulation Act shall be construed to modify, limit or supersede the operation of the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and no inference shall be made drawn on the basis of the provisions of this regulation Act regarding whether information is transaction or experience information under Section 603 of that Act.

Section 3124. Nondiscrimination

A. A licensee shall not unfairly discriminate against any consumer or customer because that consumer or customer has opted out from the disclosure of his or her nonpublic personal financial information pursuant to the provisions of this regulationAct.

B. A licensee shall not unfairly discriminate against a consumer or customer because that consumer or customer has not granted authorization for the disclosure of his or her nonpublic personal health information pursuant to the provisions of this regulationAct.

Section 3225. Violation

Drafting Note: Cite state unfair trade practices act or other applicable state law.

Section 3326. Severability

If any section or portion of a section of this regulation Act or its applicability to any person or circumstance is held invalid by a court, the remainder of the regulation Act or the applicability of the provision to other persons or circumstances shall not be affected.

Section 34. Individual Remedies

This Act may not be construed to create or imply a private cause of action for violation of its provisions, nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Section 3527. Effective Date

A. Effective date. This Act regulation has beenis effective since November 13, 2000. The amendments to this Act are effective [Insert Effective Date]. In order to provide sufficient time for licensees to establish policies and systems to comply with the amendmentsrequirements toof this regulationAct, the commissioner has extended the time for compliance with theis amendments to this Actregulation until [Insert Compliance Date]July 1, 2001.

B. (1) By [Insert Compliance Date], a licensee shall provide an initial notice, as required by Section 7, to any existing consumer who has not previously received a notice that complies with the amendments to this Act. Notice requirement for consumers who are the licensee's customers on the compliance date. By July 1, 2001, a licensee shall provide an initial notice, as required by Section 5, to consumers who are the licensee's customers on July 1, 2001.

Commented [A10]: Same recommendation re: gendered language. Reword to remove "his or her," e.g., "A licensee shall not unfairly discriminate against any consumer **for opting out of the disclosure of the consumer's** nonpublic personal information pursuant to the provisions of this Act." or "A licensee shall not unfairly discriminate against any consumer because that consumer has opted out from the disclosure of **their** nonpublic personal information pursuant to the provisions of this Act."

Commented [A11]: Same recommendation re: gendered language.

~~(2) Example. A licensee provides an initial notice to consumers who are its customers on [Insert Date]July 1, 2001, if, by that date, the licensee has established a system for providing an initial notice to all new customers and has mailed the initial notice to all the licensee's existing customers.~~

C. Two-year grandfathering of service agreements. Until [Insert Compliance Date]~~July 1, 2002~~, a contract that a licensee has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf satisfies the provisions of Section ~~15~~22A(1)(b) of this ~~regulation~~Act, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the licensee entered into the agreement on or before [Insert Compliance Date]~~July 1, 2000~~.

Commented [A12]: Recommendation to consider more neutral language (because "grandfathered" has non-neutral historical connotations), e.g., "two-year phase-in period" or "legacy service agreements."

APPENDIX A – SAMPLE CLAUSES

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A-1–Categories of information a licensee collects (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section ~~7A~~9A(1) to describe the categories of nonpublic personal information the licensee collects.

Sample Clause A-1:

We collect nonpublic personal information about you from the following sources:

Information we receive from you on applications or other forms;
Information about your transactions with us, our affiliates or others; and
Information we receive from a consumer reporting agency.

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-1 expires on July 1, 2019.~~

A-2–Categories of information a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use one of these clauses, as applicable, to meet the requirement of Section ~~7A~~9A(2) to describe the categories of nonpublic personal information the licensee discloses. The licensee may use these clauses if it discloses nonpublic personal information other than as permitted by the exceptions in Sections ~~15~~22, ~~16~~ 23 and ~~17~~24.

Sample Clause A-2, Alternative 1:

We may disclose the following kinds of nonpublic personal information about you:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premiums, and payment history"]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your creditworthiness and credit history"].

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-2, Alternative 1 expires on July 1, 2019.~~

Sample Clause A-2, Alternative 2:

We may disclose all of the information that we collect, as described [describe location in the notice, such as "above" or "below"].

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-2, Alternative 2 expires on July 1, 2019.~~

© 2026~~17~~ National Association of Insurance Commissioners

A-3–Categories of information a licensee discloses and parties to whom the licensee discloses (institutions that do not disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirements of Sections ~~7A~~9A(2) and~~,~~ (3)~~, and (4)~~ to describe the categories of nonpublic personal information ~~about customers and former customers that~~ the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses. A licensee may use this clause if the licensee does not disclose nonpublic personal information to any party, other than as permitted by the exceptions in Sections ~~16~~ 23 and ~~17~~24.

Sample Clause A-3:

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-3 expires on July 1, 2019.~~

A-4–Categories of parties to whom a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section ~~7A~~9A(3) to describe the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information. This clause may be used if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections ~~15~~22, ~~16~~ 23 and ~~17~~24~~, as well as when permitted by the exceptions in Sections 16 and 17~~.

Sample Clause A-4:

We may disclose nonpublic personal information about you to the following types of third parties:

Financial service providers, such as [provide illustrative examples, such as "life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents"];

Non-financial companies, such as [provide illustrative examples, such as "retailers, direct marketers, airlines, and publishers"]; and

Others, such as [provide illustrative examples, such as "non-profit organizations"].

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-4 expires on July 1, 2019.~~

A-5–Service provider/joint marketing exception
A licensee may use one of these clauses, as applicable, to meet the requirements of Section ~~7A~~9A(~~5~~2) related to the exception for service providers and joint marketers in Section ~~15~~22. If a licensee discloses nonpublic personal information under this exception, the licensee shall describe the categories of nonpublic personal information the licensee discloses and the categories of third parties with which the licensee has contracted.

Sample Clause A-5, Alternative 1:

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as

"your name, address, social security number, assets, income, and beneficiaries"];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premium, and payment history"]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your creditworthiness and credit history"].

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-5, Alternative 1 expires on July 1, 2019.~~

Sample Clause A-5, Alternative 2:

We may disclose all of the information we collect, as described [describe location in the notice, such as "above" or "below"] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-5, Alternative 2 expires on July 1, 2019.~~

A-6–Explanation of opt-~~-~~out right (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section ~~7A~~9A(~~6~~4) to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. The licensee may use this clause if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections ~~15~~22, ~~16~~ 23 and ~~17~~24.

Sample Clause A-6:

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [describe a reasonable means of opting out, such as "call the following toll-free number: (insert number)].

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-6 expires on July 1, 2019.~~

A-7–Confidentiality and security (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section ~~7A~~9A(8) to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A-7:

We restrict access to nonpublic personal information about you to [provide an appropriate description, such as "those employees who need to know that information to provide products or services to you"]. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-7 expires on July 1, 2019.~~

APPENDIX B – FEDERAL MODEL PRIVACY FORM

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the Federal Model Privacy Form, if the Form is accurate for each institution that uses the Form. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A. General Instructions

1. How the Model Privacy Form is used.

(a) The Model Form may be used, at the option of a "licensee"~~)~~, including a group of licensees or other financial institutions that use a common privacy notice, to meet the content requirements of the privacy notice and opt-out notice set forth in [insert citation for sections of statute or regulation sections that parallel Sections ~~7~~ 9and ~~8~~ 11 of the NAIC *Privacy of Consumer ~~Financial and Health~~ Information ~~Act~~Regulation*]

(b) The Model Form is a standardized form, including page layout, content, format, style, pagination, and shading. Licensees seeking to obtain the safe harbor through use of the Model Form may modify it only as described in these Instructions.

(c) Note that disclosure of certain information, such as assets, income, and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act (FCRA), codified at 15 U.S.C. §§ 1681-1681x, such as a requirement to permit a consumer to opt out of disclosures to affiliates, or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.

(d) The word "consumer~~ustomer~~" may be replaced by the word "member," whenever it appears in the Model Form, as appropriate.

2. The Contents of the Model Privacy Form

The Model Form consists of two pages, which may be printed on both sides of a single sheet of paper or may appear on two separate pages. Where a licensee provides a long list of licensees or financial institutions at the end of the Model Form in accordance with Instruction B3(a)(i), or provides additional information in accordance with Instruction B3(c) and such list or additional information exceeds the space available on Page Two of the Model Form, such list or additional information may extend to a third page.

(a) Page One. The first page consists of the following components:

(1) Date last revised (upper right-hand corner)
(2) Title
(3) Key frame (Why? What? How?)
(4) Disclosure table ("Reasons we can share your personal information")
(5) "To limit our sharing" box, as needed, for the licensee's opt-out information
(6) "Questions" box, for customer service contact information
(7) Mail-in opt-out form, as needed

(b) Page Two. The second page consists of the following components:

© 2026~~17~~ National Association of Insurance Commissioners

(1) Heading (Page 2)
(2) Frequently Asked Questions ("Who we are" and "What we do")
(3) Definitions
(4) "Other important information" box, as needed

3. The format of the Model Privacy Form.

The format of the Model Form may be modified only as described below.

(a) Easily readable type font. Licensees that use the Model Form must use an easily readable type font. While a number of factors together produce easily readable font, licensees are required to use a minimum of 10-point font (unless otherwise expressly permitted in these Instructions) and sufficient spacing between lines.

(b) Logo. A licensee may include a corporate logo on any page of the notice, so long as it does not interfere with the readability of the Model Form or the space constraints of each page.

(c) Page size and orientation. Each page of the Model Form must be printed in portrait orientation, the size of which must be sufficient to meet the layout and minimum font size requirements, with sufficient white space on the top, bottom, and sides of the content.

(d) Color. The Model Form must be printed on white or light color paper (such as cream) with black or other contrasting ink color. Spot color may be used to achieve visual interest, so long as the color contrast is distinctive and the color does not detract from the readability of the Model Form. Logos may also be printed in color.

(e) Languages. The Model Form may be translated into languages other than English.

B. Information Required in the Model Privacy Form

The information in the Model Form may be modified only as described below:

1. Name of licensee or group of affiliated licensees or institutions providing the notice
Insert the name of the licensee providing the notice, or a common identity of the affiliated licensees or financial institutions jointly providing the notice on the form, wherever [name of licensee] appears.

2. Page One

(a) Last revised date. The licensee must insert in the upper right-hand corner the date on which the notice was last revised. The information shall appear in minimum 8-point font as "rev. [month/year]" using either the name or number of the month, such as "rev. July 2016" or "rev. 7/16."

(b) General instructions for the "What?" box

(i) The bulleted list identifies the types of personal information that the licensee collects and shares. All licensees must use the term "Social Security Number" in the first bullet.

(ii) A licensee must use five (5) of the following terms, to complete the bulleted list: income; account balances; payment history; transaction history; transaction or loss history; credit history; credit scores; assets; investment experience; credit-based insurance scores; insurance claim history; medical information; overdraft

history; purchase history; account transactions; risk tolerance; medical-related debts; credit card or other debt; mortgage rates and payments; retirement assets; checking account information; employment information; wire transfer instructions.

(c) General instructions for the disclosure table. The left column lists reasons for sharing or using personal information. Each reason correlates to a specific legal provision described in Paragraph 2(d) of this Instruction. In the middle column, each licensee must provide a "Yes" or "No" response that accurately reflects its information-sharing policies and practices with respect to the reason listed on the left. In the right column, each licensee must provide in each box one of the following three (3) responses, as applicable, that reflects whether a consumer can limit such sharing:

"Yes," if it is required to or voluntarily provides an opt-out; "No," if it does not provide an opt-out; or

"We don't share," if it answers "No" in the middle column.

Only the sixth row ("For our affiliates to market to you") may be omitted at the option of the licensee. See Paragraph 2(d)(6) of this instruction.

(d) Specific disclosures and corresponding legal provisions

(i) For our everyday business purposes. This reason incorporates sharing information under [insert citation for sections of statute or regulation sections that parallel Sections ~~16~~ 23 and ~~17~~ 24 of NAIC model *Privacy of Consumer ~~Financial and Health~~ Information ~~Regulation~~Act*] and with service providers pursuant to [insert citation for section of statute or regulation that parallels Section ~~15~~ 22 of NAIC *Privacy of Consumer ~~Financial and Health~~ Information Act~~Regulation~~*] other than the disclosures described in Paragraphs (2)(d)(ii) or (2)(d)(iii) of this instruction.

(ii) For our marketing purposes. This reason incorporates sharing information with service providers by a licensee for its own marketing pursuant to [insert citation for section of statute or regulation that parallels Section ~~15~~ 22 of NAIC *Privacy of Consumer ~~Financial and Health~~Information ~~Regulation~~Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iii) For joint marketing with other financial companies. This reason incorporates sharing information under joint marketing agreements between 2 or more licensees or financial institutions and with any service provider used in conjunction with such agreement pursuant to [insert citation for section of statute or regulation that parallels Section ~~15~~ 22 of NAIC *Privacy of Consumer ~~Financial and Health~~Information ~~Regulation~~Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iv) For our affiliates' everyday business purposes – information about transactions and experiences. This reason incorporates sharing information specified in Sections 603(d)(2)(A)(i) and (ii) of the FCRA. A licensee that shares information for this reason may choose to provide an opt-out.

(v) For our affiliates' everyday business purposes – information about creditworthiness. This reason incorporates sharing information pursuant to Section 603(d)(2)(A)(iii) of the FCRA. A licensee that shares information for this reason must provide an opt-out.

(vi) For our affiliates to market to you. This reason incorporates sharing information specified in Section 624 of the FCRA. This reason may be omitted from the disclosure table when: the licensee does not have affiliates (or does not disclose personal information to its affiliates); the licensee's affiliates do not use personal information in a manner that requires an opt-out; or the licensee provides the affiliate marketing notice separately. Licensees

that include this reason must provide an opt-out of indefinite duration. A licensee that is required to provide an affiliate marketing opt-out, but does not include that opt-out in the Model Form under this part, must comply with Section 624 of the FCRA and [insert citation for statute or regulation that parallels NAIC *Privacy of Consumer ~~Financial and Health~~ Information Act~~Regulation~~*], with respect to the initial notice and opt-out and any subsequent renewal notice and opt-out. A licensee not required to provide an opt-out under this subparagraph may elect to include this reason in the Model Form.

(vii) For nonaffiliates to market to you. This reason incorporates sharing described in [insert citation for sections of statute or regulation sections that parallel Sections ~~8~~ 11 and ~~12(A)~~16(B) of NAIC *Privacy of Consumer ~~Financial and Health~~ Information Act~~Regulation~~*]. A licensee that shares personal information for this reason must provide an opt-out.

(e) To limit our sharing. A licensee must include this section of the Model Form only if it provides an opt-out. The word "choice" may be written in either the singular or plural, as appropriate. Licensees must select one or more of the applicable opt-out methods described: telephone, such as by a toll-free number; a web site; or use of a mail-in opt-out form. Licensees may include the word "toll-free" before telephone, as appropriate. A licensee that allows consumers to opt out online must provide either a specific web address that takes consumers directly to the opt-out page or a general web address that provides a clear and conspicuous direct link to the opt-out page. The opt-out choices made available to the consumer who contacts the licensee through these methods must correspond accurately to the "Yes" responses in the third column of the disclosure table. In the part entitled "Please note," licensees may insert a number that is 30 days or greater in the space marked "[30]." Instructions on voluntary or state privacy law opt-out information are in Paragraph 2(g)(v) of these Instructions.

(f) Questions box. Customer service contact information must be inserted as appropriate where [phone number] or [web site] appear. Licensees may elect to provide either a phone number, such as a toll-free number, or a web address, or both. Licensees may include the words "toll-free" before the telephone number, as appropriate.

(g) Mail-in opt-out form. Licensees must include this mail-in form only if they state in the "To limit our sharing" box that consumers can opt out by mail. The mail-in form must provide opt-out options that correspond accurately to the "Yes" responses in the third column of the disclosure table. Licensees that require consumers to provide only name and address may omit the section identified as "[account #]." Licensees that require additional or different information, such as a random opt-out number or a truncated account number to implement an opt-out election should modify the "[account #]" reference accordingly. This includes licensees that require customers consumers with multiple accounts to identify each account to which the opt-out should apply. A licensee must enter its opt-out mailing address in the far right of this form (see version 3); or below the form (see version 4). The reverse side of the mail-in opt-out form must not include any content of the Model Form.

(i) Joint accountholder. Only licensees that provide their joint accountholders the choice to opt out for only one accountholder, in accordance with Paragraph 3(a)(5) of these Instructions, must include in the far left column of the mail-in form the following statement:

If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.

□ Apply my choice(s) only to me.

The word "choice" may be written in either the singular or plural, as appropriate. Licensees that provide insurance products or services, provide this option, and elect to use the Model Form may substitute the word "policy" for "account" in this statement. Licensees that do not provide this option may eliminate this left column from the mail-in form.

(ii) FCRA Section 603(d)(2)(A)(iii) opt-out. If the licensee shares personal information pursuant to Section 603(d)(2)(A)(iii) of the FCRA, it must include in the mail-in opt-out form the following statement:

□ Do not share information about my creditworthiness with your affiliates for their everyday business purposes.

(iii) FCRA Section 624 opt-out. If the licensee uses Section 624 of the FCRA, in accord with paragraph 2(d)(6) of these Instructions, it must include in the mail-in opt-out form the following statement:

□ Do not allow your affiliates to use my personal information to market to me.

(iv) Nonaffiliate opt-out. If the licensee shares personal information pursuant to [insert citation for section of statute or regulation that parallels Section ~~12(A)~~16(B) of NAIC *Privacy of Consumer ~~Financial and Health~~ Information-Act~~Regulation~~*], it must include in the mail-in opt-out form the following statement:

□ Do not share my personal information with nonaffiliates to market their products and services to me.

(v) Additional opt-outs. Licensees that use the disclosure table to provide opt-out options beyond those required by Federal law must provide those opt-outs in this section of the Model Form. A licensee that chooses to offer an opt-out for its own marketing in the mail-in opt-out form must include one of the two following statements:

□ Do not share my personal information to market to me. or

□ Do not use my personal information to market to me.

A licensee that chooses to offer an opt-out for joint marketing must include the following statement:

□ Do not share my personal information with other financial institutions to jointly market to me.

(h) Barcodes. A licensee may elect to include a barcode and/or "tagline" (an internal identifier) in 6-point type at the bottom of page one, as needed for information internal to the licensee, so long as these do not interfere with the clarity or text of the form.

3. Page Two

(a) General Instructions for the Questions. Certain Questions on the Model Form may be customized as follows:

(i) "Who is providing this notice?" This question may be omitted where only one licensee provides the Model Form and that licensee is clearly identified in the title on Page One. Two or more licensees or financial institutions that jointly provide the Model Form must use this question to identify themselves as required by [insert citation for section of statute or regulation that parallels Section ~~11(F)~~15(E) of NAIC model *Privacy of Consumer ~~Financial and Health~~ Information Act~~Regulation~~*]. Where the list of licensees or financial institutions exceeds four (4) lines, the licensee must describe in the response to this question the general types of licensees or financial institutions jointly providing the notice and must separately identify those licensees or financial institutions, in minimum 8-point font, directly following the "Other important information" box, or, if that box is not included in the licensee's form, directly following the "Definitions." The list may appear in a multi- column format.

(ii) "How does [name of licensee] protect my personal information?" The licensee may only provide additional information pertaining to its safeguards practices following the designated response to this question. Such information may include information about the licensee's use of cookies or other measures it uses to safeguard personal information. Licensees are limited to a maximum of 30 additional words.

(iii) "How does [name of licensee] collect my personal information?" Licensees must use five (5) of the following terms to complete the bulleted list for this question: open an account; deposit money; pay your bills; apply for a loan; use your credit or debit card; seek financial or tax advice; apply for insurance; pay insurance premiums; file an insurance claim; seek advice about your investments; buy securities from us; sell securities to us; direct us to buy securities; direct us to sell your securities; make deposits or withdrawals from your account; enter into an investment advisory contract; give us your income information; provide employment information; give us your employment history; tell us about your investment or retirement portfolio; tell us about your investment or retirement earnings; apply for financing; apply for a lease; provide account information; give us your contact information; pay us by check; give us your wage statements; provide your mortgage information; make a wire transfer; tell us who receives the money; tell us where to send the money; show your government-issued ID; show your driver's license; order a commodity futures or option trade.

Licensees that collect personal information from their affiliates and/or credit bureaus must include the following statement after the bulleted list: "We also collect your personal information from others, such as credit bureaus, affiliates, or other companies." Licensees that do not collect personal information from their affiliates or credit bureaus but do collect information from other companies must include the following statement instead: "We also collect your personal information from other companies." Only licensees that do not collect any personal information from affiliates, credit bureaus, or other companies can omit both statements.

(iv) "Why can't I limit all sharing?" Licensees that describe state privacy law provisions in the "Other important information" box must use the bracketed sentence: "See below for more on your rights under state law." Other licensees must omit this sentence.

(v) "What happens when I limit sharing for an account I hold jointly with someone else?" Only licensees that provide opt-out options must use this question. Other licensees must omit this question. Licensees must choose one of the following two statements to respond to this question: "Your choices will apply to everyone on your account." or "Your choices will apply to everyone on your account—unless you tell us otherwise." Licensees may substitute the word "policy" for "account" in these statements.

(b) General Instructions for the Definitions. The licensee must customize the space below the responses to the three definitions in this section. This specific information must be in italicized lettering to set off the information from the standardized definitions.

(i) Affiliates. As required by [insert citation for section of statute or regulation that parallels Section ~~7~~9(A)(3) of NAIC *Privacy of Consumer ~~Financial and Health~~ Information ~~Regulation~~Act*], where [affiliate information] appears, the licensee must:

(a) If it has no affiliates, state: "[name of licensee] has no affiliates";

(b) If it has affiliates but does not share personal information with them, state: "[name of licensee] does not share with our affiliates"; or

(c) If it shares with its affiliates, state, as applicable: "Our affiliates include companies with a [common corporate identity of licensee] name; financial companies such as [insert illustrative list of companies]; nonfinancial companies, such as [insert illustrative list of companies]; and others, such as [insert illustrative list]."

(ii) Nonaffiliates. As required by [insert citation for section of statute or regulation that parallels Section ~~7(C)~~(9)(A)(3) of NAIC *Privacy of Consumer ~~Financial and Health~~ Information ~~Act~~Regulation*], where [nonaffiliate information] appears, the licensee must:

(a) If it does not share with nonaffiliated third parties, state: "[name of licensee] does not share with nonaffiliates so they can market to you"; or

(b) If it shares with nonaffiliated third parties, state, as applicable: "Nonaffiliates we share with can include [list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations]."

(iii) Joint Marketing. As required by [insert citation for section of statute or regulation that parallels Section ~~15~~ 22 of NAIC *Privacy of Consumer ~~Financial and Health~~ Information Act~~Regulation~~*], where [joint marketing] appears, the licensee must:

(a) If it does not engage in joint marketing, state: "[name of licensee] doesn't jointly market"; or

(b) If it shares personal information for joint marketing, state, as applicable: "Our joint marketing partners include [list categories of companies such as credit card companies]."

(c) General instructions for the "Other important information" box. This box is optional. The space provided for information in this box is not limited, and an additional page may be used if necessary. Only the following types of information can appear in this box:

(i) State and/or international privacy law information; and/or

(ii) A form by which the consumer may acknowledge receipt of the notice.

Chronological Summary of Actions (all references are to the Proceedings of the NAIC)

2000 Proc. 3rd Quarter 7, 10, 14-36, 904 (adopted).
2002 Proc. 3rd Quarter12, 13, 71, 72-73 (amended).
2017 Spring National Meeting (amended).

© 2026~~17~~ National Association of Insurance Commissioners

Version 1:
Model Form with No Opt-Out

Rev. [insert date]

FACTS	WHAT DOES [Name of Licensee] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores] When you are *no longer* our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

Questions?	Call [phone number] or go to [web site]

© 2026~~17~~ National Association of Insurance Commissioners

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026~~17~~ National Association of Insurance Commissioners

Version 2: Model Form with Opt-Out by Telephone and/or Online

Rev. [insert date]

FACTS	**WHAT DOES** [NAME OF LICENSEE] **DO WITH YOUR PERSONAL INFORMATION?**
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	**Does [name of licensee] share?**	**Can you limit this sharing?**
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

To limit our sharing	■ Call [phone number] —our menu will prompt you through your choice(s) **or** ■ Visit us online: [web site] **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026~~17~~ National Association of Insurance Commissioners

Rev. [insert date

Version 3: Model Form with Mail-in Opt-Out Form

FACTS	**WHAT DOES [NAME OF LICENSEE] DO WITH YOUR PERSONAL INFORMATION?**
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ▪ Social Security number and [income] ▪ [account balances] and [payment history] ▪ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

© 2026~~17~~ National Association of Insurance Commissioners

Page 2

To limit our sharing	▪ Call [phone number] —our menu will prompt you through your choice(s) ▪ Visit us online: [web site] or ▪ Mail the form below **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

Mail-in Form

Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless your mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me.	
	Name	
	Address	
	City, State, Zip	
	[Account #]	
Mail To:	[Name of Licensee] [Address] [City], [ST] [ZIP]	

Page 3

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ▪ [open an account] or [deposit money] ▪ pay your bills] or [apply for a loan] ▪ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ▪ sharing for affiliates' everyday business purposes—information about your creditworthiness ▪ affiliates from using your information to market to you ▪ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ▪ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ▪ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ▪ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026~~17~~ National Association of Insurance Commissioners

Version 4: Optional Mail-in Form

Mail-in Form	
Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me. **Name** **Address** **City, State, Zip** **[Account #]**
Mail To:	[Name of Licensee], [Address 1], [Address 2], [City], [ST] [ZIP]

Virginia:

SCOTT A. WHITE
COMMISSIONER OF INSURANCE
STATE CORPORATION COMMISSION
BUREAU OF INSURANCE

P.O. BOX 1157
RICHMOND, VIRGINIA 23218

1300 E. MAIN STREET
RICHMOND, VIRGINIA 23219

TELEPHONE: (804) 371-9741
www.scc.virginia.gov/boi

September 22, 2026

Re: Comments on the *Privacy of Consumer Financial and Health Information Regulation* (Model #672)

Dear Director Dwyer,

The Virginia Bureau of Insurance ("Bureau") appreciates the ability to offer its comments on the exposed revised draft of the *Privacy of Consumer Financial and Health Information Regulation* (Model #672) to the Privacy Protections (H) Working Group.

As I stated at the Working Group's meeting in Columbus last month, the Bureau supports the proposed revisions to Model #672. The long, transparent process that created the exposed draft yielded a proposal that strikes the appropriate balance between enhancing consumer protection and ensuring that licensees can utilize nonpublic personal information to provide the products and services that policyholders desire.

The Bureau finds that the exposed draft modernizes the insurance data protection regime by:

- making significant improvements to consumer disclosures;
- granting consumers the ability to access, correct, and delete their nonpublic personal information;
- largely maintaining the established opt-out regime; and
- creating narrow exceptions to the opt-out framework by requiring opt-in consent to disclose sensitive personal information or sell nonpublic personal information.

The Bureau provides the attached edits to further refine the definitions in the exposed draft. The Bureau offers its suggested edits for the Working Group's consideration and looks forward to continuing to engage with interested stakeholders and the Working Group to bring this project to a successful conclusion.

Sincerely,
/s/ Dan Bumpus
Deputy Commissioner
Innovative Solutions & Strategies Division

PRIVACY OF CONSUMER INFORMATION ACT

Table of Contents

ARTICLE I. GENERAL PROVISIONS

Section 1. Purpose
Section 2. Scope and Compliance
Section 3. Rule of Construction
Section 4. Definitions

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Section 5. Third-Party Service Provider Arrangements

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7. Initial and Subsequent Delivery Notice of Information Practices to Consumers Required
Section 8. Annual Notice of Information Practices to Consumers Required
Section 9. Information to be Included in Notices of Information Practices
Section 10. Short Form Initial Notice of Information Practices
Section 11. Form of Opt-In Notice to Consumers and Opt-In Methods
Section 12. Form of Opt-Out Notice to Consumers and Opt-Out Methods
Section 13. Revised Notice of Information Practices
Section 14. Notice of Information Practices to Group Policyholders
Section 15. Delivery

ARTICLE V. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 16. General Rules for Use and Disclosure of Nonpublic Personal Information
Section 17. Limits on Redisclosure and Reuse of Nonpublic Personal Information
Section 18. Limits on Sharing Access Number or Access Code Information for Marketing Purposes
Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted Advertising
Section 20. Limits on Sale of Nonpublic Personal Information
Section 21. Limits on Disclosure of Sensitive Personal Information

© 2026 National Association of Insurance Commissioners

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 22. Exception to Opt Out Requirements for Disclosure of Nonpublic Personal Information for Service Providers and Joint Marketing
Section 23. Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Information for Processing and Servicing Transactions
Section 24. Other Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Information

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 25. When Authorization Required for Disclosure of Nonpublic Personal Health Information
Section 26. Authorizations
Section 27 Authorization Request Delivery
Section 28. Relationship to Federal Rules
Section 29. Relationship to State Laws

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 30. Protection of Fair Credit Reporting Act
Section 31. Nondiscrimination
Section 32. Violation
Section 33. Severability
Section 34. Individual Remedies
Section 35. Effective Date

APPENDICES

Appendix A Sample Clauses
Appendix B Federal Model Privacy Form
Model Law Forms

© 2026 National Association of Insurance Commissioners

ARTICLE I. GENERAL PROVISIONS

Section 1. Purpose

Purpose. This Act governs the treatment of nonpublic personal health information and nonpublic personal information about individuals by all licensees of the state insurance department. This Act:

A. Requires a licensee to provide notice to individuals about its privacy policies and practices;

B. Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal information about individuals to affiliates and nonaffiliated third parties; and

C. Provides methods for individuals to prevent a licensee from disclosing that information.

Drafting Note: Whether this model is adopted as an Act or Regulation will depend upon individual state law. If a state adopts the model as an Act, reference to the model as an Act should be updated throughout the model.

Section 2. Scope and Compliance

A. Scope. This Act applies to:

(1) Nonpublic personal information about individuals who seek to obtain, obtain, or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. This Act does not apply to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes; and

(2) All nonpublic personal health information.

B. Compliance. A licensee domiciled in this state that is in compliance with this Act in a state that has not enacted laws or regulations that meet the requirements of Title V of the Gramm-Leach-Bliley Act (PL 102-106) may nonetheless be deemed to be in compliance with Title V of the Gramm-Leach-Bliley Act in the other state.

Drafting Note: Subsection B is intended to give licensees some guidance for complying with Title V of the Gramm-Leach-Bliley Act in those states that do not have laws or regulations that meet GLBA's privacy requirements.

Section 3. Rule of Construction

The examples in this Act, the sample clauses in Appendix A, and the Federal Model Privacy Form in Appendix B of this Act are not exclusive. Compliance with an example, use of a sample clause, or the Federal Privacy Model Form, to the extent applicable, constitutes compliance with this Act.

Licensees may rely on use of the Federal Privacy Form in Appendix B, consistent with the attached instructions, as a safe harbor of compliance with the Notice of Information Practices content requirements of this Act.

Use of the Federal Model Privacy Form is not required. Licensees may continue to use other types of privacy notices, including notices that contain the examples in this Act and/or the sample clauses in Appendix A, provided

© 2026 National Association of Insurance Commissioners

that such notices accurately describe the Licensee's privacy practices and otherwise meet the notice content requirements of this Act.

Section 4. Definitions

As used in this Act, unless the context requires otherwise:

A. "Affiliate" means a company that directly, or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with another company.

B. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

C. (1) "Clear and conspicuous" means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) Examples.

(a) Reasonably understandable. A licensee makes its notice reasonably understandable if it:

(i) Presents the information in the notice in clear, concise sentences, paragraphs and sections;

(ii) Uses short explanatory sentences or bullet lists whenever possible;

(iii) Uses definite, concrete, everyday words and active voice whenever possible;

(iv) Avoids multiple negatives;

(v) Avoids legal and highly technical business terminology whenever possible; and

(vi) Avoids explanations that are imprecise and readily subject to different interpretations.

(b) Designed to call attention. A licensee designs its notice to call attention to the nature and significance of the information in it if the licensee:

(i) Uses a plain-language heading to call attention to the notice;

(ii) Uses a typeface and type size that are easy to read;

(iii) Provides wide margins and ample line spacing;

(iv) Uses boldface or italics for key words; and

© 2026 National Association of Insurance Commissioners

(v) In a form that combines the licensee's notice with other information, uses distinctive type size, style, and graphic devices, such as shading or sidebars.

(c) Notices on web sites. If a licensee provides a notice on a web page, the licensee designs its notice to call attention to the nature and significance of the information in it if the licensee uses text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks or sound) do not distract attention from the notice, and the licensee either:

(i) Places the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(ii) Places a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

D. "Collect" means to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

E. "Commissioner" means the chief insurance regulatory official of the state.

Drafting Note: Use the title of the chief insurance regulatory official wherever the term "commissioner" appears. If the jurisdiction of certain health licensees, such as health maintenance organizations, lies with some state agency other than the insurance department, or if there is dual regulation, a state should add language referencing that agency to ensure the appropriate coordination of responsibilities.

F. "Company" means a corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.

G. (1) "Consumer" means an individual who seeks to obtain, obtains or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or household purposes~~, and about whom the licensee has nonpublic personal information~~, or that individual's legal representative.

Commented [DB1]: An individual is a licensee's consumer regardless of whether the licensee has nonpublic personal information on the individual.

(2) Examples.

(a) An individual who provides nonpublic personal information to a licensee in connection with obtaining or seeking to obtain financial, investment or economic advisory services relating to an insurance product or service is a consumer regardless of whether the licensee establishes an ongoing advisory relationship.

(b) An applicant for insurance prior to the inception of insurance coverage is a licensee's consumer.

(c) An individual who is a consumer of another financial institution is not a licensee's

© 2026 National Association of Insurance Commissioners

consumer solely because the licensee is acting as agent for, or provides processing or other services to, that financial institution.

(d) An individual is a licensee's consumer if:

(i) (I) The individual is a beneficiary of a life insurance policy underwritten by the licensee;

(II) The individual is a claimant under an insurance policy issued by the licensee;

(III) The individual is an insured or an annuitant under an insurance policy or an annuity, respectively, issued by the licensee; or

(IV) The individual is a mortgagor of a mortgage covered under a mortgage insurance policy; and

(ii) The licensee discloses nonpublic personal information about the individual to a nonaffiliated third party other than as permitted under Sections 22, 23, and 24 of this Act.

(e) Provided that the licensee provides the initial, annual and revised notices under Sections 7, 8, and 13 of this Act to the plan sponsor, group or blanket insurance policyholder or group annuity contractholder, or workers' compensation policyholder, and further provided that the licensee does not disclose to a nonaffiliated third party nonpublic personal financial information about an individual described in Item (i), (ii) or (iii), other than as permitted under Sections 22, 23, or 24 of this Act, such an individual is not the consumer of the licensee solely because he or she is:

(i) A participant or a beneficiary of an employee benefit plan that the licensee administers or sponsors or for which the licensee acts as a trustee, insurer or fiduciary;

(ii) Covered under a group or blanket insurance policy or group annuity contract issued by the licensee; or

(iii) A claimant covered by a workers' compensation plan.

Drafting Note: In states where the workers' compensation self-insurance or workers' compensation state fund coverage is outside the commissioner's jurisdiction, regulators may wish to urge the applicable agency or agencies to promulgate a regulation similar to this Act in order to ensure parity in treatment of workers' compensation plans and to ensure that all workers covered by such plans have privacy protections.

(f) (i) The individuals described in Subparagraph (e)(i) through (iii) of this paragraph are consumers of a licensee if the licensee does not meet all the conditions of Subparagraph (e).

(ii) In no event shall the individuals, solely by virtue of the status described in Subparagraph (e)(i) through (iii) above, be deemed to be consumers

© 2026 National Association of Insurance Commissioners

for purposes of this Act.

(g) An individual is not a licensee's consumer solely because he or she is a beneficiary of a trust for which the licensee is a trustee.

(h) An individual is not a licensee's consumer solely because he or she has designated the licensee as trustee for a trust.

H. "Consumer reporting agency" has the same meaning as in Section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

I. "Control" means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of voting securities, by contract other than a commercial contract for goods or nonmanagement services, or otherwise, unless the power is the result of an official position with or corporate office held by the person. Control shall be presumed to exist if any person, directly or indirectly, owns, controls, holds with the power to vote, or holds proxies representing, ten percent (10%) or more of the voting securities of any other person. This presumption may be rebutted by a showing made in the manner provided by [Insert Relevant Statute] that control does not exist in fact. The commissioner may determine, after furnishing all persons in interest notice and opportunity to be heard and making specific findings of fact to support the determination, that control exists in fact, notwithstanding the absence of a presumption to that effect.~~:~~

~~(1) Ownership, control or power to vote twenty-five percent (25%) or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;~~

~~(2) Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or~~

~~(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the commissioner determines.~~

Commented [DB2]: Suggested edits align the definition with the Holding Company Act.

J. "De-identified data" means information that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual.

K. (1) "Financial institution" means any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 1843(k)(4)(B) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial institution does not include:

(a) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 *et seq.*);

(b) The Federal Agricultural Mortgage Corporation or any entity charged and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*); or

(c) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions

© 2026 National Association of Insurance Commissioners

related to a transaction of a consumer, as long as the institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

L. (1) "Financial product or service" means a product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 1843(k)(4)(B**)** of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.

M. "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.

N. (1) "Licensee" means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Insurance Law of this state, [and health maintenance organizations holding a certificate of authority pursuant to Section [insert section] of this state's Public Health Law].

Drafting Note: Add bracketed language if HMOs are licensed under other than insurance statutes and cite appropriate state law.

(2) A licensee is not subject to the notice and opt out requirements for nonpublic personal information set forth in Articles I, II, III and IV of this Act if the licensee is an employee, agent or other representative of another licensee ("the principal") and:

(a) The principal otherwise complies with, and provides the notices required by, the provisions of this Act; and

(b) The licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates in a manner permitted by this Act.

(3) (a) Subject to Subparagraph (b), "licensee" shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only in regard to the excess lines placements placed pursuant to Section [insert section] of this state's laws.

(b) An excess lines broker or excess lines insurer shall be deemed to be in compliance with the notice and opt out requirements for nonpublic personal information set forth in Articles I, II, III and IV of this Act provided:

(i) The broker or insurer does not disclose nonpublic personal information of a consumer to nonaffiliated third parties for any purpose, including joint servicing or marketing under Section 22 of this Act, except as permitted by Section 23 or 24 of this Act; and

(ii) The broker or insurer delivers a notice to the consumer at the time a

© 2026 National Association of Insurance Commissioners

consumer relationship is established on which the following is printed in 16-point type:

NOTICE OF INFORMATION PRACTICES
"Neither the U.S. brokers that handled this insurance nor the insurers that have underwritten this insurance will disclose nonpublic personal information concerning the buyer to nonaffiliates of the brokers or insurers except as permitted by law."

Drafting Note: References to "excess lines broker" and "excess lines insurer" should be changed as necessary to correspond with the applicable terms used in each state.

O. (1) "Nonaffiliated third party" means any person except:

(a) A licensee's affiliate; or

(b) A person employed jointly by a licensee and any company that is not the licensee's affiliate (but nonaffiliated third party includes the other company that jointly employs the person).

(2) Nonaffiliated third party includes any company that is an affiliate solely by virtue of the direct or indirect ownership or control of the company by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

P. "Nonpublic personal health information" means any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of an individual;

(2) The provision of health care to an individual; or

(3) Payment for the provision of health care to an individual.

Q. "Nonpublic personal information" means any personally identifiable information that is linked or reasonably linkable to an identified natural person. Nonpublic personal information does not include de-identified data or publicly available information.

R. (1) "Personally identifiable information" means any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual~~:~~

~~(a) A consumer provides to a licensee to obtain an insurance product or service from the licensee;~~

~~(b) About a consumer resulting from a transaction involving an insurance product or~~

Commented [DB3]: The definition of PII should not depend on its source. A licensee could obtain PII about a consumer that is not in connection with providing an insurance product or service and should be subject to the provisions of the model law.

© 2026 National Association of Insurance Commissioners

~~service between a licensee and a consumer; or~~

~~(c) The licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.~~

(2) Examples.

(a) Information included. Personally identifiable- information includes:

(i) Information a consumer provides to a licensee on an application to obtain an insurance product or service;

(ii) Account balance information and payment history;

(iii) The fact that an individual is or has been one of the licensee's consumers or has obtained an insurance product or service from the licensee;

(iv) Any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer;

(v) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;

(vi) Any information the licensee collects through an Internet cookie (an information-collecting device from a web server); and

(vii) Information from a consumer report.

(b) Information not included. Personally identifiable information does not include:

~~(i) A list of names and addresses of customers of an entity that is not a financial institution; and~~

(ii) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.

S. "Opt in" means an affirmative direction by a consumer that authorizes a licensee to disclose the consumer's information.

T. "Opt out" means a direction by a consumer that the licensee may not disclose nonpublic personal information about the consumer to a nonaffiliated third party, except as permitted under Sections 22,23, or 24 .

Commented [DB4]: Move up before PII to present in alphabetical order.

U. (1) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

(a) Federal, state or local government records;

© 2026 National Association of Insurance Commissioners

(b) Widely distributed media; or

(c) Disclosures to the general public that are required to be made by federal, state or local law.

(2) Reasonable basis. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

(a) That the information is of the type that is available to the general public; and

(b) Whether an individual can direct that the information not be made available to the general public and, if so, that the licensee's consumer has not done so.

(3) Examples.

(a) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(b) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(c) Reasonable basis.

(i) A licensee has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(ii) A licensee has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the licensee has located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

V. "Reasonable opportunity" means any of the following:

(1) The licensee mails the notices required to the consumer and allows the consumer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within sixty (60) days from the date the licensee mailed the notices;

(2) Where a consumer agrees to receive the notices required by this Act electronically in accordance with UETA [insert state electronic transactions act statute], the licensee allows the consumer to opt out by any reasonable means at any time; or

© 2026 National Association of Insurance Commissioners

(3) For an isolated transaction, such as providing the consumer with an insurance quote, the licensee provides the notices required by this Act at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction.

X. "Sale" or "selling" means the exchange of nonpublic personal information for monetary or other valuable consideration. A licensee does not sell nonpublic personal information when:

(1) The disclosure is to a third party for the purpose of or in support of providing a product or service requested by the consumer.

(2) A licensee provides information to or receives anything of value from an insurance support organization, statistical agent, or reinsurer;

(3) A licensee provides nonpublic personal information to an affiliate or to a financial institution with which the licensee performs joint marketing;

(4) The business transfers to a third party the nonpublic personal information as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction in which the party assumes control of all or part of the licensee's assets; or

(5) A consumer uses or directs the business to (i) disclose nonpublic personal information; or (ii) interact with one or more third parties including but not limited to referrals to other licensees.

Y. "Sensitive Personal Information" means ~~personally identifiable~~ "nonpublic personal information" about a consumer that includes:

Commented [DB5]: The definition of NPI requires that it be PII

(1) Racial or ethnic origin, religious beliefs, sexual orientation, or citizenship or citizenship status; ~~or~~

(2) Genetic information or biometric data that may be processed for the purpose of uniquely identifying an individual; or~~.~~

~~(2)~~(3) Nonpublic personal information of a known child.

Z. (1) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests.

(2) "Targeted advertising" does not include:

(a) Online advertisements based on activities within a l~~L~~icensee's own websites or online applications;

(b) Online advertisements based on the context of a consumer's current search query, visit to a website, or online application;

© 2026 National Association of Insurance Commissioners

(c) Online advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(d) Processing nNonpublic ~~Personal~~ personal ~~Information~~ information solely for measuring or reporting advertising performance, reach, or frequency.

AA. "Third party service provider" ~~or "third party"~~ means a person or entity not otherwise defined as a licensee or affiliate of a licensee that:

Commented [DB6]: There are third parties who do not provide services to a licensee

(1) Provides services to the licensee; and

(2) Maintains, processes or otherwise is permitted access to nonpublic personal information through its provisions of services to the licensee.

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Section 5. Third-Party Service Provider Arrangements

A. Contract Requirements.

A licensee that discloses a consumer's nonpublic personal information to a third-party service provider shall enter into a written contract with the third-party service provider that:

(1) Prohibits the third-party service provider from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless processing is necessary to comply with the law or a valid and binding order of a governmental body, in which case the third-party service provider must notify the licensee within 48 hours unless prohibited by law;

(2) Requires the third-party service provider to delete, destroy, de-identify or return all nonpublic personal information to the licensee when requested by the licensee; or to delete nonpublic personal information after it is no longer necessary to fulfill a legal requirement or to meet the record retention requirements of the licensee or third-party service provider, and to notify the licensee of the action taken;

(3) Requires the third-party service provider to notify the licensee if it can no longer comply with its obligations under this contract and provides the licensee with a right to terminate the contract;

(4) Requires that any contract between a third-party service provider and a subcontractor with access to a consumer's nonpublic personal information must contain provisions no less protective of nonpublic personal information than those contained in the third-party service provider's agreement with the licensee;

(5) Requires the third-party service provider to provide assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act;

(6) Requires the third-party service provider to implement and maintain administrative, technical, and physical data security practices to protect the nonpublic personal information from unauthorized access, destruction, use, modification, or disclosure;

© 2026 National Association of Insurance Commissioners

(7) Requires the third-party service provider to notify the licensee of a failure to meet the obligations of Subsections (1) to (6) above within 48 hours of discovery by the third-party service provider.

B. A licensee that discloses a consumer's nonpublic personal information to a third-party service provider remains fully responsible for compliance with this Act and the handling of nonpublic personal information.

© 2026 National Association of Insurance Commissioners

Confidential

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

A. A consumer may file the following requests with a licensee, which shall be processed in accordance with the following standards:

(1) Within 45 days of receiving an authenticated request from a consumer for their nonpublic personal information, a licensee shall disclose:

(a) All nonpublic personal information about the consumer that is maintained by the licensee or any contracted third-party service provider; and

(b) A list of all third-party service providers to whom the licensee disclosed the consumer's nonpublic personal information.

(2) A licensee shall not be required to disclose the following:

(a) A consumer's Social Security Number, driver's license number or other government-issued identification number, financial account number(s), any health insurance or medical identification number, any account password(s), security questions and answers, unique biometric data or other information that could create a high risk of identity theft. The licensee may instead disclose the types of nonpublic personal information maintained by listing each type of nonpublic personal information it has about the consumer;

(b) Duplicative nonpublic personal information, if it is described in a manner reasonably understandable by the consumer and the consumer is offered an opportunity to review the nonpublic personal information for inconsistencies; or

(c) Information that is outside the scope of the request, if the consumer has requested only specified items or categories of information.

B. Correction of nonpublic personal information.

(1) A consumer may make an authenticated request for the correction of their nonpublic personal information by filing a request with the licensee that:

(a) Identifies the specific nonpublic personal information the consumer wishes to correct; and

(b) Provides an explanation of why the nonpublic personal information is incorrect.

(2) Within 45 days of receipt of the request under this subsection, a licensee shall take one of the following actions and notify the consumer:

(a) Correct the nonpublic personal information in dispute as requested by the consumer;

© 2026 National Association of Insurance Commissioners

(b) Delete the nonpublic personal information in dispute; or

(c) Deny the request and provide:

(i) The basis for refusal to correct the nonpublic personal information as requested;

(ii) Information about how the consumer may appeal the denial; and

(iii) An explanation of how the appeal will be reviewed and how the consumer will be notified of the decision on appeal.

(3) A licensee may deny a request for correction if:

(a) The nonpublic personal information is accurate and complete and if the licensee provides a process for appeal of the decision; or

(b) The nonpublic personal information that is the subject of the request was not created by the licensee, unless there is a reasonable basis to believe that the originator of the nonpublic personal information is no longer available to act on the requested correction, and the consumer has independently demonstrated the information is incorrect.

C. Deletion of nonpublic personal information.

(1) Within 45 days of an authenticated request from a consumer, a licensee shall delete the nonpublic personal information about the consumer that is maintained by the licensee or direct a third-party service provider to delete the nonpublic personal information on the licensee's behalf.

(2) The licensee is not required to delete nonpublic personal information if:

(a) The licensee is required by law or regulation to retain the nonpublic personal information;

(b) The nonpublic personal information may be necessary to perform the contract or service requested by or benefiting the consumer;

(c) The information is necessary to comply with a legal obligation; or

(d) The information is maintained in reasonable anticipation of a claim or civil or criminal proceeding.

(3) A licensee may delay fulfilling a consumer's request, up to 45 days, to delete nonpublic personal information stored on an archived or backup system. A licensee must notify the consumer of such delay.

D. Request and Response Procedures

© 2026 National Association of Insurance Commissioners

(1) Except as provided in Subsection D(1)(b), a licensee shall respond to requests submitted under this section within 45 days in the following manner:

(a) A licensee may use its secure communications portal to authenticate requests from consumers holding current accounts with the licensee, unless the licensee has reason to believe the request has been submitted through an account that has been compromised. Otherwise, the licensee may use methods that are commercially reasonable, but not unduly burdensome, to authenticate the identity of the person making the request and to verify that this person is either:

(i) The consumer;

(ii) A person acting with the consumer's written authorization, including but not limited to a valid power of attorney;

(iii) The parent or legal guardian of a consumer who is a minor, except where the information relates to health insurance claims in circumstances where the child has a legal right to obtain the services in question without the parent's or guardian's consent;

(iv) The legal guardian or other person authorized by law to act on behalf of an incapacitated consumer; or

(v) The personal representative or other person authorized by law to act on behalf of a deceased consumer.

(b) A licensee is required to notify the consumer if either of the following prevents the licensee from complying with the request:

(i) The specific nonpublic personal information at issue is not locatable or retrievable by the licensee; or

Drafting Note: Examiners should review licensees' notifications to consumers regarding nonpublic personal information that is not locatable or retrievable by the licensee and its justifications for irretrievability during Market Conduct and/or IT Exams.

(ii) The licensee is unable to verify the request after requesting that the consumer provide additional information necessary to authenticate the identity of the consumer and authenticate the consumer's request.

(c) If a licensee declines the consumer's request, the licensee shall inform the consumer of the basis for declining the request and provide instructions for how to request review of the decision.

(2) There shall be no cap on the number of requests to correct or delete nonpublic personal information.

(3) If a consumer disagrees with a licensee's refusal to correct or delete nonpublic personal information per the consumer's request, the consumer shall be permitted to file with the licensee:

© 2026 National Association of Insurance Commissioners

(a) A concise statement setting forth why the consumer disagrees with the licensee's refusal and what the consumer thinks is the correct, relevant or fair information; and

(b) The licensee shall maintain the statement with the disputed nonpublic personal information and allow anyone reviewing the disputed nonpublic personal information to be made aware of the dispute and have access to the consumer's statement.

© 2026 National Association of Insurance Commissioners

Confidential

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7. Initial and Subsequent Delivery Notice of Information Practices to Consumers Required

A. Initial Delivery of Notice. A licensee shall provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to all consumers no later than when the licensee obtains access to the consumer's nonpublic personal information, except that a licensee may provide the initial notice within a reasonable time after access to the consumer's nonpublic personal information if:

(1) Obtaining access to the consumer's nonpublic personal information is not at the consumer's election and the licensee follows the Notice of Information Practices previously sent to the consumer; or

(2) Providing notice when the licensee obtains access to the consumer's nonpublic personal information would substantially delay the consumer's transaction and the consumer agrees to receive the notice at a later time.

B. Subsequent Delivery of Notice

When a consumer with an existing relationship with a licensee obtains a new insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, the licensee satisfies the initial notice requirements of Subsection A of this section as follows:

(1) The licensee may provide a revised notice, under Section 13 , that covers the consumer's new insurance product or service; or

(2) If the initial, revised or annual notice that the licensee most recently provided to that consumer was accurate with respect to the new insurance product or service, the licensee does not need to provide a new notice of information practices under Subsection A of this section.

C. For purposes of this section:

(1) "Not at consumer's election" includes the scenario where a licensee acquires or is assigned a consumer's policy from another financial institution or residual market mechanism and the consumer does not have a choice about the licensee's acquisition or assignment.

(2) "Substantially delay the consumer's transaction" includes the scenario where the licensee and the individual agree over the telephone or electronically to enter into a

© 2026 National Association of Insurance Commissioners

(3) consumer relationship involving prompt delivery of the insurance product or service but does not include the scenario where the relationship is initiated in person at the licensee's office or through other means by which the consumer may view the notice, such as on a website.

Section 8. Annual Notice of Information Practices to Consumers Required

General rule. A licensee shall provide a clear and conspicuous notice to consumers that accurately reflects its privacy policies and practices at least once in any period of twelve (12) consecutive months. A licensee may define the twelve-consecutive-month period, but the licensee shall apply it to the consumer on a consistent basis.

A. Example. A licensee provides a notice annually if it defines the twelve-consecutive-month period as a calendar year and provides the annual notice to the consumer once in each calendar year following the calendar year in which the licensee provided the initial notice. For example, if a consumer opens an account on any day of year 1, the licensee shall provide an annual notice to that consumer by December 31 of year 2.

(1) Exceptions.

(1) A licensee that provides nonpublic personal information to nonaffiliated third parties only in accordance with Sections 22, 23, or 24 and has not changed its policies and practices with regard to disclosing Nonpublic Personal Information from the policies and practices that were disclosed in the most recent disclosure sent to consumers in accordance with this section or Section 7 shall not be required to provide an annual disclosure under this section until such time as the licensee fails to comply with any criteria described in this paragraph.

(2) A licensee is not required to provide notice if the licensee no longer has access to the consumer's nonpublic personal information.

(2) For the purposes of this Act, a licensee no longer has an obligation to continue to notify a consumer if the licensee's records do not contain a valid address. An address is deemed invalid if electronic or regular mail sent to that address by the licensee has been returned as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.

Section 9. Information to be Included in Notices of Information Practices

A. General rule. The initial, annual and revised Notice of Information Practices that a licensee provides under Sections 7,8, and 13 shall include each of the following items of information, in addition to any other information the licensee wishes to provide, that applies to the licensee and to the consumers to whom the licensee sends its Notice of Information Practices:

(1) The categories of nonpublic personal information that the licensee collects, including, but not limited to, whether information is collected from the consumer, through the consumer's transactions with affiliates or nonaffiliated third parties, or consumer reporting agencies;

© 2026 National Association of Insurance Commissioners

(2) The categories of nonpublic personal information that the licensee discloses, including at least one example in each category. Categories may include, but are not limited to, application information, transaction information, or consumer reports;

(3) The categories of affiliates and nonaffiliated third parties, and the types of business in which they engage, to whom the licensee discloses nonpublic personal information, other than those parties to whom the licensee discloses information under Sections 22, 23, and 24. The types of businesses may be described in general terms only if the licensee uses illustrative examples of each significant line of business;

(4) An explanation of the consumer's right under Section 12 to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;

(5) An explanation of the consumer's rights with regard to the sale of nonpublic personal information and disclosure of sensitive personal information pursuant to Sections 20 and 21;

(6) A description of the consumer's options to request access, correction, or deletion of nonpublic personal information about the consumer as established under this Act and the instructions for exercising such options;

(7) Any disclosures that the licensee makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);

(8) The licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; by

(a) Describing in general terms who is authorized to have access to the information; and

(b) Stating whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance with the licensee's policy. The licensee is not required to describe technical information about the safeguards it uses; and

(c) Any disclosure that the licensee makes as authorized under Section 22, 23, or 24, except that the licensee is not required to list those exceptions in the initial or annual Notice of Information Practices required by Sections 7 and 8. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.

B. The licensee's notice may include:

(1) Categories of nonpublic personal information that the licensee reserves the right to disclose in the future, but does not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the

© 2026 National Association of Insurance Commissioners

right in the future to disclose, but to whom the licensee does not currently disclose, nonpublic personal information.

C. Exceptions:

If a licensee does not disclose, and does not reserve the right to disclose, nonpublic personal information about consumers to affiliates or nonaffiliated third parties except as authorized under Sections22, 23, or 24, the licensee shall state that in its notice, in addition to the information it shall provide under Subsections A(1) and A(8) and Subsection B of this section.

D. Sample Clauses and Federal Model Privacy Form.

(1) Licensees are not required to use any prescribed clauses or model form.

(2) The commissioner may determine that a Licensee's use of any of the following constitutes compliance with this Act:

(a) Sample clauses illustrating some of the notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner;

(b) Model forms illustrating notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner; or

(c) The Federal Model Privacy Forms are included in Appendix A and Appendix B, of this Act.

Section 10. Short Form Initial Notice of Information Practices

A. A licensee may satisfy the initial notice requirements in Sections 7A and 13A by providing a Short Form Initial Notice of Information Practices at the same time the licensee delivers an opt-out notice as required in Section 12 if:

(1) The licensee provides the consumer a reasonable means to obtain its Notice of Information Practices; and

(2) The licensee provides the Notice of Information Practices upon request.

B. A Short Form Initial Notice of Information Practices shall meet all of the following requirements.

(1) Be clear and conspicuous;

(2) State that the licensee's Notice of Information Practices is available upon request;

(3) Explain the reasonable means to obtain the licensee's Notice of Information Practices;

(4) Contain contact information for the commissioner; and

(5) Describe how the consumer can request access to or correction of their nonpublic personal information.

© 2026 National Association of Insurance Commissioners

C. For purposes of this section "reasonable means to obtain the licensee's Notice of Information Practices" includes:

(1) Providing a toll-free telephone number that the consumer may call to request the notice;

(2) Providing a website or other electronic medium that is easily accessible by the consumer; or

(3) Maintaining copies of the notice at the licensee's place of business to be provided upon request.

Section 11. Form of Opt-In Notice to Consumers and Opt-In Methods

A. If a licensee is required to provide an opt-in~~t~~ notice under Sections 20 or 21, it shall provide a clear and conspicuous notice to each of its consumers that accurately explains the information proposed to be disclosed, the use of that information, and the consumer's option to opt in to that use. The notice shall state:

(1) The licensee discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;

(2) The consumer has the option to opt in to that disclosure; and

(3) A reasonable means by which the consumer may exercise the option to opt in.

B. The licensee shall not disclose that information to a nonaffiliated third party unless the consumer has affirmatively opted in to the use.

C. The opt-in must be an affirmative act by the consumer. The licensee cannot deem a failure to respond as an opt-in or use pre-checked boxes.

D. The opt-in should be obtained separately from any other communication or consent.

E. The opt-in may be revoked at any time by the consumer.

Section 12. Form of Opt-Out Notice to Consumers and Opt-Out Methods

A. (1) If a licensee is required to provide an opt-out notice, it shall provide a clear and conspicuous notice to each consumer that accurately explains the right to opt out under that section. To the extent applicable, the notice shall state:

(a) That the licensee discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;

(b) That the consumer has the right to opt out of that disclosure; and

(c) A reasonable means by which the consumer may exercise the opt-out right.

(2) Requirements

© 2026 National Association of Insurance Commissioners

(a) A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if the licensee:

(i) Identifies all of the categories of nonpublic personal information it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to whom the licensee discloses the information, as described in Section 9A(2) and (3), and states the consumer can opt out of the disclosure of that information; and

(ii) Identifies the insurance products or services the consumer obtains from the licensee, either singly or jointly, to which the opt-out would apply.

(b) A licensee provides a reasonable means to exercise an opt-out right if it:

(i) Designates check-off boxes in a prominent position on the relevant forms with the opt-out notice;

(ii) Includes a reply form together with the opt-out notice;

(iii) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the licensee's website, if the consumer agrees to the electronic delivery of information; or

(iv) Provides a toll-free telephone number that consumers may call to opt out.

(c) A licensee does not provide a reasonable means of opting out if:

(i) The only means of opting out is for the consumer to write a letter to the licensee to exercise their opt-out right; or

(ii) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the licensee provided with the initial notice but did not include with the subsequent notice.

(d) A licensee may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

B. A licensee may provide the opt-out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 7.

C. If a licensee provides the opt-out notice after it provides the initial notice, the licensee shall include a copy of the initial notice with the opt-out notice in writing or, if the consumer agrees, electronically.

D. Joint relationships.

(1) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt-out notice. The licensee's opt-out notice shall explain how the licensee will treat an opt-out direction by a joint consumer (as explained in Paragraph (2) of this subsection).

© 2026 National Association of Insurance Commissioners

(2) Any of the joint consumers may exercise the right to opt out. The licensee may either:

(a) Treat an opt-out direction by a joint consumer as applying to all of the associated joint consumers; or

(b) Permit each joint consumer to opt out separately.

(3) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all the joint consumers.

(4) A licensee may not require all joint consumers to opt out before it implements any opt-out direction.

E. A licensee shall comply with a consumer's opt-out direction as soon as reasonably practicable but no later than 10 days after the licensee receives it.

F. A consumer may exercise the right to opt out at any time. A consumer's direction to opt-out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.

Section 13. Revised Notice of Information Practices

A. Except as otherwise authorized in this Act, a licensee shall not, directly or through an affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that the licensee provided to that consumer under Section 7, unless:

(1) The licensee has provided to the consumer a clear and conspicuous revised notice that accurately describes its policies and practices;

(2) The licensee has provided to the consumer a new opt-out notice;

(3) The licensee has given the consumer a reasonable opportunity, before the licensee discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(4) The consumer does not opt out.

B. Examples.

(1) Except as otherwise permitted by Sections 19, 20 and 21, a licensee shall provide a revised notice before it:

(a) Discloses a new category of nonpublic personal information to any nonaffiliated third party; or

(b) Discloses nonpublic personal information to a new category of nonaffiliated third party.

(2) A revised notice is not required if the licensee discloses nonpublic personal information to a new nonaffiliated third party that the licensee adequately described in its prior notice.

© 2026 National Association of Insurance Commissioners

Section 14. Notice of Information Practices to Group Policyholders

Unless a licensee is providing notices of information practices directly to covered individuals described in Section 4G)2)(e)(i), (ii) or (iii), a licensee shall provide initial, annual and revised notices to the plan sponsor, group or blanket insurance policyholder or group annuity contract holder, or workers' compensation policyholder, in the manner described in Sections 7 through 13 of this Act, describing the licensee's privacy practices with respect to nonpublic personal information about individuals covered under the policies, contracts or plans. Compliance with this section satisfies the licensees initial, annual and renewal Notice of Information Practices as required by Sections 7 and 8 and delivery provisions of Section 15.

Section 15. Delivery

A. A licensee shall provide any notices that this Act requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer interacts with the licensee online or in some other electronic fashion, electronically.

B. (1) A licensee may reasonably expect that a consumer will receive actual notice if the licensee:

(a) Hand-delivers a printed copy of the notice to the consumer;

(b) Mails a printed copy of the notice to the last known address of the consumer separately, or in a policy, billing or other written communication;

(c) For a consumer who conducts transactions electronically, in accordance with UETA (insert state electronic transactions act statute), posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service;

(i) The notice should be posted in a manner that enables a consumer to print or save it using programs or apps that are widely available and free of charge.

(ii) Notice is available electronically as long as it is in force.

(d) For an isolated transaction with a consumer, such as the licensee providing an insurance quote or selling the consumer travel insurance, posts the notice and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular insurance product or service.

(e) Provides the notice by any other means authorized by the commissioner.

(2) Examples of unreasonable expectation of actual notice. A licensee may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:

(a) Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or

(b) Sends the notice via electronic mail to a consumer who does not otherwise

© 2026 National Association of Insurance Commissioners

communicate with the licensee electronically.

C. A licensee may reasonably expect that a consumer will receive actual notice of the licensee's Notice of Information Practices if:

(1) The consumer uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or

(2) The consumer has requested that the licensee refrain from sending any information regarding the consumer relationship, and the licensee's current privacy notice remains available to the consumer upon request.

D. A licensee may not provide any notice required by this Act solely by orally explaining the notice, either in person or over the telephone.

E. A licensee may provide a joint notice from the licensee and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the licensee and the other institutions. A licensee also may provide a notice on behalf of another financial institution.

F. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of Sections 7A, 8A and 13A, respectively, by providing one notice to those consumers jointly.

© 2026 National Association of Insurance Commissioners

ARTICLE V. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 16. General Rules for Use and Disclosure of Nonpublic Personal Information

A. Use and Disclosure

(1) A licensee may use and disclose nonpublic personal information about a consumer for purposes of processing a business transaction requested or authorized by the consumer.

(2) A licensee may disclose nonpublic personal information with affiliates, provided the affiliates' use and disclosure comply with this Act.

(3) A licensee shall not disclose nonpublic personal information to a nonaffiliated third party except as permitted by this Act.

(4) This section applies to nonpublic personal information collected before and after a consumer exercises an opt-out right under Section 19 or an opt-in right under Sections 20 and 21.(5) If a consumer submits an opt-out request during a transaction and the requested information is necessary to complete that transaction, the licensee shall:

(a) Inform the consumer that the transaction cannot be completed without the information; and

(b) Confirm whether the consumer wishes to proceed.

B. Limits on Disclosure. Except as provided by Section 16A(1), before disclosing a consumer's nonpublic personal information to a nonaffiliated third party, whether directly or through an affiliate, a licensee shall:

(1) Provide the initial notice required by Section 7;

(2) Provide a clear and conspicuous notice to the consumer that details:

(a) The consumer's right to opt out of disclosure for targeted advertising under Section 19;

(b) The consumer's option to opt in to the sale of nonpublic personal information under Section 20; or

(c) The consumer's option to opt in to the disclosure of sensitive personal information Section 21.

(3) Provide a reasonable opportunity for the consumer to exercise any applicable opt-out right before disclosure; and

(4) Obtain and document the consumer's opt-in or opt-out election, as applicable.

Section 17. Limits on Redisclosure and Reuse of Nonpublic Personal Information

A. If a licensee receives nonpublic personal information from a nonaffiliated third-party service provider under an exception in Article VI of this Act,

© 2026 National Association of Insurance Commissioners

the licensee may use and disclose the information in the ordinary course of business to carry out the activity covered by the exception under which the licensee received the information.

B. (1) If a licensee receives nonpublic personal information from a nonaffiliated third-party service provider other than under an exception in Article VI of this Act, the licensee may disclose the information only to the following, provided the disclosure is consistent with this Act:

(a) Affiliates of the third party-service provider from which the licensee received the information; and

(b) Affiliates of the licensee who may disclose the information only to the extent that the disclosure would be permissible by the licensee pursuant to this Act.

(2) Example. If a licensee obtains a customer list from a nonaffiliated third-party service provider outside of the exceptions in Article VI:

(a) The licensee may use that list for its own purposes consistent with this Act; and

(b) The licensee may disclose that list to another nonaffiliated third-party service provider only as permitted by this Act.

C. If a licensee discloses nonpublic personal information to a nonaffiliated third-party service provider under an exception in S Article VI of this Act, the third party-service provider:

(1) May disclose the information to the licensee's affiliates; and

(2) May disclose and use the information in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

D. If a licensee discloses nonpublic personal information to a nonaffiliated third-party service provider other than under an exception in Article VI of this Act, the third-party service provider may disclose the information only:

(1) To the licensee's affiliates who may disclose the information only to the extent that it would be permissible for the licensee to disclose the information pursuant to this Act: and

(2) To any other person, if the disclosure would be lawful if the licensee made it directly to that person.

Section 18. Limits on Sharing Access Number or Access Code Information for Marketing Purposes

A. A licensee shall not, directly or through an affiliate, disclose, other than to a consumer reporting agency, a policy number or similar form of access number or access code for a consumer's policy or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

B. Exceptions. Subsection A of this section does not apply if a licensee discloses a policy number or similar form of access number or access code:

© 2026 National Association of Insurance Commissioners

(1) To the licensee's service provider solely in order to perform marketing for the licensee's own products or services, as long as the service provider is not authorized to directly initiate charges to the account;

(2) To a licensee who is a producer solely in order to perform marketing for the licensee's own products or services; or

(3) To a participant in an affinity or similar program where the participants in the program are identified to the consumer when the consumer enters into the program.

(4) Where the policy number, or similar form of access number or access code, is in an encrypted form, as long as the licensee does not provide a means to decode the access number or access code.

Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted ~~Marketing~~ Advertising

A. Except as otherwise authorized in this Act, a licensee may not, directly or through any affiliate, disclose for the purpose of targeted advertising any nonpublic personal information about a consumer to a nonaffiliated third party unless the consumer has been provided clear and conspicuous notice and a reasonable opportunity to opt out of targeted advertising in accordance with the requirements of Section 12 of this Act.

B. A licensee shall act on a consumer's request to opt out within 15 days of receipt.

C. A licensee is under no obligation to obtain additional information to execute the opt-out request.

D. A licensee may not solicit the consumer to change their election to opt out for twelve months.

E. A consumer has the right to opt out at any time.

Section 20. Limits on Sale of Nonpublic Personal Information

Before a licensee may sell nonpublic personal information:

A. The licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

B. The consumer must affirmatively opt in to the sale of their nonpublic personal information.

Section 21. Limits on Disclosure of Sensitive Personal Information

A. Except as provided by Subsection B below, a licensee may disclose a consumer's sensitive personal information only for those purposes and uses identified in Article VI and as expressly permitted or required by Article VI or other provisions of this Act.

B. Before a licensee may disclose a consumer's sensitive personal information for purposes other than those specified in subsection A of this section:

(1) A licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

© 2026 National Association of Insurance Commissioners

(2) The consumer must affirmatively opt in to disclosure of their sensitive personal information.

© 2026 National Association of Insurance Commissioners

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 22. Exception to Opt-Out Requirements for Disclosure of Nonpublic Personal Information for Service Providers and Joint Marketing

A. General rule.

(1) The opt-out requirements in Sections 12 and 19 do not apply when a licensee provides nonpublic personal information to a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf, if the licensee:

(a) Provides the initial notice in accordance with Section7; and

(b) Enters into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in Sections 23 or 24 in the ordinary course of business to carry out those purposes.

(2) Example. If a licensee discloses nonpublic personal information under this section to a financial institution with which the licensee performs joint marketing, the licensee's contractual agreement with that institution meets the requirements of Paragraph (1)(b) of this subsection if it prohibits the institution from disclosing or using the nonpublic personal information except as necessary to carry out the joint marketing or under an exception in Sections 23 or 24 in the ordinary course of business to carry out that joint marketing.

B. Service may include joint marketing. The services a nonaffiliated third party performs for a licensee under Subsection A of this section may include marketing of the licensee's own products or services or marketing of financial products or services offered pursuant to joint agreements between the licensee and one or more financial institutions.

C. Definition of "joint agreement." For purposes of this section, "joint agreement" means a written contract pursuant to which a licensee and one or more financial institutions jointly offer, endorse or sponsor a financial product or service.

Section 23. Exceptions to Notice and Opt-Out Requirements for Disclosure of Nonpublic Personal Information for Processing and Servicing Transactions

A. Exceptions for processing transactions at consumer's request. The requirements for initial notice in Section 7A(2), the opt-out in Sections 12 and 19, and service providers and joint marketing in Section 22 do not apply if the licensee discloses nonpublic personal information as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Servicing or processing an insurance product or service that a consumer requests or authorizes;

© 2026 National Association of Insurance Commissioners

(2) Maintaining or servicing the consumer's account with a licensee, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity;

(3) A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer; or

(4) Reinsurance or stop loss or excess loss insurance.

B. "Necessary to effect, administer or enforce a transaction" means that the disclosure is:

(1) Required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or

(2) Required, or is a usual, appropriate or acceptable method:

(a) To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer's account in the ordinary course of providing the insurance product or service;

(b) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

(c) To provide a confirmation, statement or other record of the transaction, or information on the status or value of the insurance product or service to the consumer or the consumer's agent or broker;

(d) To accrue or recognize incentives or bonuses associated with the transaction that are provided by a licensee or any other party;

(e) To underwrite insurance at the consumer's request or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects or as otherwise required or specifically permitted by federal or state law; or

(f) In connection with:

(i) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited or otherwise paid using a debit, credit or other payment card, check or account number, or by other payment means;

(ii) The transfer of receivables, accounts or interests therein; or

(iii) The audit of debit, credit or other payment information.

© 2026 National Association of Insurance Commissioners

Section 24. Other Exceptions to Notice and Opt-Out Requirements for Disclosure of Nonpublic Personal Information

A. Exceptions to opt out requirements. The requirements for initial notice to consumers in Section 7A(2), the opt-out in Sections 12 and 19, and service providers and joint marketing in Section 22 do not apply when a licensee discloses nonpublic personal information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

(2) (a) To protect the confidentiality or security of a licensee's records pertaining to the consumer, service, product or transaction;

(b) To protect against or prevent actual or potential fraud or unauthorized transactions;

(c) For required institutional risk control or for resolving consumer disputes or inquiries;

(d) To persons holding a legal or beneficial interest relating to the consumer; or

(e) To persons acting in a fiduciary or representative capacity on behalf of the consumer;

(f) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted nonpublic personal information.

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating a licensee, persons that are assessing the licensee's compliance with industry standards, and the licensee's attorneys, accountants and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the federal Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, the Securities and Exchange Commission, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance authority, and the Federal Trade Commission), self-regulatory organizations or for an investigation on a matter related to public safety;

(5) (a) To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or

(b) From a consumer report reported by a consumer reporting agency;

© 2026 National Association of Insurance Commissioners

(6) In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of the business or unit;

(7) (a) To comply with federal, state or local laws, rules and other applicable legal requirements;

(b) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities; or

(c) To respond to judicial process or government regulatory authorities having jurisdiction over a licensee for examination, compliance or other purposes as authorized by law; or

(8) For purposes related to the replacement of a group benefit plan, a group health plan, a group welfare plan or a workers' compensation plan.

B. Example of revocation of consent. A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under Section 12F.

Drafting Note: Because the notice requirements of this Act could be a financial burden on a company in liquidation or receivership and negatively impact the ability of the liquidator or receiver to pay claims, regulators may want to consider adding an additional exception providing that licensees in liquidation or receivership are not subject to the notice provisions of this Act.

© 2026 National Association of Insurance Commissioners

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 25. When Authorization Required for Disclosure of Nonpublic Personal Health Information

A. A licensee shall not disclose nonpublic personal health information about a consumer unless an authorization is obtained from the consumer whose nonpublic personal health information is sought to be disclosed.

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee:

(1) Claims administration any processing;

(2) Claims adjustment and management;

(3) Detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity;

(4) Underwriting;

(5) Policy placement or issuance;

(6) Loss control;

(7) Ratemaking and guaranty fund functions;

(8) Reinsurance and excess loss insurance;

(9) Risk management;

(10) Case management;

(11) Disease management;

(12) Quality assurance;

(13) Quality improvement;

(14) Performance evaluation;

(15) Provider credentialing verification;

(16) Utilization review;

(17) Peer review activities;

(18) Actuarial, scientific, medical or public policy research;

(19) Grievance procedures;

© 2026 National Association of Insurance Commissioners

(20) Internal administration of compliance, managerial, and information systems;

(21) Policyholder service functions;

(22) Auditing;

(23) Reporting;

(24) Database security;

(25) Administration of consumer disputes and inquiries;

(26) External accreditation standards;

(27) The replacement of a group benefit plan or workers' compensation policy or program;

(28) Activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit;

(29) Any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services or other applicable laws;

(30) Disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes including subrogation, and

(31) Any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with the legal process.

C. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable

Section 26. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article VII shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer who is the subject of the nonpublic personal health information;

(2) A general description of the types of nonpublic personal health information to be disclosed;

(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

© 2026 National Association of Insurance Commissioners

(4) The signature, including electronic signatures, of the consumer who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer may revoke the authorization at any time and the procedure for making a revocation.

(6) Any additional information necessary to comply with HIPAA or any other applicable law.

B. An authorization for the purposes of this Article VII shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article VII at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

E. A signed copy of the authorization shall be provided to the consumer.

Section 27. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer as part of an opt-out notice pursuant to Section 12, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section 25A.

Section 28. Relationship to Federal Rules

A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

This Act shall not apply to nonprofits, such as the National Association of Insurance Commissioners or the National Insurance Crime Bureau, when processing or sharing information solely for investigating criminal or fraudulent insurance acts.

Section 29. Relationship to State Laws

Nothing in this Article shall preempt or supersede existing state law related to medical records, consumer data privacy, health or insurance information privacy.

© 2026 National Association of Insurance Commissioners

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 30. Protection of Fair Credit Reporting Act

Nothing in this Act shall be construed to modify, limit or supersede the operation of the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and no inference shall be made regarding whether information is transaction or experience information under Section 603 of that Act.

Section 31. Nondiscrimination

A. A licensee shall not unfairly discriminate against any consumer because that consumer has opted out from the disclosure of his or her nonpublic personal information pursuant to the provisions of this Act.

B. A licensee shall not unfairly discriminate against a consumer because that consumer has not granted authorization for the disclosure of his or her nonpublic personal health information pursuant to the provisions of this Act.

Section 32. Violation

Drafting Note: Cite state unfair trade practices act or other applicable state law.

Section 33. Severability

If any section or portion of a section of this Act or its applicability to any person or circumstance is held invalid by a court, the remainder of the Act or the applicability of the provision to other persons or circumstances shall not be affected.

Section 34. Individual Remedies

This Act may not be construed to create or imply a private cause of action for violation of its provisions, nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Section 35. Effective Date

A. Effective date. This Acthas been effective since November 13, 2000. The amendments to this Act are effective [Insert Effective Date]. In order to provide sufficient time for licensees to establish policies and systems to comply with the amendments to this Act, the commissioner has extended the time for compliance with the amendments to this Act until [Insert Compliance Date].

B. By [Insert Compliance Date], a licensee shall provide an initial notice, as required by Section 7, to any existing consumer who has not previously received a notice that complies with the amendments to this Act.

C. Two-year grandfathering of service agreements. Until [Insert Compliance Date], a contract that a licensee has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf satisfies the provisions of Section 22A(1)(b) of this Act, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the licensee entered into the agreement on or before

© 2026 National Association of Insurance Commissioners

[Insert Compliance Date].

© 2026 National Association of Insurance Commissioners

Confidential

APPENDIX A – SAMPLE CLAUSES

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A-1–Categories of information a licensee collects (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(1) to describe the categories of nonpublic personal information the licensee collects.

Sample Clause A-1:

We collect nonpublic personal information about you from the following sources:

Information we receive from you on applications or other forms;
Information about your transactions with us, our affiliates or others; and
Information we receive from a consumer reporting agency.

A-2–Categories of information a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use one of these clauses, as applicable, to meet the requirement of Section 9A(2) to describe the categories of nonpublic personal information the licensee discloses. The licensee may use these clauses if it discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-2, Alternative 1:

We may disclose the following kinds of nonpublic personal information about you:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premiums, and payment history"]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your creditworthiness and credit history"].

Sample Clause A-2, Alternative 2:

We may disclose all of the information that we collect, as described [describe location in the notice, such as "above" or "below"].

A-3–Categories of information a licensee discloses and parties to whom the licensee discloses (institutions that do not disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirements of Sections 9A(2) and (3) to describe the

© 2026 National Association of Insurance Commissioners

categories of nonpublic personal information the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses. A licensee may use this clause if the licensee does not disclose nonpublic personal information to any party, other than as permitted by the exceptions in Sections 23 and 24.

Sample Clause A-3:

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

A-4–Categories of parties to whom a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(3) to describe the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information. This clause may be used if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-4:

We may disclose nonpublic personal information about you to the following types of third parties:

Financial service providers, such as [provide illustrative examples, such as "life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents"];

Non-financial companies, such as [provide illustrative examples, such as "retailers, direct marketers, airlines, and publishers"]; and

Others, such as [provide illustrative examples, such as "non-profit organizations"].

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

A-5–Service provider/joint marketing exception
A licensee may use one of these clauses, as applicable, to meet the requirements of Section 9A(2) related to the exception for service providers and joint marketers in Section 22. If a licensee discloses nonpublic personal information under this exception, the licensee shall describe the categories of nonpublic personal information the licensee discloses and the categories of third parties with which the licensee has contracted.

Sample Clause A-5, Alternative 1:

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premium, and payment history"]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your

© 2026 National Association of Insurance Commissioners

creditworthiness and credit history"].

Sample Clause A-5, Alternative 2:

We may disclose all of the information we collect, as described [describe location in the notice, such as "above" or "below"] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

A-6–Explanation of opt- out right (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(4) to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. The licensee may use this clause if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-6:

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [describe a reasonable means of opting out, such as "call the following toll-free number: (insert number)].

A-7–Confidentiality and security (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(8) to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A-7:

We restrict access to nonpublic personal information about you to [provide an appropriate description, such as "those employees who need to know that information to provide products or services to you"]. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

© 2026 National Association of Insurance Commissioners

APPENDIX B – FEDERAL MODEL PRIVACY FORM

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the Federal Model Privacy Form, if the Form is accurate for each institution that uses the Form. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A. General Instructions

1. How the Model Privacy Form is used.

(a) The Model Form may be used, at the option of a "licensee", including a group of licensees or other financial institutions that use a common privacy notice, to meet the content requirements of the privacy notice and opt-out notice set forth in [insert citation for sections of statute or regulation sections that parallel Sections 9and 11 of the NAIC *Privacy of Consumer InformationAct*]

(b) The Model Form is a standardized form, including page layout, content, format, style, pagination, and shading. Licensees seeking to obtain the safe harbor through use of the Model Form may modify it only as described in these Instructions.

(c) Note that disclosure of certain information, such as assets, income, and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act (FCRA), codified at 15 U.S.C. §§ 1681-1681x, such as a requirement to permit a consumer to opt out of disclosures to affiliates, or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.

(d) The word "consumer" may be replaced by the word "member," whenever it appears in the Model Form, as appropriate.

2. The Contents of the Model Privacy Form

The Model Form consists of two pages, which may be printed on both sides of a single sheet of paper or may appear on two separate pages. Where a licensee provides a long list of licensees or financial institutions at the end of the Model Form in accordance with Instruction B3(a)(i), or provides additional information in accordance with Instruction B3(c) and such list or additional information exceeds the space available on Page Two of the Model Form, such list or additional information may extend to a third page.

(a) Page One. The first page consists of the following components:

(1) Date last revised (upper right-hand corner)
(2) Title
(3) Key frame (Why? What? How?)
(4) Disclosure table ("Reasons we can share your personal information")
(5) "To limit our sharing" box, as needed, for the licensee's opt-out information
(6) "Questions" box, for customer service contact information
(7) Mail-in opt-out form, as needed

(b) Page Two. The second page consists of the following components:

© 2026 National Association of Insurance Commissioners

(1) Heading (Page 2)
(2) Frequently Asked Questions ("Who we are" and "What we do")
(3) Definitions
(4) "Other important information" box, as needed

3. The format of the Model Privacy Form.

The format of the Model Form may be modified only as described below.

(a) Easily readable type font. Licensees that use the Model Form must use an easily readable type font. While a number of factors together produce easily readable font, licensees are required to use a minimum of 10-point font (unless otherwise expressly permitted in these Instructions) and sufficient spacing between lines.

(b) Logo. A licensee may include a corporate logo on any page of the notice, so long as it does not interfere with the readability of the Model Form or the space constraints of each page.

(c) Page size and orientation. Each page of the Model Form must be printed in portrait orientation, the size of which must be sufficient to meet the layout and minimum font size requirements, with sufficient white space on the top, bottom, and sides of the content.

(d) Color. The Model Form must be printed on white or light color paper (such as cream) with black or other contrasting ink color. Spot color may be used to achieve visual interest, so long as the color contrast is distinctive and the color does not detract from the readability of the Model Form. Logos may also be printed in color.

(e) Languages. The Model Form may be translated into languages other than English.

B. Information Required in the Model Privacy Form

The information in the Model Form may be modified only as described below:

1. Name of licensee or group of affiliated licensees or institutions providing the notice
Insert the name of the licensee providing the notice, or a common identity of the affiliated licensees or financial institutions jointly providing the notice on the form, wherever [name of licensee] appears.

2. Page One

(a) Last revised date. The licensee must insert in the upper right-hand corner the date on which the notice was last revised. The information shall appear in minimum 8-point font as "rev. [month/year]" using either the name or number of the month, such as "rev. July 2016" or "rev. 7/16."

(b) General instructions for the "What?" box

(i) The bulleted list identifies the types of personal information that the licensee collects and shares. All licensees must use the term "Social Security Number" in the first bullet.

(ii) A licensee must use five (5) of the following terms, to complete the bulleted list: income; account balances; payment history; transaction history; transaction or loss history; credit history; credit scores; assets; investment experience; credit-based insurance scores; insurance claim history; medical information; overdraft

© 2026 National Association of Insurance Commissioners

history; purchase history; account transactions; risk tolerance; medical-related debts; credit card or other debt; mortgage rates and payments; retirement assets; checking account information; employment information; wire transfer instructions.

(c) General instructions for the disclosure table. The left column lists reasons for sharing or using personal information. Each reason correlates to a specific legal provision described in Paragraph 2(d) of this Instruction. In the middle column, each licensee must provide a "Yes" or "No" response that accurately reflects its information-sharing policies and practices with respect to the reason listed on the left. In the right column, each licensee must provide in each box one of the following three (3) responses, as applicable, that reflects whether a consumer can limit such sharing:

"Yes," if it is required to or voluntarily provides an opt-out; "No," if it does not provide an opt-out; or

"We don't share," if it answers "No" in the middle column.

Only the sixth row ("For our affiliates to market to you") may be omitted at the option of the licensee. See Paragraph 2(d)(6) of this instruction.

(d) Specific disclosures and corresponding legal provisions

(i) For our everyday business purposes. This reason incorporates sharing information under [insert citation for sections of statute or regulation sections that parallel Sections 23 and 24 of NAIC model *Privacy of Consumer InformationAct*] and with service providers pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*] other than the disclosures described in Paragraphs (2)(d)(ii) or (2)(d)(iii) of this instruction.

(ii) For our marketing purposes. This reason incorporates sharing information with service providers by a licensee for its own marketing pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iii) For joint marketing with other financial companies. This reason incorporates sharing information under joint marketing agreements between 2 or more licensees or financial institutions and with any service provider used in conjunction with such agreement pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iv) For our affiliates' everyday business purposes – information about transactions and experiences. This reason incorporates sharing information specified in Sections 603(d)(2)(A)(i) and (ii) of the FCRA. A licensee that shares information for this reason may choose to provide an opt-out.

(v) For our affiliates' everyday business purposes – information about creditworthiness. This reason incorporates sharing information pursuant to Section 603(d)(2)(A)(iii) of the FCRA. A licensee that shares information for this reason must provide an opt-out.

(vi) For our affiliates to market to you. This reason incorporates sharing information specified in Section 624 of the FCRA. This reason may be omitted from the disclosure table when: the licensee does not have affiliates (or does not disclose personal information to its affiliates); the licensee's affiliates do not use personal information in a manner that requires an opt-out; or the licensee provides the affiliate marketing notice separately. Licensees that include this reason must provide an opt-out of indefinite duration. A licensee that is required to provide an

© 2026 National Association of Insurance Commissioners

Confidential

affiliate marketing opt-out, but does not include that opt-out in the Model Form under this part, must comply with Section 624 of the FCRA and [insert citation for statute or regulation that parallels NAIC *Privacy of Consumer Information Act*], with respect to the initial notice and opt-out and any subsequent renewal notice and opt-out. A licensee not required to provide an opt-out under this subparagraph may elect to include this reason in the Model Form.

(vii) For nonaffiliates to market to you. This reason incorporates sharing described in [insert citation for sections of statute or regulation sections that parallel Sections 11 and 16(B) of NAIC *Privacy of Consumer Information Act*]. A licensee that shares personal information for this reason must provide an opt-out.

(e) To limit our sharing. A licensee must include this section of the Model Form only if it provides an opt-out. The word "choice" may be written in either the singular or plural, as appropriate. Licensees must select one or more of the applicable opt-out methods described: telephone, such as by a toll-free number; a web site; or use of a mail-in opt-out form. Licensees may include the word "toll-free" before telephone, as appropriate. A licensee that allows consumers to opt out online must provide either a specific web address that takes consumers directly to the opt-out page or a general web address that provides a clear and conspicuous direct link to the opt-out page. The opt-out choices made available to the consumer who contacts the licensee through these methods must correspond accurately to the "Yes" responses in the third column of the disclosure table. In the part entitled "Please note," licensees may insert a number that is 30 days or greater in the space marked "[30]." Instructions on voluntary or state privacy law opt-out information are in Paragraph 2(g)(v) of these Instructions.

(f) Questions box. Customer service contact information must be inserted as appropriate where [phone number] or [web site] appear. Licensees may elect to provide either a phone number, such as a toll-free number, or a web address, or both. Licensees may include the words "toll-free" before the telephone number, as appropriate.

(g) Mail-in opt-out form. Licensees must include this mail-in form only if they state in the "To limit our sharing" box that consumers can opt out by mail. The mail-in form must provide opt-out options that correspond accurately to the "Yes" responses in the third column of the disclosure table. Licensees that require consumers to provide only name and address may omit the section identified as "[account #]." Licensees that require additional or different information, such as a random opt-out number or a truncated account number to implement an opt-out election should modify the "[account #]" reference accordingly. This includes licensees that require customers consumers with multiple accounts to identify each account to which the opt-out should apply. A licensee must enter its opt-out mailing address in the far right of this form (see version 3); or below the form (see version 4). The reverse side of the mail-in opt-out form must not include any content of the Model Form.

(i) Joint accountholder. Only licensees that provide their joint accountholders the choice to opt out for only one accountholder, in accordance with Paragraph 3(a)(5) of these Instructions, must include in the far left column of the mail-in form the following statement:

If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.

□ Apply my choice(s) only to me.

The word "choice" may be written in either the singular or plural, as appropriate. Licensees that provide insurance products or services, provide this option, and elect to use the Model Form may substitute the word "policy" for "account" in this statement. Licensees that do not provide this option may eliminate this left column from the mail-in form.

(ii) FCRA Section 603(d)(2)(A)(iii) opt-out. If the licensee shares personal information pursuant to Section

© 2026 National Association of Insurance Commissioners

603(d)(2)(A)(iii) of the FCRA, it must include in the mail-in opt-out form the following statement:

□ Do not share information about my creditworthiness with your affiliates for their everyday business purposes.

(iii) FCRA Section 624 opt-out. If the licensee uses Section 624 of the FCRA, in accord with paragraph 2(d)(6) of these Instructions, it must include in the mail-in opt-out form the following statement:

□ Do not allow your affiliates to use my personal information to market to me.

(iv) Nonaffiliate opt-out. If the licensee shares personal information pursuant to [insert citation for section of statute or regulation that parallels Section 16(B) of NAIC *Privacy of Consumer InformationAct*], it must include in the mail-in opt-out form the following statement:

□ Do not share my personal information with nonaffiliates to market their products and services to me.

(v) Additional opt-outs. Licensees that use the disclosure table to provide opt-out options beyond those required by Federal law must provide those opt-outs in this section of the Model Form. A licensee that chooses to offer an opt-out for its own marketing in the mail-in opt-out form must include one of the two following statements:

□ Do not share my personal information to market to me. or

□ Do not use my personal information to market to me.

A licensee that chooses to offer an opt-out for joint marketing must include the following statement:

□ Do not share my personal information with other financial institutions to jointly market to me.

(h) Barcodes. A licensee may elect to include a barcode and/or "tagline" (an internal identifier) in 6-point type at the bottom of page one, as needed for information internal to the licensee, so long as these do not interfere with the clarity or text of the form.

3. Page Two

(a) General Instructions for the Questions. Certain Questions on the Model Form may be customized as follows:

(i) "Who is providing this notice?" This question may be omitted where only one licensee provides the Model Form and that licensee is clearly identified in the title on Page One. Two or more licensees or financial institutions that jointly provide the Model Form must use this question to identify themselves as required by [insert citation for section of statute or regulation that parallels Section 15(E) of NAIC model *Privacy of Consumer Information Act*]. Where the list of licensees or financial institutions exceeds four (4) lines, the licensee must describe in the response to this question the general types of licensees or financial institutions jointly providing the notice and must separately identify those licensees or financial institutions, in minimum 8-point font, directly following the "Other important information" box, or, if that box is not included in the licensee's form, directly following the "Definitions." The list may appear in a multi- column format.

(ii) "How does [name of licensee] protect my personal information?" The licensee may only provide additional information pertaining to its safeguards practices following the designated response to this question. Such information may include information about the licensee's use of cookies or other measures it uses to

© 2026 National Association of Insurance Commissioners

safeguard personal information. Licensees are limited to a maximum of 30 additional words.

(iii) "How does [name of licensee] collect my personal information?" Licensees must use five (5) of the following terms to complete the bulleted list for this question: open an account; deposit money; pay your bills; apply for a loan; use your credit or debit card; seek financial or tax advice; apply for insurance; pay insurance premiums; file an insurance claim; seek advice about your investments; buy securities from us; sell securities to us; direct us to buy securities; direct us to sell your securities; make deposits or withdrawals from your account; enter into an investment advisory contract; give us your income information; provide employment information; give us your employment history; tell us about your investment or retirement portfolio; tell us about your investment or retirement earnings; apply for financing; apply for a lease; provide account information; give us your contact information; pay us by check; give us your wage statements; provide your mortgage information; make a wire transfer; tell us who receives the money; tell us where to send the money; show your government-issued ID; show your driver's license; order a commodity futures or option trade.

Licensees that collect personal information from their affiliates and/or credit bureaus must include the following statement after the bulleted list: "We also collect your personal information from others, such as credit bureaus, affiliates, or other companies." Licensees that do not collect personal information from their affiliates or credit bureaus but do collect information from other companies must include the following statement instead: "We also collect your personal information from other companies." Only licensees that do not collect any personal information from affiliates, credit bureaus, or other companies can omit both statements.

(iv) "Why can't I limit all sharing?" Licensees that describe state privacy law provisions in the "Other important information" box must use the bracketed sentence: "See below for more on your rights under state law." Other licensees must omit this sentence.

(v) "What happens when I limit sharing for an account I hold jointly with someone else?" Only licensees that provide opt-out options must use this question. Other licensees must omit this question. Licensees must choose one of the following two statements to respond to this question: "Your choices will apply to everyone on your account." or "Your choices will apply to everyone on your account—unless you tell us otherwise." Licensees may substitute the word "policy" for "account" in these statements.

(b) General Instructions for the Definitions. The licensee must customize the space below the responses to the three definitions in this section. This specific information must be in italicized lettering to set off the information from the standardized definitions.

(i) Affiliates. As required by [insert citation for section of statute or regulation that parallels Section 9(A)(3) of NAIC *Privacy of Consumer Information Act*], where [affiliate information] appears, the licensee must:

(a) If it has no affiliates, state: "[name of licensee] has no affiliates";

(b) If it has affiliates but does not share personal information with them, state: "[name of licensee] does not share with our affiliates"; or

(c) If it shares with its affiliates, state, as applicable: "Our affiliates include companies with a [common corporate identity of licensee] name; financial companies such as [insert illustrative list of companies]; nonfinancial companies, such as [insert illustrative list of companies]; and others, such as [insert illustrative list]."

(ii) Nonaffiliates. As required by [insert citation for section of statute or regulation that parallels Section 9)(A)(3) of NAIC *Privacy of Consumer InformationAct*], where [nonaffiliate information] appears, the licensee must:

© 2026 National Association of Insurance Commissioners

(a) If it does not share with nonaffiliated third parties, state: "[name of licensee] does not share with nonaffiliates so they can market to you"; or

(b) If it shares with nonaffiliated third parties, state, as applicable: "Nonaffiliates we share with can include [list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations]."

(iii) Joint Marketing. As required by [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*], where [joint marketing] appears, the licensee must:

(a) If it does not engage in joint marketing, state: "[name of licensee] doesn't jointly market"; or

(b) If it shares personal information for joint marketing, state, as applicable: "Our joint marketing partners include [list categories of companies such as credit card companies]."

(c) General instructions for the "Other important information" box. This box is optional. The space provided for information in this box is not limited, and an additional page may be used if necessary. Only the following types of information can appear in this box:

(i) State and/or international privacy law information; and/or

(ii) A form by which the consumer may acknowledge receipt of the notice.

Chronological Summary of Actions (all references are to the Proceedings of the NAIC)

2000 Proc. 3rd Quarter 7, 10, 14-36, 904 (adopted).
2002 Proc. 3rd Quarter12, 13, 71, 72-73 (amended).
2017 Spring National Meeting (amended).

© 2026 National Association of Insurance Commissioners

Version 1:
Model Form with No Opt-Out

Rev. [insert date]

FACTS	WHAT DOES [Name of Licensee] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores] When you are *no longer* our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

Questions?	Call [phone number] or go to [web site]

© 2026 National Association of Insurance Commissioners

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Confidential

Version 2: Model Form with Opt-Out by Telephone and/or Online

Rev. [insert date]

FACTS	WHAT DOES [NAME OF LICENSEE] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

To limit our sharing	■ Call [phone number] —our menu will prompt you through your choice(s) **or** ■ Visit us online: [web site] **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

© 2026 National Association of Insurance Commissioners

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Confidential

Rev. [insert date

Version 3: Model Form with Mail-in Opt-Out Form

FACTS	WHAT DOES **[NAME OF LICENSEE]** DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

© 2026 National Association of Insurance Commissioners

Page 2

To limit our sharing	▪ Call [phone number] —our menu will prompt you through your choice(s) ▪ Visit us online: [web site] or ▪ Mail the form below **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

Mail-in Form

Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless your mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me.	
	Name	
	Address	
	City, State, Zip	
	[Account #]	
Mail To:	[Name of Licensee] [Address] [City], [ST] [ZIP]	

© 2026 National Association of Insurance Commissioners

Confidential

Page 3

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ▪ [open an account] or [deposit money] ▪ pay your bills] or [apply for a loan] ▪ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ▪ sharing for affiliates' everyday business purposes—information about your creditworthiness ▪ affiliates from using your information to market to you ▪ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ▪ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ▪ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ▪ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Version 4: Optional Mail-in Form

Mail-in Form	
Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me. **Name** **Address** **City, State, Zip** **[Account #]**
Mail To:	[Name of Licensee], [Address 1], [Address 2], [City], [ST] [ZIP]

© 2026 National Association of Insurance Commissioners

Industry Comments:



September 22, 2026

RE: ACLI Comments to the Revised Chair's Draft of Model 672 to the Privacy Protections (H) Working Group

Dear Chair Dwyer and Vice Chairs Houdek and Cornelius:

We appreciate the care, transparency, and amount of time spent on this drafting effort to modernize Model 672. Consumers deserve stronger protections with regard to the use, processing, and sharing of their data and there are opportunities in this draft to strengthen those protections in a meaningful way while still ensuring consumers have access to affordable and readily available products and services. While the revised draft addresses many items necessary for a modernized and more uniform framework, there are still several key areas which would benefit from revisions to provide a workable path forward. Throughout the process, ACLI has been supportive of this effort, providing redlines and recommendations and hopes to continue to be a collaborative partner, available to provide any follow-up via conversations or written comments.

Of ACLI's recommended revisions to the draft, the below items indicate the highest levels of concern from our feedback, as mirrored in our joint trades' coalition letter:

- Expansion of the "Consumer" Definition and the Removal of the "Customer" Definition
- Scope of Access, Correction, and Deletion Rights
- Third-Party Service Provider Requirements
- Sale, Targeted Advertising, and Sensitive Personal Information
- Lack of Basis in and Cohesion with Existing Frameworks
- Nonpersonal public information (NPI) and nonpublic personal health information (NPHI) Definitions

However, in order to address inconsistencies within the draft and suggest areas for harmonization, our suggested redlines ("ACLI Appendix A" or "Appendix A"), if adopted, would provide for a more cohesive draft that would make adoptability in states more seamless. In order to most easily address concerns within the draft, the below comments are organized in the order of the Articles presented for review.

ARTICLE I. GENERAL PROVISIONS

ACLI does not have specific concerns at this time for Sections 1, 2, or 3.

Section 4 Definitions

"Biometric data" definition. The biometric data definition does not currently include references to HIPAA information which could cause issues with consumer understanding and scope. ACLI's suggested edit, mirrors Virginia Consumer Data Protection Act (VCDPA Section 59.1-575). This alignment with an existing

The American Council of Life Insurers (ACLI) is the leading trade association driving public policy and advocacy on behalf of the life insurance industry. 90 million American families rely on the life insurance industry for financial protection and retirement security. ACLI's member companies are dedicated to protecting consumers' financial wellbeing through life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, and dental, vision and other supplemental benefits. ACLI's 275 member companies represent 94 percent of industry assets in the United States.

privacy law not only demonstrates consistency in expectations for consumers in regards to how their biometric data is treated, but also demonstrates important exclusions covered under HIPAA.

> **Suggested Edit:** "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA, unless such data is generated to identify a specific individual.

"Consumer" definition expansion. The absence of a "customer" definition creates a myriad of issues in the draft including direct contradictions and confusion that would make application and compliance impossible. We suggest editing the "consumer" definition as outlined elsewhere, and, importantly, folding the "customer" definition back into the draft. Overall, we suggest returning to the existing Model 672 method of distinguishing the customer and consumer definitions to original form, which will avoid the litany of issues described below and elsewhere. Not only does this simplify edits elsewhere that are warranted as a result of deleting this definition and folding it into "consumer" in the first place, but also allows for consumers (and customers) to understand their rights as aligned with other important privacy laws to date.

- *Precedent of Customer/Consumer Definition Distinctions:* For states that have adopted Model 672 and in complying with GLBA, there is precedent in both 672 and GLBA for distinguishing between consumers and customers, particularly as it pertains to providing notices. For example, it would be very confusing to a consumer who does not have a customer relationship with a licensee to receive a notice despite not having a policy with a licensee. Another issue is the current definition would appear to apply to an individual who applied for, but was denied coverage. If so, would that person be considered a customer, and if not, does that mean their data is automatically deleted or destroyed? This definition change and deletion of the "customer" definition open the door to a great number of questions such as these. Additionally, this requirement might prove impossible where printed notices are required if a licensee does not even have the address of a "consumer".
- *Impact on Notices:* The compliance cost and burden increases significantly if licensees are meant to send printed notices to all consumers, not just customers. If this is the intended result, we would seek clarification on how this better protects individuals seeking products and services as it would necessitate significant implementation flexibility for the expanded scope to claimants and beneficiaries.

"Consumer" Definition and Deletion of "Customer" Definition Specific Issues:

- A particular concern with the written definition of "consumer" is subsection (e) which provides for notice obligations. If this definition is maintained as written without a customer distinction, particularly helpful clarifications would be 1) when the notice clock begins for claimants/beneficiaries (and whether an initial notice can be satisfied through existing claims communications) and 2) permission to utilize existing statutory claim notices or onboarding workflows as substitutes and anchors to avoid duplicative notices.
- There is also an issue with subsection (e) as it pertains to references to Sections 22-24. We suggest striking this language or otherwise including Sections 19-21 as well. Any licensee activity touching those three sections as well could inadvertently void the carve-out for group participants and beneficiaries.

- Another specific example is a contradiction between subsection f(ii) and f(i). This illustrates some of the issues with deleting the "customer" definition and some of the contradictions within the draft as a result of deleting "customer" and not tracking that change throughout. As it stands, the statements in f(i) and f(ii) cannot both be true. If the draft does NOT include a "customer" definition again, we suggest deleting f(ii) in its entirety to avoid contradiction and confusion.

Suggested Edit: Please see edits provided in ACLI Appendix A for Consumer and Customer definitions.

"Genetic Information" Definition. Because of the reference to the term "genetic information," in the "sensitive personal information" definition, this term should be defined as well. ACLI's redlines recommend a definition that aligns with HIPAA.

Suggested Edit: XX. "Genetic information" means the same as ascribed to it under materials regulated under the Health Insurance Portability and Accountability Act (HIPAA) as specified in 45 CFR 160.103.

"Licensee" definition. For "Licensee" subsection (2), we recommend striking the enumeration of Articles in subsection 2 so as not to create an exclusionary list which does not accommodate all references necessary or include Articles V and VI explicitly. ACLI's redlines demonstrate the simpler approach of deleting the enumeration.

Suggested Edit: A licensee is not subject to the notice and opt out requirements for nonpublic personal information set forth in ~~Articles I, II, III and IV of~~ this Act if the licensee is an employee, agent or other representative of another licensee ("the principal") and:

"Nonpublic personal health information" and "Nonpublic personal information" definitions. The definition appears to expand dramatically what may be considered non-public health data. The reasonable standard here will likely cause confusion and compliance hardships. Insurers may need to expend additional resources on data mapping and increase operational overhead, all leading to added costs. Further, this definition is not consistent with GLBA or existing provisions in other states, causing unequal consumer experience across states and confusion surrounding the distinctions between types of data.

- Additionally, in combining the term of "nonpublic personal health information" and "health information," important information is lost which causes issues elsewhere in the draft. If this definition is to be retained, examples concerning implementation guidance for "reasonably linkable" standard in the insurance context would be necessary. We would further recommend if this is kept, the draft should clarify whether inference-based linkage requires a certain threshold of feasibility. Leaving this definition as is would also necessitate a risk-based compliance approach (similar to other privacy regimes) rather than forcing every marginal field into a "linked" mapping category.
- In conjunction with the nonpublic personal health definition, there are also issues with the nonpublic personal information definition. The NPI definition is not consistent with GLBA or existing state protections, creating confusion for consumers as to the distinctions between their data types. Other issues surround this definition, including the expansion to "any natural person" licensees gather information about. The assumption is that this would apply to business to business contact, witnesses, police officers, etc. This expansion appears to be unintended in its impact.

- Further the deletion of "nonpublic personal financial information" causes significant issues throughout the draft as well as deviation from historically utilized terms that harmonize across jurisdictions. We would recommend continuing to provide separate definitions for NPI, NPHI, and NPFI, in accordance with the original Model 672 definitions as demonstrated in our redlines.

Suggested Edit: Due to the extensive nature of the redlines across these three definitions, we refer to the Appendix A for ACLI's suggested redlines.

"**Opt-in" and "Opt-out" definitions and impacts.** While the impact of opt-in and opt-out go beyond the actual the definitions, we would suggest at the outset deleting the two defined terms to avoid confusion or otherwise limit the consumer understanding of opt-in and opt-out just to the definition and not the narrow categories to which they apply elsewhere. Other existing frameworks do not currently maintain definitions for these two terms, however ACLI is happy to provide follow-up redlines or guidance if we are able to maintain a better understanding as to the purpose and inclusion of these terms by the working group.

- With these proposed changes surrounding opt-in and opt-out, the consent and choice structure is narrowed and does not adequately follow the precedent known and set by GLBA. The opt-in and opt-out mechanics focus heavily on the "disclosure of nonaffiliated third parties" rather than broader "use/sharing" categories which would create compliance issues that impact the recipient-structure area of licensee operations as opposed to the business-purpose area. This would warrant significant lead time for licensees to accommodate those changes due to the structure of operations today. ACLI is happy to gather further member comments or facilitate direct member conversations with working group members to better dialogue on how these changes would impact business operations and, in turn, consumer access to products and services.
- Importantly, introducing separate consent models, including an opt-in requirement for sales and an opt-out right for targeted advertising, creates a more complex and fragmented framework that may be difficult for consumers to understand and navigate. It will also likely require significant system modifications, new consent-tracking capabilities, revised notices and workflows, and could lead to operational delays and increased compliance risk.
- While the "opt-in" definition is broad, "authorizes disclosures," the real triggers are very narrow (e.g. the sale of nonpublic personal information and sensitive personal information outside permitted purposes). This raises a risk of over-implementing consent in low-risk places that cause significant hindrances on effectuating products and services. This also raises the risk of under-implementing where sensitive-category processing matters. A more precise approach to balancing opt-in and opt-out in practice and understanding the implications of the language as provided is helpful in order to adequately address consumer concerns with use and sharing of data while also maintaining opportunities for consumers to maintain their understanding of opt-out in effectuating their products and services.
- We would offer that there appears to be a strong misconception around the strength of consumer rights under "opt-out" practices. Namely, we reiterate that these practices are grounded in existing GLBA and decades-long expectations for licensees and consumers as to how consumers control the use and sharing of consumer data. These are not "gotcha" or otherwise predatory in nature so much as opportunities for consumers to exercise their data rights as they choose in a way designed to expand the opportunities for consumers to receive the most seamless execution of their products and services

without inadvertently missing an opportunity to opt-in or not fully understanding the impact of choosing not to opt-in to certain data sharing and use practices, which will inherently cause hurdles and administrative red tape in a licensee's ability to effectuate products and services.

- The definitions as written here contain very broad exceptions to opt-out for nonaffiliated third party services, including but not limited to, disclosing NPI about a consumer to licensee service providers, transaction processing providers, fraud or security vendors, and other legal providers.
- These particular restrictions within the opt-out definition essentially strip the meaning of opt-out and overly complicate the consent regime. This makes opt-out mimic paperwork and not meaningful behavioral constraints that benefit consumers.

Other opt-in/opt-out issues of note for the Working Group's consideration:

- Impact on current workflows for licensees using biometric or identity verification.
- Practical impact on compliance in capturing a consumer's election, which is often distributed across multiple channels (web portal, call center, mail), increasing the risk of gaps and inconsistent treatment.
- Recipient classification issues (i.e. where a vendor behaves like a service provider operationally but is treated contractually/structurally as a third party).
- Rules about whether opt-outs can be treated collectively versus separately can be implemented inconsistently without a robust account/coverage data model.

Suggested Edit: Please see the Appendix A for outlined redlines to address the specific opt-in and opt-out issues throughout the draft.

"Processing" definition addition. Because the draft utilizes this term and distinguishes "processing" from other uses of data, this term should be defined. We suggest the redline below also reflected in Appendix A.

Suggested Edit: XX. "Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

"Reasonable opportunity" definition. If the definition of "reasonable opportunity" remains, several considerations as to the potential cost and operational burden should be considered. Storing consent and election information as well as the additional compliance risk created by these requirements should all be considered. There would also need to be further clarifications on several questions, such as:

- If individuals are able to access the privacy policy through an insurer's website, does the insurer still need to comply with the requirements in this section?
- Are licensees required to provide a printed copy to every consumer they interact with at the point of collection of information. If so, when would the printed copy need to be provided to each person? (This is a key area where the deletion, and therefore distinction, of the "customer" versus "consumer" definitions would create significant unintended consequences with harms that outweigh benefits to consumers).

Suggested Edit: As it pertains to this definition and our redlines, we would suggest redlining the draft to return the "customer" definition and, therefore, "customer" term throughout this definition to remedy the aforementioned problems. Edits are reflected in Appendix A redlines.

"Sale" or "selling" definition. Subsection X(1) currently allows for instances where disclosures are made pursuant to a contract or direct mailing service where the customer did not request the service, but it is otherwise required for compliance reasons and would be expected by the customer in further effectuation of their product or service.

Suggested Edit: The disclosure is to a third party for the purpose of or in support of providing a product or service requested ~~by~~ for the consumer.

- Subsection X(3) currently addresses providing nonpublic personal information to an "affiliate or to a financial institution with which the licensee performs joint marketing." Based on this language, application should extend to non-affiliated third parties as well.

Suggested Edit: A licensee provides nonpublic personal information to an affiliate, non-affiliated third party, or to a financial institution with which the licensee performs joint marketing;

"Sensitive Personal Information" definition. Under the current definition, there is redundant language that can be removed to provide clarity. Additionally, as noted above, "genetic information" should be defined as it is referenced in this definition.

Suggested Edit: Sensitive Personal Information" means ~~personally identifiable~~ "nonpublic personal information" about a consumer that includes:

- Subsection Y(2) should be edited to reflect genetic information or biometric data that is processed, not "may be" as the latter indicates a much broader scope of information.

Suggested Edit: Genetic information or biometric data that ~~may be~~ is processed for the purpose of uniquely identifying an individual.

"Targeted advertising" definition. The current definition references "personal data" which is an undefined term and would create confusion as to application. We recommend changing this language to nonpublic personal information.

Suggested Edit: "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on ~~personal data~~ nonpublic personal information obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests.

"Third Party Service Provider" or "third party" definition. "Third party service provider" is the more accurate and preferred term here, with "third party" creating an unusual definition term and could invite potential issues (i.e. separate definition of nonaffiliated third party). We suggest not including "third party" as an equal term to "third party service provider."

Suggested Edit: "Third party service provider" ~~or "third party"~~ means a person or entity not otherwise defined as a licensee or affiliate of a licensee that:

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Section 5 Third-Party Service Provider Arrangements

General Concerns with Section 5. As written, this draft would require insurers to review and amend a large number of existing vendor contracts, even where current agreements already contain robust privacy, security, and confidentiality protections. Importantly, these new requirements would cause significant time and expense surrounding contract remediation, would potentially invite vendors to re-negotiate unrelated commercial terms, and overall apply additional burdens for insurers that have already

relatively recently remediated contracts to comply with CPRA requirements. If these new requirements added a substantial or meaningful benefit to consumers as a whole that outweighed the burdens outlined, consumer protection arguments would make sense. However, in this instance it appears that the benefit to the average consumer would not be substantial and the potential for harm via less accessible or affordable products and services would be great.

Suggestion: We recommend reviewing the specific subsection concerns below as well as our attached Appendix A. By reviewing each piece of this Section, weighing the actual benefits to consumers versus the potential consumer harm, revisions to this Section would create a much stronger point of alignment for adoption across a breadth of states. Further, in considering any changes to this Section, we encourage this Working Group to consider prospective application for new agreements and renewals rather than re-negotiation and broad remediation of all existing contracts.

Section 5(A)(4). Not only does the requirement suggested in Section 5(A)(4) go beyond the scope of licensee agreements, this is a mandate on third party service providers, significantly hindering any bargaining power and necessitating complete re-negotiation of a significant amount of contracts. Further, many licensees already exercise best practices and other due diligence surrounding their relationships with third party service providers.

- This creates significant privity of contract issues beyond the scope of the licensee and third party service provider's agreement. We therefore, strongly suggest deleting this subsection. In the absence of deletion, we recommend language that does not require or stipulate provisions in the third party service provider and subcontractor's contract (of which the licensee is not a party to) but instead must "recommend to the third party service provider provisions no less protective."

Suggested Edit: Delete Subsection 4 in its entirety as outlined in Appendix A redlines.

Section 5(A)(6)-(7). Both of these requirements are neither appropriate nor necessary in a Privacy Model as they are duplicative of Security Model # 668, duplicative of state AG breach notification considerations (to notify the Data Owner), and would trigger an avalanche of negotiations and re-opening of contracts with many third party service providers. Further, Section 5(A)(6) conflates privacy and security which could lead to confusion in state adoption.

- Moreover, Section 5(A)(7) conflicts with many state laws and regulations. Specifically, the 48 hour requirement conflicts with the 72 hours required by the NYDFS cybersecurity regulation and the new SEC cybersecurity rule. In fact, the SEC also considered 48 hours but ultimately concluded that time frame was inconsistent with other regulations.
- Lastly, the obligation to notify here is not tied to a breach of nonpublic information; rather, notice is triggered without a breach of nonpublic personal information if the third party service provider fails to implement reasonable controls to protect personal data. If a third party service provider is required to notify customers each time there is a lapse in its security (absent a suspected or actual breach of nonpublic information), consumers would be inundated with notices that are not actionable in any real way. Because this provision is unworkable, conflicts with other established provisions, and conflates privacy and security, we recommend striking the provision in its entirety.

Suggested Edit: Delete both Subsection 6 and 7 in their entirety as outlined in Appendix A redlines.

Section 5(B). Section 5 would make licensees solely responsible for third party service provider compliance, creating indemnification issues and contract issues. This provision would

severely impact allocation of risks and could result in even those who intentionally disregard contractual promises avoiding responsibility for their actions and, where applicable, their own independent legal obligations. Shielding third party service providers who fail to live up to their contractual promises from accountability will actually reduce consumer protection and is out of sync with other privacy enactments.

- As opposed to making the life insurance industry a significant outlier and imposing requirements and obligations that would not be feasible, this language should instead align with existing consumer protection frameworks like the disclosures and requirements under current laws (i.e. HIPAA and NYDFS Part 500).

Suggested Edit: Delete Subsection B in its entirety as outlined in Appendix A redlines.

ARTICLE III. CONSUMER REQUESTS

Section 6 Access, Correction, and Deletion of Nonpublic Personal Information

Section 6 "Customer or former customer." ACLI's Appendix A includes the full extent of redline suggestions and should be consulted as the complete document of our redlines to date. Primarily, for this section Appendix A returns language back to reflecting the distinction between "customer" and "consumer," which is particularly pertinent as it relates to requests. Requests from "consumers" as currently defined would pose a litany of issues, not only due to issues surrounding claimants and beneficiaries, but also for bad faith requests intended to lay groundwork for litigation as opposed to legitimate customer or former customer requests.

Section 6(A)(1)(b). As previously mentioned, a list of third party service providers will not provide the consumer with meaningful information. Categories are much more helpful and allow consumers to understand why their information is being shared in the first place (i.e. TPSP roles and categories that provide beneficial knowledge to consumers). Additionally, exposing third-party relationships publicly is burdensome and could disclose confidential/proprietary vendor relationships. Further, there are cybersecurity risks from disclosure of certain venders related to security. This is a contractual, business, and security issue as noted previously.

Section 6(A)(2). As drafted, this section likely will cause confusion due to Section 6(A)(1) language. Section 6(A)(1) directs consumers to make requests, but in a later section narrows what can be requested. It puts licensees and consumers in an adversarial position, which will likely cause customer complaints. We suggest redlining as outlined in Appendix A. This mirrors the language more closely between 1 and 2 to assist in customer understanding of their rights and exceptions.

Section 6(A)(3) Addition. A lookback period is necessary to limit request responses (CCPA 1798.130(a)(2)(B)). Appendix A suggests an added subsection 3 which would address this necessary limiting provision.

Section 6(B)(3). Further exceptions are necessary to address situations where a customer or former customer requests correction of information that was not under the licensee's control or that the licensee does not maintain in an accessible operational system.

Section 6(C)(1). The 45-day SLA (intake, authentication, cross-coordination with TPSPs under the new Article II contract terms) is a new operational build for carriers whose systems are currently structured

around GLBA-style opt-out administration rather than individual-rights request fulfillment, for the population of consumers who ARE covered.

- This 45 day timeline does not provide adequate time for what is requested, particularly of third parties. The degree of requirements included in Section 6(C)(1) does not mirror other existing state frameworks and places an extreme operational burden on licensees.
- For life insurers in particular, the amount of data stored in legacy systems can require more time than what is outlined in this subsection. Further, there is the potential for consumer harm if this process is rushed. Lastly, the concern of deleting information that could potentially be valuable to the customer at a later date would all be alleviated by a longer period of time to accommodate the requirements outlined in Section 6(C)(1). For these reasons, and absent comparable provisions that outline time periods to accommodate this level of operation in other frameworks, we suggest a 90 day timeline.

Section 6(C) Additional Suggested Language. Other edits reflected in Section 6(C) attempt to cover the scope of information out of licensee control or information that would otherwise cause issues unintended by regulators in drafting. These edits largely mimic existing frameworks.

- **Section 6(C)(2)(e)-(g).** Information that is not under a licensee's control and is not maintained in an accessible operational system, retained data solely used (and adequately restricted) for disaster recovery, and information that is technically infeasible to retrieve should all be included under the listed exceptions. These are all important exceptions found in other frameworks that are not currently covered by (a)-(d). Appendix A reflects our suggested revisions.
- **Section 6(C)(3).** The edits suggested in Appendix A mimic the CCPA which addresses the same reason for delay and does not require overly burdensome provisions that would create operational infeasibilities.
- **Section 6(C)(4).** This edit is intended to remedy situations where the strict 45-day timeline for deletion is at the request of information not actively used or readily stored by a licensee.

Section 6(D). The draft does not currently have a cap on the number of correction or deletion requests, which does not pose any necessary limitations to ease operational burden and unnecessary or abusive requests. Without a reasonable limit, consumers could submit an unlimited number of nuisance requests, creating a significant operational burden. This could also become especially problematic in the litigation context. CA addressed this issue under the CCPA with a limit of 2 requests per calendar year, as demonstrated in our redlines.

- **Section 6(D)(1)(d).** In order to provide clear guidance on timeline and when the clock begins for the requirements outlined in this section, we suggest adding language to establish a clear timeline and direction of when the time begins for licensees to complete a customer or former customer's request.

Section 6(D)(b). Appendix A provides language with limiting provisions to avoid the need for the creation of licensee arbitration hubs or general dispute arbiters and still allow customers and former customers meaningful correction standing in the event of a dispute.

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7 Initial and Subsequent Delivery Notice of Information Practices to Consumers Required

Section 7(A). A return to the existing language as opposed to the revised chair's draft would provide a more operable and proven method of clearly protecting consumer rights via notice obligations without placing unreasonable expectations on time provided for licensees to give such notice. A notice at collection is extremely difficult to provide when the company does not collect the information directly from the individual. CCPA addressed this by providing language that is mirrored in ACLI's suggestion in the attached redlines of Appendix A. Other edits suggested in the redline for Section 7(A) reflect a better understanding of when a consumer would expect to receive a notice and how, operationally speaking, licensees would implement such notice requirements.

- **Section 7(A)(1).** The duty here is triggered when a company "obtains access to nonpublic personal information," but for claimants the person may not be "choosing" the insurer the way a normal applicant/customer does, they are filing a claim to get benefits. Additionally, for beneficiaries, the person may not even know that someone has elected them as a beneficiary. Further, this language may be problematic, such as for policy acquisitions/assignments where the insurer must determine whether the consumer had a real choice. The exception is trying to solve a "customer choice/continuing relationship" concept, but it is implemented using "consumer election" language that may not match how claims are initiated. The drafting appears to rely on a subjective factual inquiry ("Was it at their election?") that is hard to administer consistently.
    - Under GLBA, a licensee generally provides an initial privacy notice when establishing a customer relationship or, for certain consumers, before specific disclosures to nonaffiliated third parties. The change to "when the Licensee *obtains access* to the consumer's nonpublic personal information" raises interpretive questions as to what constitutes "access." For example, does the licensee obtain access to a consumer's information when the licensee receives information from an agent or broker acting as an intermediary in the insurance transaction? If so, this substantially changes the scope of providing initial notices and does not align with long held consumer expectations.
    - The change in trigger of "obtaining access" would also theoretically require notice to third-party claimants, additional drivers listed on a policy, adverse claimants and other individuals with no ongoing relationship to the licensee. This would require a licensee to identify every point in which Nonpublic Personal Information is first obtained and the exceptions may not adequately protect ordinary insurance operations (i.e. Information received from third parties). The existing GLBA customer-relationship framework is clearer, more workable, and better aligned with consumer expectations.
    - The suggested edits in Appendix A, provide an explicit provision to address instances where a licensee neither collects nor controls the collection of personal information directly from the consumer. These edits also replace the election-based test with an objective, event-based trigger, paired with a delivery mechanism modeled on Section 14 for situations where direct delivery isn't practicable.

Section 7(C). Further clarification is necessary to address what is meant by "electronic." For example, does electronic mean website, text message communications, emails, etc? The carve-outs may create a paperwork or data recording burden and warrant different levels of treatment depending on the electronic channel utilized, creating different and confusing consumer experiences.

- **Section 7(C)(2)** should be edited to alleviate previously cited issues with unclear coverage of each type of communication. Appendix A suggests such edits.

Section 8 Annual Notice of Information Practices to Consumers Required

Section 8. Section 8 highlights another key area where the delineation between "customer" and "consumer" is crucial to not creating an inordinate operational burden to address an unintended audience. The annual privacy notice should only be required for customers with an ongoing relationship.

- Extending this requirement to all consumers – including those who simply expressed interest in a product –is not practical and does not serve consumer interests, even acting as a deterrent for consumers in deciding whether to become a customer in the future. This also creates an obligation to send these annual notices to individuals the licensee does not have a customer relationship with in perpetuity. The existing model appropriately limited the annual notice requirement to customers with an ongoing relationship and only for the duration of that relationship.
- Further, because of the inclusion of beneficiaries in the current "consumer" definition of the draft, this would require providing notices to beneficiaries, which could disclose that an individual is a beneficiary, even though beneficiary designations can change at any time. There may also be legitimate reasons why a policyowner would not want a beneficiary to be aware that they have been designated.

Therefore, ACLI suggests returning to that language as outlined in ACLI Appendix A.

Section 9 Information to be Included in Notices of Information Practices

Section 9(A). The edits provided in Section 9(A) would significantly increase company resources, time, and operational costs due to the nature of printing and mailing notices and altering current practices. To address those edits that increase costs but do not provide a substantial benefit to customers and consumers, we would suggest the changes in Appendix A.

- Importantly, for **Section 9(A)(3),** this would potentially require more transparency regarding sharing practices with affiliates than non-affiliate third parties because both the affiliates and non-affiliates may be providing the same types of services. For example, an affiliate reinsurer may need to be disclosed in the notice, and a nonaffiliate third party reinsurer may not need to provide notice because they fall within Section 22, 23, and 24. One remedy would be including affiliates in Sections 22, 23, and 24.

Section 9(B). Clarification under Section 9(B)(2) would be helpful to understanding the "future sharing" that category-based notices are intended to cover. Enumerating or listing what is intended by "disclose in the future, but does not currently disclose," would be helpful.

- Additionally, clarification on how "future sharing" affects the obligation to provide revised notices (Section 13) and whether adding new categories triggers revisions/material change, even if disclosures remain within described categories, would be helpful.

ACLI does not have a suggested redline, but would be ready to provide one after clarification on the aforementioned question is provided.

Section 10 Short Form Initial Notice of Information Practices

Section 10(A). It would be helpful to have clarification surrounding what would happen if a licensee under Section 10(A) does not have to deliver an opt-out and whether that means that a licensee would be unable to utilize the short form notice.

- For example, in Model 670, short form notice is not necessary unless the customer is applying for or renewing a product or service. The current language here suggests that insurers would be expected to deliver a short form notice to *everyone*.

- Lastly, in considering the purpose of a short form notice and readability for consumers, it would be helpful when editing to review the additional information requirements and whether they impact the value of the notice and do not detract from the purpose of being short and readable.

Section 10(B)(4). The requirement to include the commissioner's contact information in the Short Form Notice of Information Practices is particularly challenging for insurers operating nationally. Compliance would likely require the creation and maintenance of separate state-specific notices, ongoing monitoring contact information, and system changes to ensure the appropriate notice is delivered based on the consumer's state. These changes would add substantial administrative complexity and cost while providing information that consumers can readily obtain through publicly available resources. Including the commissioner information would also potentially confuse the consumer. The commissioner's contact information does not directly relate to the notice's purpose of explaining privacy practices and, because, in part, the consumer may interpret this as encouraging complaints regarding routine privacy practices even when the licensee is in compliance, this section should be removed. We suggest striking subsection 10(B)(4).

Section 11 Form of Opt-In Notice to Consumers and Opt-In Methods

Section 11. Overall, more clarification and definitions are necessary for this section, particularly as it creates a non-GLBA opt-in regime which will necessitate significant changes and lead time for implementation by licensees.

- **Section 11(B).** This language as drafted will cause confusion, notably due to the fact that Sections 13, 14, and 15 of GLBA currently offer an opt-out regime for sharing with nonaffiliated parties (not withstanding exceptions and exemptions). GLBA also allows for opportunities for gaining customer consent that is not illustrated here and would provide greater consistency.
- **Section 11(C).** "Affirmative act" is not defined in the draft and can cause confusion on what is acceptable under this term. We suggest if including this term throughout the draft, the revisions reflect a definition for this term.
- **Section 11(D).** If language is retained in Section 11(D), would verbal opt-in be separate or disallowed? How would this be documented? These issues illustrate the complications with making this an opt-in standard and the deviation from consumer-expected approaches under GLBA.
    - Similar to other subsections within Section 11, subsection (E) also raises questions as to what constitutes a proper revocation and acceptable forms of revocation. Further, it raises the question of what degree of specificity is required when revoking consent. Is the revocation a blanket revocation, or is it specific to certain types of sharing? Clarification here would be helpful.

Section 12 Form of Opt-Out Notice to Consumers and Opt-Out Methods

Section 12(A)(1)(a) includes language stating that the licensee "reserves the right" to disclose NPI, language inconsistent with current industry practices and current consumer expectations. We suggest striking this language.

Section 12(A)(2)(a)(ii) requires opt-out notices be individualized which not only creates reworking of licensee current systems, but also does not appear to provide a corresponding and balanced benefit to consumers. We would suggest deleting this requirement entirely to avoid room for errors, substantial operational buildouts, and confusion to consumers.

Further, **Section 12(A)(2)(a)(i)** is sufficient to address the concerns sought after in subsection (ii). If there is an area (ii) seeks to address that Working Group members do not believe is alleviated by (i), we would be happy to discuss other language changes to address those issues that would not create the feasibility and workability issue currently present.

Section 12(A)(2)(b)(iii) should allow for licensees to provide a means for opt-out on their website as an option without a prior agreement from the customer. This reflects a more modern approach to data privacy, providing for durability in this Model revision.

Section 12(E). ACLI respectfully requests clarification that "10 days" in Section 12(E) means business days, or otherwise provide a longer compliance period (i.e. 15–30 days) for operational feasibility, particularly where systems, vendor updates, and downstream propagation are required. Appendix A reflects suggested redlines.

Section 13 Revised Notice of Information Practices

Section 13(B)(1). In understanding what the trigger is for providing notice, it would be helpful to express a materiality standard. For example, does a new category of nonaffiliated third parties constitute a material change if the information was already being shared? ACLI welcomes any further dialogue on how to address a materiality threshold or how to otherwise express a clear trigger for revised notices.

Section 14 Notice of Information Practices to Group Policyholders

No comments on Section 14 at this time.

Section 15 Delivery

Section 15(A). Suggested redlines in Appendix A reflect a more modernized approach to the methods in which consumers and customers currently engage via website access.

Section 15(B). As the draft is currently written, for electronic customers, the notice must be posted and the customer must acknowledge receipt as a necessary step to obtain the product or service which differs significantly from GLBA workflows where notice could be delivered without blocking the transaction.

- This would likely force licensees to make changes to purchase and quote-flows and potentially "quote" itself as a transaction step requiring acknowledgement.
- If the Working Group does not revise this subsection, a flexible implementation period would be necessary for electronic notice acknowledgment.
- Appendix A clarifies that "necessary step" means the notice must be presented and acknowledged at or before contract initiation (not necessarily blocking all quote or marketing-inquiry steps).

ARTICLE V. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

We do not have comments at this time on Sections 16 and 18. In Appendix A, we provide some clerical changes to Section 16 for readability.

Section 17 Limits on Redisclosure and Reuse of Nonpublic Personal Information

Section 17 currently does not reference the full scope of parties addressed under the exceptions in Article VI. For clarification purposes, we recommend addressing all parties subject to exceptions under Article VI, not just nonaffiliated third-party service providers.

Section 19 Limits on Disclosure of Nonpublic Personal Information in Targeted Advertising

Section 19. Section 19 should clarify that the opt-out is completed through the licensee's website, not by mail. A website-based opt-out is consistent with other modern privacy provisions such as those in CCPA. This is also consistent with the use described here, which is specific to website and online activity.

- **Section 19** should also include a provision addressing instances where the opt-out request does not match the personal data in the licensee's records.

These suggestions are supported by the provided redlines in Appendix A.

Section 20 Limits on Sale of Nonpublic Personal Information

We do not have comments at this time on Section 20.

Section 21 Limits on Disclosure of Sensitive Personal Information

Section 21. An opt-out standard, as expressed elsewhere is necessary for best effectuating the products and services of the customer as well as creating the least amount of confusion for the customer as to the opt-in and opt-out rights they maintain. Suggested redlines are provided in Appendix A.

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Sections 22-24 Headings. Due to edits (provided in Appendix A) to Article V provisions, the headings in Sections 22-24 should reflect both opt-out and opt-in. Please see ACLI Appendix A.

Other than the aforementioned headings, we do not have comments at this time for Sections 22-24.

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 25 When Authorization Required for Disclosure of Nonpublic Personal Health Information

We do not have comments at this time for Section 25.

Section 26 Authorizations

Section 26. At present, it is unclear if (E) is requiring licensees to sign a copy of the authorization to submit to the consumer after it is received by the licensee or if licensees are being required to send a copy of the authorization that was signed by the consumer and submitted by the consumer back to the consumer (who should have their own copy already). Clarification here would be helpful.

We do not have comments at this time for Sections 27-29.

ARTICLE VIII. ADDITIONAL PROVISIONS

We do not have comments at this time for Sections 30-33.

Section 34 Individual Remedies

Section 34. ACLI strongly supports the inclusion of this provision and highly encourages the Working Group to maintain this language to ensure consumers and customers maintain adequate protections without creating a destructive and inappropriate abusive litigation opportunity.

Section 35 Effective Date

Section 35. No edits at this time, but we did want to highlight the necessity for flexibility in this section moving forward. Effective dates and compliance deadlines should strongly consider the implementation timelines that will be necessary based on the existing language and the increase in operational burdens and necessary compliance build-outs.

APPENDICES

We do not have comments at this time for Appendix A and Appendix B.

Thank you for the opportunity to provide these comments and attached redlines and we look forward to future conversations to ensure the best future for this draft.

Thank you,

Kirsten Wolfford
Associate General Counsel
ACLI

ACLI Appendix A

ACLI Suggested Redlines to Chair's Draft of Modernized Model 672

- ACLI Text Guide/Note: The black text is the Privacy Protections (H) Working Group's clean version of modernized Model 672 as of September 2026. Red and green text indicate ACLI suggested language.

PRIVACY OF CONSUMER INFORMATION ACT

Table of Contents

ARTICLE I. GENERAL PROVISIONS

Section 1. Purpose
Section 2. Scope and Compliance
Section 3. Rule of Construction
Section 4. Definitions

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Section 5. Third-Party Service Provider Arrangements

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7. Initial and Subsequent Delivery Notice of Information Practices to Consumers Required
Section 8. Annual Notice of Information Practices to Consumers Required
Section 9. Information to be Included in Notices of Information Practices
Section 10. Short Form Initial Notice of Information Practices
Section 11. Form of Opt-In Notice to Consumers and Opt-In Methods
Section 12. Form of Opt-Out Notice to Consumers and Opt-Out Methods
Section 13. Revised Notice of Information Practices
Section 14. Notice of Information Practices to Group Policyholders
Section 15. Delivery

ARTICLE V. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 16. General Rules for Use and Disclosure of Nonpublic Personal Information
Section 17. Limits on Redisclosure and Reuse of Nonpublic Personal Information
Section 18. Limits on Sharing Access Number or Access Code Information for Marketing Purposes
Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted Advertising
Section 20. Limits on Sale of Nonpublic Personal Information
Section 21. Limits on Disclosure of Sensitive Personal Information

© 2026 National Association of Insurance Commissioners

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 22. Exception to Opt Out and Opt-In Requirements for Disclosure of Nonpublic Personal Information for Service Providers and Joint Marketing
Section 23. Exceptions to Notice and Opt Out and Opt-In Requirements for Disclosure of Nonpublic Personal Information for Processing and Servicing Transactions
Section 24. Other Exceptions to Notice and Opt Out and Opt-In Requirements for Disclosure of Nonpublic Personal Information

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 25. When Authorization Required for Disclosure of Nonpublic Personal Health Information
Section 26. Authorizations
Section 27 Authorization Request Delivery
Section 28. Relationship to Federal Rules
Section 29. Relationship to State Laws

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 30. Protection of Fair Credit Reporting Act
Section 31. Nondiscrimination
Section 32. Violation
Section 33. Severability
Section 34. Individual Remedies
Section 35. Effective Date

APPENDICES

Appendix A Sample Clauses
Appendix B Federal Model Privacy Form
Model Law Forms

© 2026 National Association of Insurance Commissioners

ARTICLE I. GENERAL PROVISIONS

Section 1. Purpose

Purpose. This Act governs the treatment of nonpublic personal health information and nonpublic personal information about individuals by all licensees of the state insurance department. This Act:

A. Requires a licensee to provide notice to individuals about its privacy policies and practices;

B. Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal information about individuals to affiliates and nonaffiliated third parties; and

C. Provides methods for individuals to prevent a licensee from disclosing that information.

Drafting Note: Whether this model is adopted as an Act or Regulation will depend upon individual state law. If a state adopts the model as an Act, reference to the model as an Act should be updated throughout the model.

Section 2. Scope and Compliance

A. Scope. This Act applies to:

(1) Nonpublic personal information about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. This Act does not apply to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes; and

(2) All nonpublic personal health information.

B. Compliance. A licensee domiciled in this state that is in compliance with this Act in a state that has not enacted laws or regulations that meet the requirements of Title V of the Gramm-Leach-Bliley Act (PL 102-106) may nonetheless be deemed to be in compliance with Title V of the Gramm-Leach-Bliley Act in the other state.

Drafting Note: Subsection B is intended to give licensees some guidance for complying with Title V of the Gramm-Leach-Bliley Act in those states that do not have laws or regulations that meet GLBA's privacy requirements.

© 2026 National Association of Insurance Commissioners

Section 3. Rule of Construction

The examples in this Act, the sample clauses in Appendix A, and the Federal Model Privacy Form in Appendix B of this Act are not exclusive. Compliance with an example, use of a sample clause, or the Federal Privacy Model Form, to the extent applicable, constitutes compliance with this Act.

Licensees may rely on use of the Federal Privacy Form in Appendix B, consistent with the attached instructions, as a safe harbor of compliance with the Notice of Information Practices content requirements of this Act.

Use of the Federal Model Privacy Form is not required. Licensees may continue to use other types of privacy notices, including notices that contain the examples in this Act and/or the sample clauses in Appendix A, provided that such notices accurately describe the Licensee's privacy practices and otherwise meet the notice content requirements of this Act.

Section 4. Definitions

As used in this Act, unless the context requires otherwise:

A. "Affiliate" means a company that controls, is controlled by or is under common control with another company.

B. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA, unless such data is generated to identify a specific individual.

C. (1) "Clear and conspicuous" means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) Examples.

(a) Reasonably understandable. A licensee makes its notice reasonably understandable if it:

(i) Presents the information in the notice in clear, concise sentences, paragraphs and sections;

(ii) Uses short explanatory sentences or bullet lists whenever possible;

(iii) Uses definite, concrete, everyday words and active voice whenever possible;

(iv) Avoids multiple negatives;

(v) Avoids legal and highly technical business terminology whenever possible; and

© 2026 National Association of Insurance Commissioners

(vi) Avoids explanations that are imprecise and readily subject to different interpretations.

(b) Designed to call attention. A licensee designs its notice to call attention to the nature and significance of the information in it if the licensee:

(i) Uses a plain-language heading to call attention to the notice;

(ii) Uses a typeface and type size that are easy to read;

(iii) Provides wide margins and ample line spacing;

(iv) Uses boldface or italics for key words; and

(v) In a form that combines the licensee's notice with other information, uses distinctive type size, style, and graphic devices, such as shading or sidebars.

(c) Notices on web sites. If a licensee provides a notice on a web page, the licensee designs its notice to call attention to the nature and significance of the information in it if the licensee uses text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks or sound) do not distract attention from the notice, and the licensee either:

(i) Places the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(ii) Places a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

D. "Collect" means to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

E. "Commissioner" means the chief insurance regulatory official of the state.

Drafting Note: Use the title of the chief insurance regulatory official wherever the term "commissioner" appears. If the jurisdiction of certain health licensees, such as health maintenance organizations, lies with some state agency other than the insurance department, or if there is dual regulation, a state should add language referencing that agency to ensure the appropriate coordination of responsibilities.

© 2026 National Association of Insurance Commissioners

F. "Company" means a corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.

G. (1) "Consumer" means an individual who seeks to obtain, obtains or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, and about whom the licensee has nonpublic personal information, or that individual's legal representative.

(2) Examples.

(a) An individual who provides nonpublic personal information to a licensee in connection with obtaining or seeking to obtain financial, investment or economic advisory services relating to an insurance product or service is a consumer regardless of whether the licensee establishes an ongoing advisory relationship.

(b) An applicant for insurance prior to the inception of insurance coverage is a licensee's consumer.

(c) An individual who is a consumer of another financial institution is not a licensee's consumer solely because the licensee is acting as agent for, or provides processing or other services to, that financial institution.

(d) An individual is a licensee's consumer if:

(i) (I) The individual is a beneficiary of a life insurance policy underwritten by the licensee;

(II) The individual is a claimant under an insurance policy issued by the licensee;

(III) The individual is an insured or an annuitant under an insurance policy or an annuity, respectively, issued by the licensee; or

(IV) The individual is a mortgagor of a mortgage covered under a mortgage insurance policy; and

(ii) The licensee discloses nonpublic personal information about the individual to a nonaffiliated third party other than as permitted under Sections 22, 23, and 24 of this Act.

(e) Provided that the licensee provides the initial, annual and revised notices under Sections 7, 8, and 13 of this Act to the plan sponsor, group or blanket insurance policyholder or group annuity contractholder, or workers' compensation policyholder, and further provided that the licensee does not disclose to a nonaffiliated third party nonpublic personal financial information about an individual described in Item (i), (ii) or (iii), other than as permitted under ~~Sections 22, 23, or 24~~ of this Act, such an individual is not the consumer of the licensee solely because he or she is:

© 2026 National Association of Insurance Commissioners

(i) A participant or a beneficiary of an employee benefit plan that the licensee administers or sponsors or for which the licensee acts as a trustee, insurer or fiduciary;

(ii) Covered under a group or blanket insurance policy or group annuity contract issued by the licensee; or

(iii) A claimant covered by a workers' compensation plan.

Drafting Note: In states where the workers' compensation self-insurance or workers' compensation state fund coverage is outside the commissioner's jurisdiction, regulators may wish to urge the applicable agency or agencies to promulgate a regulation similar to this Act in order to ensure parity in treatment of workers' compensation plans and to ensure that all workers covered by such plans have privacy protections.

(f) (i) The individuals described in Subparagraph (e)(i) through (iii) of this paragraph are consumers of a licensee if the licensee does not meet all the conditions of Subparagraph (e).

~~(ii) In no event shall the individuals, solely by virtue of the status described in Subparagraph (e)(i) through (iii) above, be deemed to be consumers for purposes of this Act.~~

(g) An individual is not a licensee's consumer solely because he or she is a beneficiary of a trust for which the licensee is a trustee.

(h) An individual is not a licensee's consumer solely because he or she has designated the licensee as trustee for a trust.

H. "Consumer reporting agency" has the same meaning as in Section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

I. "Control" means:

(1) Ownership, control or power to vote twenty-five percent (25%) or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

(2) Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or

(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the commissioner determines.

XX. "Customer" means a consumer who has a continuing relationship with a licensee under which the licensee provides one or more insurance products or services to the consumer that are to be used primarily for personal, family, or household purposes.

J. "De-identified data" means information that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual.

K. (1) "Financial institution" means any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 1843(k)(4)(B**)** of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

© 2026 National Association of Insurance Commissioners

(2) Financial institution does not include:

(a) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 *et seq.*);

(b) The Federal Agricultural Mortgage Corporation or any entity charged and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*); or

(c) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as the institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

L. (1) "Financial product or service" means a product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 1843(k)(4)(B**)** of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.

XX. "Genetic information" means the same as ascribed to it under materials regulated under the Health Insurance Portability and Accountability Act (HIPAA) as specified in 45 CFR 160.103.

M. "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.

© 2026 National Association of Insurance Commissioners

N. (1) "Licensee" means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Insurance Law of this state, [and health maintenance organizations holding a certificate of authority pursuant to Section [insert section] of this state's Public Health Law].

Drafting Note: Add bracketed language if HMOs are licensed under other than insurance statutes and cite appropriate state law.

(2) A licensee is not subject to the notice and opt out requirements for nonpublic personal information set forth in ~~Articles I, II, III and IV of~~ this Act if the licensee is an employee, agent or other representative of another licensee ("the principal") and:

(a) The principal otherwise complies with, and provides the notices required by, the provisions of this Act; and

(b) The licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates in a manner permitted by this Act.

(3) (a) Subject to Subparagraph (b), "licensee" shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only in regard to the excess lines placements placed pursuant to Section [insert section] of this state's laws.

(b) An excess lines broker or excess lines insurer shall be deemed to be in compliance with the notice and opt out requirements for nonpublic personal information set forth in Articles I, II, III and IV of this Act provided:

(i) The broker or insurer does not disclose nonpublic personal information of a consumer to nonaffiliated third parties for any purpose, including joint servicing or marketing under Section 22 of this Act, except as permitted by Section 23 or 24 of this Act; and

(ii) The broker or insurer delivers a notice to the consumer at the time a consumer relationship is established on which the following is printed in 16-point type:

NOTICE OF INFORMATION PRACTICES
"Neither the U.S. brokers that handled this insurance nor the insurers that have underwritten this insurance will disclose nonpublic personal information concerning the buyer to nonaffiliates of the brokers or insurers except as permitted by law."

Drafting Note: References to "excess lines broker" and "excess lines insurer" should be changed as necessary to correspond with the applicable terms used in each state.

O. (1) "Nonaffiliated third party" means any person except:

(a) A licensee's affiliate; or

© 2026 National Association of Insurance Commissioners

(b) A person employed jointly by a licensee and any company that is not the licensee's affiliate (but nonaffiliated third party includes the other company that jointly employs the person).

(2) Nonaffiliated third party includes any company that is an affiliate solely by virtue of the direct or indirect ownership or control of the company by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

P. ~~"Nonpublic personal h~~Health information" means any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of an individual;

(2) The provision of health care to an individual; or

(3) Payment for the provision of health care to an individual.

Q. "Nonpublic personal information" means ~~any personally identifiable information that is linked or reasonably linkable to an identified natural person.~~ Nonpublic personal financial information and nonpublic personal health information. Nonpublic personal information does not include de-identified data or publicly available information.

XX. "Nonpublic personal health information" means health information:

(1) That identifies an individual who is the subject of the information; or

(2) With respect to which there is a reasonable basis to believe that the information could be used to identify an individual.

XX. "Nonpublic personal financial information" means:

(1) Personally identifiable financial information; and

(2) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

R. (1) "Personally identifiable information" means any information:

(a) A consumer provides to a licensee to obtain an insurance product or service from the licensee;

(b) About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

(c) The licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.

© 2026 National Association of Insurance Commissioners

(2) Examples.

(a) Information included. Personally identifiable information includes:

(i) Information a consumer provides to a licensee on an application to obtain an insurance product or service;

(ii) Account balance information and payment history;

(iii) The fact that an individual is or has been one of the licensee's consumers or has obtained an insurance product or service from the licensee;

(iv) Any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer;

(v) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;

(vi) Any information the licensee collects through an Internet cookie (an information-collecting device from a web server); and

(vii) Information from a consumer report.

(b) Information not included. Personally identifiable information does not include:

(i) A list of names and addresses of customers of an entity that is not a financial institution; and

(ii) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.

S. ~~"Opt in" means an affirmative direction by a consumer that authorizes a licensee to disclose the consumer's information.~~

~~T. "Opt out" means a direction by a consumer that the licensee may not disclose nonpublic personal information about the consumer to a nonaffiliated third party, except as permitted under Sections 22,23, or 24 .~~

XX. "Process" or "processing" means any operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

U. (1) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

© 2026 National Association of Insurance Commissioners

(a) Federal, state or local government records;

(b) Widely distributed media; or

(c) Disclosures to the general public that are required to be made by federal, state or local law.

(2) Reasonable basis. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

(a) That the information is of the type that is available to the general public; and

(b) Whether an individual can direct that the information not be made available to the general public and, if so, that the licensee's consumer has not done so.

(3) Examples.

(a) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(b) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(c) Reasonable basis.

(i) A licensee has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(ii) A licensee has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the licensee has located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

V. "Reasonable opportunity" means any of the following:

(1) The licensee mails the notices required to the ~~consumer~~ customer and allows the ~~consumer~~ customer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within sixty (60) days from the date the licensee mailed the notices;

(2) Where a ~~consumer~~ customer agrees to receive the notices required by this Act electronically in accordance with UETA [insert state electronic transactions act statute],

© 2026 National Association of Insurance Commissioners

the licensee allows the ~~consumer~~ customer to opt out by any reasonable means at any time; or

(3) For an isolated transaction, such as providing the ~~consumer~~ customer with an insurance quote, the licensee provides the notices required by this Act at the time of the transaction and requests that the ~~consumer~~ customer decide, as a necessary part of the transaction.

X. "Sale" or "selling" means the exchange of nonpublic personal information for monetary or other valuable consideration. A licensee does not sell nonpublic personal information when:

(1) The disclosure is to a third party for the purpose of or in support of providing a product or service requested ~~by~~ for the consumer.

(2) A licensee provides information to or receives anything of value from an insurance support organization, statistical agent, or reinsurer;

(3) A licensee provides nonpublic personal information to an affiliate, non-affiliated third party, or to a financial institution with which the licensee performs joint marketing;

(4) The business transfers to a third party the nonpublic personal information as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction in which the party assumes control of all or part of the licensee's assets; or

(5) A consumer uses or directs the business to (i) disclose nonpublic personal information; or (ii) interact with one or more third parties including but not limited to referrals to other licensees.

Y. "Sensitive Personal Information" means ~~personally identifiable~~ "nonpublic personal information" about a consumer that includes:

(1) Racial or ethnic origin, religious beliefs, sexual orientation, or citizenship or citizenship status; or

(2) Genetic information or biometric data that ~~may be~~ is processed for the purpose of uniquely identifying an individual.

Z. (1) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on ~~personal data~~ nonpublic personal information obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests.

(2) "Targeted advertising" does not include:

(a) Online advertisements based on activities within a Licensee's own websites or online applications;

(b) Online advertisements based on the context of a consumer's current search

© 2026 National Association of Insurance Commissioners

query, visit to a website, or online application;

(c) Online advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(d) Processing Nonpublic Personal Information solely for measuring or reporting advertising performance, reach, or frequency.

AA. "Third party service provider" ~~or "third party"~~ means a person or entity not otherwise defined as a licensee or affiliate of a licensee that:

(1) Provides services to the licensee; and

(2) Maintains, processes or otherwise is permitted access to nonpublic personal information through its provisions of services to the licensee.

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Section 5. Third-Party Service Provider Arrangements

A. Contract Requirements.

A licensee that discloses a consumer's nonpublic personal information to a third-party service provider shall enter into a written contract with the third-party service provider that:

(1) Prohibits the third-party service provider from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless processing is necessary to comply with the law or a valid and binding order of a governmental body, in which case the third-party service provider must notify the licensee within 48 hours unless prohibited by law;

(2) Requires the third-party service provider to delete, destroy, de-identify or return all nonpublic personal information to the licensee when requested by the licensee; or to delete nonpublic personal information after it is no longer necessary to fulfill a legal requirement or to meet the record retention requirements of the licensee or third-party service provider, and to notify the licensee of the action taken;

(3) Requires the third-party service provider to notify the licensee if it can no longer comply with its obligations under this contract and provides the licensee with a right to terminate the contract;

~~(4) Requires that any contract between a third-party service provider and a subcontractor with access to a consumer's nonpublic personal information must contain provisions no less protective of nonpublic personal information than those contained in the third-party service provider's agreement with the licensee;~~

(5) Requires the third-party service provider to provide assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act;

~~(6) Requires the third-party service provider to implement and maintain administrative,~~

© 2026 National Association of Insurance Commissioners

~~technical, and physical data security practices to protect the nonpublic personal information from unauthorized access, destruction, use, modification, or disclosure;~~

~~(7) Requires the third-party service provider to notify the licensee of a failure to meet the obligations of Subsections (1) to (6) above within 48 hours of discovery by the third-party service provider.~~

B. ~~A licensee that discloses a consumer's nonpublic personal information to a third-party service provider remains fully responsible for compliance with this Act and the handling of nonpublic personal information.~~

© 2026 National Association of Insurance Commissioners

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

A. A ~~consumer~~ customer or former customer may file the following requests with a licensee, which shall be processed in accordance with the following standards:

(1) Within 45 days of receiving an authenticated request from a ~~consumer~~ customer or former customer for their nonpublic personal information, a licensee shall disclose:

(a) All nonpublic personal information about the consumer that is maintained by the licensee ~~or any contracted third-party service provider;~~ and

(b) A list of ~~all~~ categories of third-party service providers to whom the licensee disclosed the consumer's nonpublic personal information.

(2) A customer or former customer may file requests, except for the following which a licensee shall not be required to disclose ~~the following~~:

(a) A ~~consumer's~~ customer or former customer's Social Security Number, driver's license number or other government-issued identification number, financial account number(s), any health insurance or medical identification number, any account password(s), security questions and answers, unique biometric data or other information that could create a high risk of identity theft. The licensee may instead disclose the types of nonpublic personal information maintained by listing each type of nonpublic personal information it has about the consumer;

(b) Duplicative nonpublic personal information, if it is described in a manner reasonably understandable by the consumer and the ~~consumer~~ customer or former customer is offered an opportunity to review the nonpublic personal information for inconsistencies; or

(c) Information that is outside the scope of the request, if the ~~consumer~~ customer or former customer has requested only specified items or categories of information.

(3) The disclosure of the required information shall cover the 12-month period preceding the business' receipt of the authenticated consumer request provided that, a consumer may request that the business disclose the required information beyond the 12-month period, and the business shall be required to provide that information unless doing so proves impossible or would involve a disproportionate effort. A consumer's right to request required information beyond the 12-month period, and a business' obligation to provide that information, shall only apply to personal information collected on or after [XX]. Nothing in this subparagraph shall require a business to keep personal information for any length of time.

B. Correction of nonpublic personal information.

(1) A ~~consumer~~ customer may make an authenticated request for the correction of their nonpublic personal information by filing a request with the licensee that:

© 2026 National Association of Insurance Commissioners

(a) Identifies the specific nonpublic personal information the consumer wishes to correct; and

(b) Provides an explanation of why the nonpublic personal information is incorrect.

(2) Within 45 days of receipt of the request under this subsection, a licensee shall take one of the following actions and notify the ~~consumer~~ customer or former customer:

(a) Correct the nonpublic personal information in dispute as requested by the ~~consumer~~ customer or former customer;

(b) Delete the nonpublic personal information in dispute; or

(c) Deny the request and provide:

(i) The basis for refusal to correct the nonpublic personal information as requested;

(ii) Information about how the ~~consumer~~ customer or former customer may appeal the denial; and

(iii) An explanation of how the appeal will be reviewed and how the ~~consumer~~ customer or former customer will be notified of the decision on appeal.

(3) A licensee may deny a request for correction if:

(a) The nonpublic personal information is accurate and complete and if the licensee provides a process for appeal of the decision;

(b) It is not technically feasible to fulfill the request; or

(c) The nonpublic personal information that is the subject of the request was not created by the licensee, under the control of the licensee, or otherwise is not maintained in an accessible operational system to the licensee, unless, at the discretion of the licensee:

(i) there is a reasonable basis to believe that the originator of the nonpublic personal information is no longer available to act on the requested correction,

(ii) the consumer has independently demonstrated the information is incorrect, AND

(iii) Licensee correction of the information does not violate any existing laws.

C. Deletion of nonpublic personal information.

(1) Within ~~45~~ 90 days of an authenticated request from a ~~consumer~~ customer or former customer, a licensee shall delete the nonpublic personal information about the ~~consumer~~ customer or former customer that is maintained by the licensee or direct a

© 2026 National Association of Insurance Commissioners

third-party service provider to delete the nonpublic personal information on the licensee's behalf.

(2) The licensee is not required to delete nonpublic personal information if:

(a) The licensee is required by law or regulation to retain the nonpublic personal information;

(b) The nonpublic personal information may be necessary to perform the contract or service requested by or benefiting the consumer;

(c) The information is necessary to comply with a legal obligation; ~~or~~

(d) The information is maintained in reasonable anticipation of a claim or civil or criminal proceeding;

(e) The information is not under the licensee's control and is not maintained in an accessible operational system to the licensee;

(f) Retained data is stored in a backup or archive system solely used for disaster recovery and is not actively used, accessed, or reintroduced into production except under strict conditions; or

(g) Fulfilling the request is not technically feasible due to the specific nonpublic personal information not being locatable or retrievable by the licensee.

(3) ~~A licensee may delay fulfilling a consumer's request, up to 45 days, to delete nonpublic personal information stored on an archived or backup system. A licensee must notify the consumer of such delay.~~ If a business, service provider, or contractor stores personal information on archived or backup systems, it may delay compliance with a customer or former customer's deletion request for that data until the archived or backup system is restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose.

(4) A licensee may delay fulfilling a consumer's request if the nonpublic personal information requested to be deleted is not otherwise reasonably related to a business purpose or otherwise actively utilized by the licensee.

D. Request and Response Procedures

(1) Except as provided in Subsection D(1)(b), a licensee shall respond to requests submitted under this section within 45 days in the following manner:

(a) A licensee may use its secure communications portal to authenticate requests from consumers holding current accounts with the licensee, unless the licensee has reason to believe the request has been submitted through an account that has been compromised. Otherwise, the licensee may use methods that are commercially reasonable, but not unduly burdensome, to authenticate the identity of the person making the request and to verify that this person is either:

(i) The ~~consumer~~ customer or former customer;

(ii) A person acting with the ~~consumer's~~ customer or former customer's written authorization, including but not limited to a valid power of

© 2026 National Association of Insurance Commissioners

attorney;

(iii) The parent or legal guardian of a ~~consumer~~ customer or former customer who is a minor, except where the information relates to health insurance claims in circumstances where the child has a legal right to obtain the services in question without the parent's or guardian's consent;

(iv) The legal guardian or other person authorized by law to act on behalf of an incapacitated ~~consumer~~ customer or former customer; or

(v) The personal representative or other person authorized by law to act on behalf of a deceased ~~consumer~~ customer or former customer.

(b) A licensee is required to notify the ~~consumer~~ customer or former customer if either of the following prevents the licensee from complying with the request:

(i) The specific nonpublic personal information at issue is not locatable or retrievable by the licensee; or

Drafting Note: Examiners should review licensees' notifications to consumers regarding nonpublic personal information that is not locatable or retrievable by the licensee and its justifications for irretrievability during Market Conduct and/or IT Exams.

(ii) The licensee is unable to verify the request after requesting that the ~~consumer~~ customer or former customer provide additional information necessary to authenticate the identity of the consumer and authenticate the ~~consumer's~~ customer or former customer's request.

(c) If a licensee declines the ~~consumer's~~ customer or former customer's request, the licensee shall inform the ~~consumer~~ customer or former customer of the basis for declining the request and provide instructions for how to request review of the decision.

(d) Upon receipt of a request from a customer or former customer, a licensee shall have 15 days to authenticate the request as set forth in Section D(1)(a). If the licensee is unable to authenticate the request after 15 days it shall deny the request and shall inform the requestor. Once a request is authenticated, a licensee shall complete the request within the time set forth in Subsection D.

(2) There shall be ~~no cap on the number~~ limit of 2 requests to correct or delete nonpublic personal information per calendar year.

(3) If a ~~consumer~~ customer or former customer disagrees with a licensee's refusal to correct or delete nonpublic personal information per the ~~consumer's~~ customer or former customer's request, the ~~consumer~~ customer or former customer shall be permitted to file with the licensee:

© 2026 National Association of Insurance Commissioners

(a) A concise statement setting forth why the ~~consumer~~ customer or former customer disagrees with the licensee's refusal and what the ~~consumer~~ customer or former customer thinks is the correct, relevant or fair information; and

(b) The licensee shall maintain the statement with the disputed nonpublic personal information and allow ~~anyone reviewing~~ the following persons or entities ~~the disputed nonpublic personal information~~ to be made aware of the dispute and have access to the ~~consumer's~~ customer or former customer's statement:

(i) persons or entities that receive or use the disputed nonpublic personal information for a purpose that would be affected by accuracy; and

(ii) have a legitimate need to know for compliance or processing purposes.

© 2026 National Association of Insurance Commissioners

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7. Initial and Subsequent Delivery Notice of Information Practices to Consumers Required

A. Initial Delivery of Notice. A licensee shall provide a clear and conspicuous notice that accurately reflects its privacy policies and practices ~~to all consumers no later than when the licensee obtains access to the consumer's nonpublic personal information, except that a licensee may provide the initial notice within a reasonable time after access to the consumer's nonpublic personal information if:~~ no later than when the licensee processes the consumer's nonpublic personal information, except that a licensee may provide initial notice within a reasonable time after access to the consumer's nonpublic personal information if:

(1) ~~Obtaining access to~~ Processing the consumer's nonpublic personal information is not at the consumer's election and the licensee follows the Notice of Information Practices previously sent to the consumer; or

(2) Providing notice when the licensee ~~obtains access to~~ processes the consumer's nonpublic personal information would substantially delay the consumer's transaction and the consumer agrees to receive the notice at a later time.

XX. Where a licensee did not directly collect nonpublic personal information from the consumer and the consumer relationship arose through a claim, beneficiary designation, assignment, or other transaction not initiated by the consumer's own selection of the licensee, the licensee shall provide the notice required under this Section at the time it first collects or obtains access to the consumer's nonpublic personal information in connection with that claim, assignment, or transaction, regardless of whether the consumer selected the licensee. Where direct delivery to the consumer is not practicable, the licensee may satisfy this requirement by delivering notice through the policyholder, contract holder, or other intermediary through whom the claim or transaction was submitted, consistent with the delivery mechanism described in Section 14.

B. Subsequent Delivery of Notice

When a consumer with an existing relationship with a licensee obtains a new insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, the licensee satisfies the initial notice requirements of Subsection A of this section as follows:

(1) The licensee may provide a revised notice, under Section 13 , that covers the consumer's new insurance product or service; or

(2) If the initial, revised or annual notice that the licensee most recently provided to that consumer was accurate with respect to the new insurance product or service, the licensee does not need to provide a new notice of information practices under Subsection A of this section.

C. For purposes of this section:

(1) "Not at consumer's election" includes the scenario where a licensee acquires or is assigned a consumer's policy from another financial institution or residual market

© 2026 National Association of Insurance Commissioners

mechanism and the consumer does not have a choice about the licensee's acquisition or assignment.

(2) "Substantially delay the consumer's transaction" includes the scenario where the licensee and the individual agree over the telephone or electronically, via licensee website chat features, email, and text message communications, to enter into a consumer relationship involving prompt delivery of the insurance product or service but does not include the scenario where the relationship is initiated in person ~~at the licensee's office or~~ through other means by which the consumer may view the notice, such as on a website.

Section 8. Annual Notice of Information Practices to Consumers Required

General rule. A licensee shall provide a clear and conspicuous notice to ~~consumers~~ customers that accurately reflects its privacy policies and practices at least once in any period of twelve (12) consecutive months. A licensee may define the twelve-consecutive-month period, during which that relationship exists, but the licensee shall apply it to the ~~consumer~~ customer on a consistent basis.

A. Example. A licensee provides a notice annually if it defines the twelve-consecutive-month period as a calendar year and provides the annual notice to the ~~consumer~~ customer once in each calendar year following the calendar year in which the licensee provided the initial notice. For example, if a ~~consumer~~ customer opens an account on any day of year 1, the licensee shall provide an annual notice to that consumer by December 31 of year 2.

(1) Exceptions.

(1) A licensee that provides nonpublic personal information to nonaffiliated third parties only in accordance with Sections 22, 23, or 24 and has not changed its policies and practices with regard to disclosing Nonpublic Personal Information from the policies and practices that were disclosed in the most recent disclosure sent to consumers in accordance with this section or Section 7 shall not be required to provide an annual disclosure under this section until such time as the licensee fails to comply with any criteria described in this paragraph.

(2) A licensee is not required to provide notice if the licensee no longer has access to the consumer's nonpublic personal information.

(2) For the purposes of this Act, a ~~-~~licensee no longer has an obligation to continue to notify a consumer if the licensee's records do not contain a valid address. An address is deemed invalid if electronic or regular mail sent to that address by the licensee has been returned as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.

© 2026 National Association of Insurance Commissioners

Section 9. Information to be Included in Notices of Information Practices

A. General rule. The initial, annual and revised Notice of Information Practices that a licensee provides under Sections 7,8, and 13 shall include each of the following items of information, in addition to any other information the licensee wishes to provide, that applies to the licensee and to the consumers to whom the licensee sends its Notice of Information Practices:

(1) The categories of nonpublic personal information that the licensee collects, including, but not limited to, whether information is collected from the consumer, through the consumer's transactions with affiliates or nonaffiliated third parties, or consumer reporting agencies;

(2) The categories of nonpublic personal information that the licensee discloses, including at least one example in each category. Categories may include, but are not limited to, application information, transaction information, or consumer reports;

(3) The categories of affiliates and nonaffiliated third parties, and the types of business in which they engage, to whom the licensee discloses nonpublic personal information, other than those parties to whom the licensee discloses information under Sections 22, 23, and 24. The types of businesses may be described in general terms only if the licensee uses illustrative examples of each significant line of business;

(4) An explanation of the consumer's right under Section 12 to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;

(5) An explanation of the consumer's rights with regard to the sale of nonpublic personal information and disclosure of sensitive personal information pursuant to Sections 20 and 21;

(6) A description of the consumer's options to request access, correction, or deletion of nonpublic personal information about the consumer as established under this Act and the instructions for exercising such options;

(7) Any disclosures that the licensee makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);

(8) The licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; by

(a) Describing in general terms who is authorized to have access to the information; and

(b) Stating whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance with the licensee's policy. The licensee is not required to describe technical information about the safeguards it uses; and

(c) Any disclosure that the licensee makes as authorized under Section 22, 23, or

© 2026 National Association of Insurance Commissioners

24, except that the licensee is not required to list those exceptions in the initial or annual Notice of Information Practices required by Sections 7 and 8. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.

B. The licensee's notice may include:

(1) Categories of nonpublic personal information that the licensee reserves the right to disclose in the future, but does not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the right in the future to disclose, but to whom the licensee does not currently disclose, nonpublic personal information.

C. Exceptions:

If a licensee does not disclose, and does not reserve the right to disclose, nonpublic personal information about consumers to affiliates or nonaffiliated third parties except as authorized under Sections22, 23, or 24, the licensee shall state that in its notice, in addition to the information it shall provide under Subsections A(1) and A(8) and Subsection B of this section.

D. Sample Clauses and Federal Model Privacy Form.

(1) Licensees are not required to use any prescribed clauses or model form.

(2) The commissioner may determine that a Licensee's use of any of the following constitutes compliance with this Act:

(a) Sample clauses illustrating some of the notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner;

(b) Model forms illustrating notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner; or

(c) The Federal Model Privacy Forms are included in Appendix A and Appendix B, of this Act.

Section 10. Short Form Initial Notice of Information Practices

A. A licensee may satisfy the initial notice requirements in Sections 7A and 13A by providing a Short Form Initial Notice of Information Practices at the same time the licensee delivers an opt-out notice as required in Section 12 if:

(1) The licensee provides the consumer a reasonable means to obtain its Notice of Information Practices; and

© 2026 National Association of Insurance Commissioners

(2) The licensee provides the Notice of Information Practices upon request.

B. A Short Form Initial Notice of Information Practices shall meet all of the following requirements.

(1) Be clear and conspicuous;

(2) State that the licensee's Notice of Information Practices is available upon request;

(3) Explain the reasonable means to obtain the licensee's Notice of Information Practices;

~~(4) Contain contact information for the commissioner; and~~

(5) Describe how the consumer can request access to or correction of their nonpublic personal information.

C. For purposes of this section "reasonable means to obtain the licensee's Notice of Information Practices" includes:

(1) Providing a toll-free telephone number that the consumer may call to request the notice;

(2) Providing a website or other electronic medium that is easily accessible by the consumer; or

(3) Maintaining copies of the notice at the licensee's place of business to be provided upon request.

Section 11. Form of Opt-In Notice to Consumers and Opt-In Methods

A. If a licensee is required to provide an opt-int notice under Sections 20 or 21, it shall provide a clear and conspicuous notice to each of its consumers that accurately explains the information proposed to be disclosed, the use of that information, and the consumer's option to opt in to that use. The notice shall state:

(1) The licensee discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;
(2) The consumer has the option to opt in to that disclosure; and
(3) A reasonable means by which the consumer may exercise the option to opt in.

B. The licensee shall not disclose that information to a nonaffiliated third party unless the consumer has affirmatively opted in to the use.

C. The opt-in must be an affirmative act by the consumer. The licensee cannot deem a failure to respond as an opt-in or use pre-checked boxes.

D. The opt-in should be obtained separately from any other communication or consent.

E. The opt-in may be revoked at any time by the consumer.

© 2026 National Association of Insurance Commissioners

Section 12. Form of Opt-Out Notice to Consumers and Opt-Out Methods

A. (1) If a licensee is required to provide an opt-out notice, it shall provide a clear and conspicuous notice to each consumer that accurately explains the right to opt out under that section. To the extent applicable, the notice shall state:

(a) That the licensee discloses ~~or reserves the right to disclose~~ nonpublic personal information about its consumer to a nonaffiliated third party;

(b) That the consumer has the right to opt out of that disclosure; and

(c) A reasonable means by which the consumer may exercise the opt-out right.

(2) Requirements

(a) A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if the licensee:

(i) Identifies all of the categories of nonpublic personal information it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to whom the licensee discloses the information, as described in Section 9A(2) and (3), and states the consumer can opt out of the disclosure of that information; and

~~(ii) Identifies the insurance products or services the consumer obtains from the licensee, either singly or jointly, to which the opt-out would apply.~~

(b) A licensee provides a reasonable means to exercise an opt-out right if it:

(i) Designates check-off boxes in a prominent position on the relevant forms with the opt-out notice;

(ii) Includes a reply form together with the opt-out notice;

(iii) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the licensee's website, ~~if the consumer agrees to the electronic delivery of information~~; or

(iv) Provides a toll-free telephone number that consumers may call to opt out.

(c) A licensee does not provide a reasonable means of opting out if:

(i) The only means of opting out is for the consumer to write a letter to the licensee to exercise their opt-out right; or

(ii) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the licensee provided with the initial notice but did not include with the subsequent notice.

(d) A licensee may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

© 2026 National Association of Insurance Commissioners

B. A licensee may provide the opt-out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 7.

C. If a licensee provides the opt-out notice after it provides the initial notice, the licensee shall include a copy of the initial notice with the opt-out notice in writing or, if the consumer agrees, electronically.

D. Joint relationships.

(1) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt-out notice. The licensee's opt-out notice shall explain how the licensee will treat an opt-out direction by a joint consumer (as explained in Paragraph (2) of this subsection).

(2) Any of the joint consumers may exercise the right to opt out. The licensee may either:

(a) Treat an opt-out direction by a joint consumer as applying to all of the associated joint consumers; or

(b) Permit each joint consumer to opt out separately.

(3) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all the joint consumers.

(4) A licensee may not require all joint consumers to opt out before it implements any opt-out direction.

E. A licensee shall comply with a consumer's opt-out direction as soon as reasonably practicable but no later than 10 business days after the licensee receives it.

F. A consumer may exercise the right to opt out at any time. A consumer's direction to opt-out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.

Section 13. Revised Notice of Information Practices

A. Except as otherwise authorized in this Act, a licensee shall not, directly or through an affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that the licensee provided to that consumer under Section 7, unless:

(1) The licensee has provided to the consumer a clear and conspicuous revised notice that accurately describes its policies and practices;

(2) The licensee has provided to the consumer a new opt-out notice;

(3) The licensee has given the consumer a reasonable opportunity, before the licensee discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(4) The consumer does not opt out.

B. Examples.

© 2026 National Association of Insurance Commissioners

(1) Except as otherwise permitted by Sections 19, 20 and 21, a licensee shall provide a revised notice before it:

(a) Discloses a new category of nonpublic personal information to any nonaffiliated third party; or

(b) Discloses nonpublic personal information to a new category of nonaffiliated third party.

(2) A revised notice is not required if the licensee discloses nonpublic personal information to a new nonaffiliated third party that the licensee adequately described in its prior notice.

Section 14. Notice of Information Practices to Group Policyholders

Unless a licensee is providing notices of information practices directly to covered individuals described in Section 4G)2)(e)(i), (ii) or (iii), a licensee shall provide initial, annual and revised notices to the plan sponsor, group or blanket insurance policyholder or group annuity contract holder, or workers' compensation policyholder, in the manner described in Sections 7 through 13 of this Act, describing the licensee's privacy practices with respect to nonpublic personal information about individuals covered under the policies, contracts or plans. Compliance with this section satisfies the licensees initial, annual and renewal Notice of Information Practices as required by Sections 7 and 8 and delivery provisions of Section 15.

Section 15. Delivery

A. A licensee shall provide any notices that this Act requires so that each consumer can reasonably be expected to receive or have access to actual notice in writing or, if the consumer interacts with the licensee online or in some other electronic fashion, electronically.

B. (1) A licensee may reasonably expect that a consumer will receive actual notice if the licensee:

(a) Hand-delivers a printed copy of the notice to the consumer;

(b) Mails a printed copy of the notice to the last known address of the consumer separately, or in a policy, billing or other written communication;

(c) For a consumer who conducts transactions electronically, in accordance with UETA (insert state electronic transactions act statute), posts the notice on the electronic site, including via mobile applications, and requires the consumer to acknowledge receipt of the notice as a necessary step, meaning the notice must be presented and acknowledged at or before contract initiation, to obtaining a particular insurance product or service;

(i) The notice should be posted in a manner that enables a consumer to print or save it using programs or apps that are widely available and free of charge.

© 2026 National Association of Insurance Commissioners

(ii) Notice is available electronically as long as it is in force.

(d) For an isolated transaction with a consumer, such as the licensee providing an insurance quote or selling the consumer travel insurance, posts the notice and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular insurance product or service.

(i) Transaction in this instance does not include pre-sale quotes or informational quotes, triggering the acknowledgement requirement.

(e) Provides the notice by any other means authorized by the commissioner.

(2) Examples of unreasonable expectation of actual notice. A licensee may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:

(a) Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or

(b) Sends the notice via electronic mail to a consumer who does not otherwise communicate with the licensee electronically.

C. A licensee may reasonably expect that a ~~consumer~~ customer will receive actual notice of the licensee's Notice of Information Practices if:

(1) The ~~consumer~~ customer uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or

(2) The ~~consumer~~ customer has requested that the licensee refrain from sending any information regarding the ~~consumer~~ customer relationship, and the licensee's current privacy notice remains available to the ~~consumer~~ customer upon request.

D. A licensee may not provide any notice required by this Act solely by orally explaining the notice, either in person or over the telephone.

E. A licensee may provide a joint notice from the licensee and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the licensee and the other institutions. A licensee also may provide a notice on behalf of another financial institution.

F. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of Sections 7A, 8A and 13A, respectively, by providing one notice to those consumers jointly.

© 2026 National Association of Insurance Commissioners

ARTICLE V. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 16. General Rules for Use and Disclosure of Nonpublic Personal Information

A. Use and Disclosure

(1) A licensee may use and disclose nonpublic personal information about a consumer for purposes of processing a business transaction requested or authorized by the consumer.

(2) A licensee may disclose nonpublic personal information ~~with~~ to affiliates, provided the affiliates' use and disclosure comply with this Act.

(3) A licensee ~~shall not~~ may disclose nonpublic personal information to a nonaffiliated third party except as permitted by this Act.

(4) This section applies to nonpublic personal information collected before and after a consumer exercises an opt-out right under Section 19 or an opt-in right under Sections 20 and 21.(5) If a consumer submits an opt-out request during a transaction and the requested information is necessary to complete that transaction, the licensee shall:

(a) Inform the consumer that the transaction cannot be completed without the information; and

(b) Confirm whether the consumer wishes to proceed.

B. Limits on Disclosure**.** Except as provided by Section 16A(1), before disclosing a consumer's nonpublic personal information to a nonaffiliated third party, whether directly or through an affiliate, a licensee shall:

(1) Provide the initial notice required by Section 7;

(2) Provide a clear and conspicuous notice to the consumer that details, as relevant:

(a) The consumer's right to opt out of disclosure for targeted advertising under Section 19;

(b) The consumer's option to opt in to the sale of nonpublic personal information under Section 20; or

(c) The consumer's option to opt in to the disclosure of sensitive personal information Section 21.

(3) Provide a reasonable opportunity for the consumer to exercise any applicable opt-out right before disclosure; and

(4) Obtain and document the consumer's opt-in or opt-out election, as applicable.

Section 17. Limits on Redisclosure and Reuse of Nonpublic Personal Information

A. If a licensee receives nonpublic personal information from a nonaffiliated third-party service provider, financial institution, or third party licensee under an exception in Article

© 2026 National Association of Insurance Commissioners

VI of this Act,

the licensee may use and disclose the information in the ordinary course of business to carry out the activity covered by the exception under which the licensee received the information.

B. (1) If a licensee receives nonpublic personal information from a nonaffiliated third-party service provider other than under an exception in Article VI of this Act, the licensee may disclose the information only to the following, provided the disclosure is consistent with this Act:

(a) Affiliates of the third party-service provider from which the licensee received the information; and

(b) Affiliates of the licensee who may disclose the information only to the extent that the disclosure would be permissible by the licensee pursuant to this Act.

(2) Example. If a licensee obtains a customer list from a nonaffiliated third-party service provider outside of the exceptions in Article VI:

(a) The licensee may use that list for its own purposes consistent with this Act; and

(b) The licensee may disclose that list to another nonaffiliated third-party service provider only as permitted by this Act.

C. If a licensee discloses nonpublic personal information to a nonaffiliated third-party service provider under an exception in S Article VI of this Act, the third party-service provider:

(1) May disclose the information to the licensee's affiliates; and

(2) May disclose and use the information in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

D. If a licensee discloses nonpublic personal information to a nonaffiliated third-party service provider other than under an exception in Article VI of this Act, the third-party service provider may disclose the information only:

(1) To the licensee's affiliates who may disclose the information only to the extent that it would be permissible for the licensee to disclose the information pursuant to this Act: and

(2) To any other person, if the disclosure would be lawful if the licensee made it directly to that person.

© 2026 National Association of Insurance Commissioners

Section 18. Limits on Sharing Access Number or Access Code Information for Marketing Purposes

A. A licensee shall not, directly or through an affiliate, disclose, other than to a consumer reporting agency, a policy number or similar form of access number or access code for a consumer's policy or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

B. Exceptions. Subsection A of this section does not apply if a licensee discloses a policy number or similar form of access number or access code:

(1) To the licensee's service provider solely in order to perform marketing for the licensee's own products or services, as long as the service provider is not authorized to directly initiate charges to the account;

(2) To a licensee who is a producer solely in order to perform marketing for the licensee's own products or services; or

(3) To a participant in an affinity or similar program where the participants in the program are identified to the consumer when the consumer enters into the program.

(4) Where the policy number, or similar form of access number or access code, is in an encrypted form, as long as the licensee does not provide a means to decode the access number or access code.

Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted Advertising

A. Except as otherwise authorized in this Act, a licensee may not, directly or through any affiliate, disclose for the purpose of targeted advertising any nonpublic personal information about a consumer to a nonaffiliated third party unless the consumer has been provided clear and conspicuous notice and a reasonable opportunity to opt out of targeted advertising in accordance with the requirements of Section 12 of this Act, completed through the licensee's website.

B. A licensee shall act on a consumer's request to opt out within 15 days of receipt.

C. A licensee is under no obligation to obtain additional information to execute the opt-out request.

D. A licensee may not solicit the consumer to change their election to opt out for twelve months.

E. A consumer has the right to opt out at any time.

F. A licensee shall not be obligated to act on any request where the personal data in the opt-out request does not match the licensee's records.

Section 20. Limits on Sale of Nonpublic Personal Information

Before a licensee may sell nonpublic personal information:

A. The licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

© 2026 National Association of Insurance Commissioners

B. The consumer must affirmatively opt in to the sale of their nonpublic personal information.

Section 21. Limits on Disclosure of Sensitive Personal Information

A. Except as provided by Subsection B below, a licensee may disclose a consumer's sensitive personal information only for those purposes and uses identified in Article VI and as expressly permitted or required by Article VI or other provisions of this Act.

B. Before a licensee may disclose a consumer's sensitive personal information for purposes other than those specified in subsection A of this section:

(1) A licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

(2) The consumer ~~must affirmatively opt in to~~ may opt out of the disclosure of their sensitive personal information.

© 2026 National Association of Insurance Commissioners

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 22. Exception to Opt-Out and Opt-In Requirements for Disclosure of Nonpublic Personal Information for Service Providers and Joint Marketing

A. General rule.

(1) The opt-out requirements in Sections 12 and 19 do not apply when a licensee provides nonpublic personal information to a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf, if the licensee:

(a) Provides the initial notice in accordance with Section7; and

(b) Enters into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in Sections 23 or 24 in the ordinary course of business to carry out those purposes.

(2) Example. If a licensee discloses nonpublic personal information under this section to a financial institution with which the licensee performs joint marketing, the licensee's contractual agreement with that institution meets the requirements of Paragraph (1)(b) of this subsection if it prohibits the institution from disclosing or using the nonpublic personal information except as necessary to carry out the joint marketing or under an exception in Sections 23 or 24 in the ordinary course of business to carry out that joint marketing.

B. Service may include joint marketing. The services a nonaffiliated third party performs for a licensee under Subsection A of this section may include marketing of the licensee's own products or services or marketing of financial products or services offered pursuant to joint agreements between the licensee and one or more financial institutions.

C. Definition of "joint agreement." For purposes of this section, "joint agreement" means a written contract pursuant to which a licensee and one or more financial institutions jointly offer, endorse or sponsor a financial product or service.

Section 23. Exceptions to Notice and Opt-Out and Opt-In Requirements for Disclosure of Nonpublic Personal Information for Processing and Servicing Transactions

A. Exceptions for processing transactions at consumer's request. The requirements for initial notice in Section 7A(2), the opt-out in Sections 12 and 19, and service providers and joint marketing in Section 22 do not apply if the licensee discloses nonpublic personal information as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Servicing or processing an insurance product or service that a consumer requests or authorizes;

© 2026 National Association of Insurance Commissioners

(2) Maintaining or servicing the consumer's account with a licensee, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity;

(3) A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer; or

(4) Reinsurance or stop loss or excess loss insurance.

B. "Necessary to effect, administer or enforce a transaction" means that the disclosure is:

(1) Required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or

(2) Required, or is a usual, appropriate or acceptable method:

(a) To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer's account in the ordinary course of providing the insurance product or service;

(b) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

(c) To provide a confirmation, statement or other record of the transaction, or information on the status or value of the insurance product or service to the consumer or the consumer's agent or broker;

(d) To accrue or recognize incentives or bonuses associated with the transaction that are provided by a licensee or any other party;

(e) To underwrite insurance at the consumer's request or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects or as otherwise required or specifically permitted by federal or state law; or

(f) In connection with:

(i) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited or otherwise paid using a debit, credit or other payment card, check or account number, or by other payment means;

(ii) The transfer of receivables, accounts or interests therein; or

(iii) The audit of debit, credit or other payment information.

© 2026 National Association of Insurance Commissioners

Section 24. Other Exceptions to Notice and Opt-Out and Opt-In Requirements for Disclosure of Nonpublic Personal Information

A. Exceptions to opt out requirements. The requirements for initial notice to consumers in Section 7A(2), the opt-out in Sections 12 and 19, and service providers and joint marketing in Section 22 do not apply when a licensee discloses nonpublic personal information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

(2) (a) To protect the confidentiality or security of a licensee's records pertaining to the consumer, service, product or transaction;

(b) To protect against or prevent actual or potential fraud or unauthorized transactions;

(c) For required institutional risk control or for resolving consumer disputes or inquiries;

(d) To persons holding a legal or beneficial interest relating to the consumer; or

(e) To persons acting in a fiduciary or representative capacity on behalf of the consumer;

(f) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted nonpublic personal information.

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating a licensee, persons that are assessing the licensee's compliance with industry standards, and the licensee's attorneys, accountants and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the federal Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, the Securities and Exchange Commission, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance authority, and the Federal Trade Commission), self-regulatory organizations or for an investigation on a matter related to public safety;

(5) (a) To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or

(b) From a consumer report reported by a consumer reporting agency;

© 2026 National Association of Insurance Commissioners

(6) In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of the business or unit;

(7) (a) To comply with federal, state or local laws, rules and other applicable legal requirements;

(b) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities; or

(c) To respond to judicial process or government regulatory authorities having jurisdiction over a licensee for examination, compliance or other purposes as authorized by law; or

(8) For purposes related to the replacement of a group benefit plan, a group health plan, a group welfare plan or a workers' compensation plan.

B. Example of revocation of consent. A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under Section 12F.

Drafting Note: Because the notice requirements of this Act could be a financial burden on a company in liquidation or receivership and negatively impact the ability of the liquidator or receiver to pay claims, regulators may want to consider adding an additional exception providing that licensees in liquidation or receivership are not subject to the notice provisions of this Act.

© 2026 National Association of Insurance Commissioners

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 25. When Authorization Required for Disclosure of Nonpublic Personal Health Information

A. A licensee shall not disclose nonpublic personal health information about a consumer unless an authorization is obtained from the consumer whose nonpublic personal health information is sought to be disclosed.

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee:

(1) Claims administration any processing;

(2) Claims adjustment and management;

(3) Detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity;

(4) Underwriting;

(5) Policy placement or issuance;

(6) Loss control;

(7) Ratemaking and guaranty fund functions;

(8) Reinsurance and excess loss insurance;

(9) Risk management;

(10) Case management;

(11) Disease management;

(12) Quality assurance;

(13) Quality improvement;

(14) Performance evaluation;

(15) Provider credentialing verification;

(16) Utilization review;

(17) Peer review activities;

(18) Actuarial, scientific, medical or public policy research;

(19) Grievance procedures;

© 2026 National Association of Insurance Commissioners

(20) Internal administration of compliance, managerial, and information systems;

(21) Policyholder service functions;

(22) Auditing;

(23) Reporting;

(24) Database security;

(25) Administration of consumer disputes and inquiries;

(26) External accreditation standards;

(27) The replacement of a group benefit plan or workers' compensation policy or program;

(28) Activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit;

(29) Any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services or other applicable laws;

(30) Disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes including subrogation, and

(31) Any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with the legal process.

C. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable

Section 26. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article VII shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer who is the subject of the nonpublic personal health information;

(2) A general description of the types of nonpublic personal health information to be disclosed;

(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

(4) The signature, including electronic signatures, of the consumer who is the subject of the

© 2026 National Association of Insurance Commissioners

nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer may revoke the authorization at any time and the procedure for making a revocation.

(6) Any additional information necessary to comply with HIPAA or any other applicable law.

B. An authorization for the purposes of this Article VII shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article VII at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

E. A signed copy of the authorization shall be provided to the consumer.

Section 27. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer as part of an opt-out notice pursuant to Section 12, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section 25A.

Section 28. Relationship to Federal Rules

A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

This Act shall not apply to nonprofits, such as the National Association of Insurance Commissioners or the National Insurance Crime Bureau, when processing or sharing information solely for investigating criminal or fraudulent insurance acts.

Section 29. Relationship to State Laws

Nothing in this Article shall preempt or supersede existing state law related to medical records, consumer data privacy, health or insurance information privacy.

© 2026 National Association of Insurance Commissioners

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 30. Protection of Fair Credit Reporting Act

Nothing in this Act shall be construed to modify, limit or supersede the operation of the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and no inference shall be made regarding whether information is transaction or experience information under Section 603 of that Act.

Section 31. Nondiscrimination

A. A licensee shall not unfairly discriminate against any consumer because that consumer has opted out from the disclosure of his or her nonpublic personal information pursuant to the provisions of this Act.

B. A licensee shall not unfairly discriminate against a consumer because that consumer has not granted authorization for the disclosure of his or her nonpublic personal health information pursuant to the provisions of this Act.

Section 32. Violation

Drafting Note: Cite state unfair trade practices act or other applicable state law.

Section 33. Severability

If any section or portion of a section of this Act or its applicability to any person or circumstance is held invalid by a court, the remainder of the Act or the applicability of the provision to other persons or circumstances shall not be affected.

Section 34. Individual Remedies

This Act may not be construed to create or imply a private cause of action for violation of its provisions, nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Section 35. Effective Date

A. Effective date. This Act has been effective since November 13, 2000. The amendments to this Act are effective [Insert Effective Date]. In order to provide sufficient time for licensees to establish policies and systems to comply with the amendments to this Act, the commissioner has extended the time for compliance with the amendments to this Act until [Insert Compliance Date].

B. By [Insert Compliance Date], a licensee shall provide an initial notice, as required by Section 7, to any existing consumer who has not previously received a notice that complies with the amendments to this Act.

C. Two-year grandfathering of service agreements. Until [Insert Compliance Date], a contract that a licensee has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf satisfies the provisions of Section 22A(1)(b) of this Act, even if

© 2026 National Association of Insurance Commissioners

the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the licensee entered into the agreement on or before [Insert Compliance Date].

© 2026 National Association of Insurance Commissioners

APPENDIX A – SAMPLE CLAUSES

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A-1–Categories of information a licensee collects (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(1) to describe the categories of nonpublic personal information the licensee collects.

Sample Clause A-1:

We collect nonpublic personal information about you from the following sources:

Information we receive from you on applications or other forms;
Information about your transactions with us, our affiliates or others; and
Information we receive from a consumer reporting agency.

A-2–Categories of information a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use one of these clauses, as applicable, to meet the requirement of Section 9A(2) to describe the categories of nonpublic personal information the licensee discloses. The licensee may use these clauses if it discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-2, Alternative 1:

We may disclose the following kinds of nonpublic personal information about you:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premiums, and payment history"]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your creditworthiness and credit history"].

Sample Clause A-2, Alternative 2:

We may disclose all of the information that we collect, as described [describe location in the notice, such as "above" or "below"].

A-3–Categories of information a licensee discloses and parties to whom the licensee discloses (institutions that do not disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirements of Sections 9A(2) and (3) to describe the

© 2026 National Association of Insurance Commissioners

categories of nonpublic personal information the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses. A licensee may use this clause if the licensee does not disclose nonpublic personal information to any party, other than as permitted by the exceptions in Sections 23 and 24.

Sample Clause A-3:

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

A-4–Categories of parties to whom a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(3) to describe the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information. This clause may be used if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-4:

We may disclose nonpublic personal information about you to the following types of third parties:

Financial service providers, such as [provide illustrative examples, such as “life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents”];

Non-financial companies, such as [provide illustrative examples, such as “retailers, direct marketers, airlines, and publishers”]; and

Others, such as [provide illustrative examples, such as “non-profit organizations”].

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

A-5–Service provider/joint marketing exception
A licensee may use one of these clauses, as applicable, to meet the requirements of Section 9A(2) related to the exception for service providers and joint marketers in Section 22. If a licensee discloses nonpublic personal information under this exception, the licensee shall describe the categories of nonpublic personal information the licensee discloses and the categories of third parties with which the licensee has contracted.

Sample Clause A-5, Alternative 1:

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as “your name, address, social security number, assets, income, and beneficiaries”];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as “your policy coverage, premium, and payment history”]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as “your

© 2026 National Association of Insurance Commissioners

creditworthiness and credit history"].

Sample Clause A-5, Alternative 2:

We may disclose all of the information we collect, as described [describe location in the notice, such as "above" or "below"] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

A-6–Explanation of opt- out right (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(4) to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. The licensee may use this clause if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-6:

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [describe a reasonable means of opting out, such as "call the following toll-free number: (insert number)].

A-7–Confidentiality and security (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(8) to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A-7:

We restrict access to nonpublic personal information about you to [provide an appropriate description, such as "those employees who need to know that information to provide products or services to you"]. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

© 2026 National Association of Insurance Commissioners

APPENDIX B – FEDERAL MODEL PRIVACY FORM

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the Federal Model Privacy Form, if the Form is accurate for each institution that uses the Form. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A. General Instructions

1. How the Model Privacy Form is used.

(a) The Model Form may be used, at the option of a "licensee", including a group of licensees or other financial institutions that use a common privacy notice, to meet the content requirements of the privacy notice and opt-out notice set forth in [insert citation for sections of statute or regulation sections that parallel Sections 9and 11 of the NAIC *Privacy of Consumer InformationAct*]

(b) The Model Form is a standardized form, including page layout, content, format, style, pagination, and shading. Licensees seeking to obtain the safe harbor through use of the Model Form may modify it only as described in these Instructions.

(c) Note that disclosure of certain information, such as assets, income, and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act (FCRA), codified at 15 U.S.C. §§ 1681-1681x, such as a requirement to permit a consumer to opt out of disclosures to affiliates, or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.

(d) The word "consumer" may be replaced by the word "member," whenever it appears in the Model Form, as appropriate.

2. The Contents of the Model Privacy Form

The Model Form consists of two pages, which may be printed on both sides of a single sheet of paper or may appear on two separate pages. Where a licensee provides a long list of licensees or financial institutions at the end of the Model Form in accordance with Instruction B3(a)(i), or provides additional information in accordance with Instruction B3(c) and such list or additional information exceeds the space available on Page Two of the Model Form, such list or additional information may extend to a third page.

(a) Page One. The first page consists of the following components:

(1) Date last revised (upper right-hand corner)
(2) Title
(3) Key frame (Why? What? How?)
(4) Disclosure table ("Reasons we can share your personal information")
(5) "To limit our sharing" box, as needed, for the licensee's opt-out information
(6) "Questions" box, for customer service contact information
(7) Mail-in opt-out form, as needed

(b) Page Two. The second page consists of the following components:

© 2026 National Association of Insurance Commissioners

(1) Heading (Page 2)
(2) Frequently Asked Questions ("Who we are" and "What we do")
(3) Definitions
(4) "Other important information" box, as needed

3. The format of the Model Privacy Form.

The format of the Model Form may be modified only as described below.

(a) Easily readable type font. Licensees that use the Model Form must use an easily readable type font. While a number of factors together produce easily readable font, licensees are required to use a minimum of 10-point font (unless otherwise expressly permitted in these Instructions) and sufficient spacing between lines.

(b) Logo. A licensee may include a corporate logo on any page of the notice, so long as it does not interfere with the readability of the Model Form or the space constraints of each page.

(c) Page size and orientation. Each page of the Model Form must be printed in portrait orientation, the size of which must be sufficient to meet the layout and minimum font size requirements, with sufficient white space on the top, bottom, and sides of the content.

(d) Color. The Model Form must be printed on white or light color paper (such as cream) with black or other contrasting ink color. Spot color may be used to achieve visual interest, so long as the color contrast is distinctive and the color does not detract from the readability of the Model Form. Logos may also be printed in color.

(e) Languages. The Model Form may be translated into languages other than English.

B. Information Required in the Model Privacy Form

The information in the Model Form may be modified only as described below:

1. Name of licensee or group of affiliated licensees or institutions providing the notice
Insert the name of the licensee providing the notice, or a common identity of the affiliated licensees or financial institutions jointly providing the notice on the form, wherever [name of licensee] appears.

2. Page One

(a) Last revised date. The licensee must insert in the upper right-hand corner the date on which the notice was last revised. The information shall appear in minimum 8-point font as "rev. [month/year]" using either the name or number of the month, such as "rev. July 2016" or "rev. 7/16."

(b) General instructions for the "What?" box

(i) The bulleted list identifies the types of personal information that the licensee collects and shares. All licensees must use the term "Social Security Number" in the first bullet.

(ii) A licensee must use five (5) of the following terms, to complete the bulleted list: income; account balances; payment history; transaction history; transaction or loss history; credit history; credit scores; assets; investment experience; credit-based insurance scores; insurance claim history; medical information; overdraft

© 2026 National Association of Insurance Commissioners

history; purchase history; account transactions; risk tolerance; medical-related debts; credit card or other debt; mortgage rates and payments; retirement assets; checking account information; employment information; wire transfer instructions.

(c) General instructions for the disclosure table. The left column lists reasons for sharing or using personal information. Each reason correlates to a specific legal provision described in Paragraph 2(d) of this Instruction. In the middle column, each licensee must provide a "Yes" or "No" response that accurately reflects its information-sharing policies and practices with respect to the reason listed on the left. In the right column, each licensee must provide in each box one of the following three (3) responses, as applicable, that reflects whether a consumer can limit such sharing:

"Yes," if it is required to or voluntarily provides an opt-out; "No," if it does not provide an opt-out; or

"We don't share," if it answers "No" in the middle column.

Only the sixth row ("For our affiliates to market to you") may be omitted at the option of the licensee. See Paragraph 2(d)(6) of this instruction.

(d) Specific disclosures and corresponding legal provisions

(i) For our everyday business purposes. This reason incorporates sharing information under [insert citation for sections of statute or regulation sections that parallel Sections 23 and 24 of NAIC model *Privacy of Consumer InformationAct*] and with service providers pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*] other than the disclosures described in Paragraphs (2)(d)(ii) or (2)(d)(iii) of this instruction.

(ii) For our marketing purposes. This reason incorporates sharing information with service providers by a licensee for its own marketing pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iii) For joint marketing with other financial companies. This reason incorporates sharing information under joint marketing agreements between 2 or more licensees or financial institutions and with any service provider used in conjunction with such agreement pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iv) For our affiliates' everyday business purposes – information about transactions and experiences. This reason incorporates sharing information specified in Sections 603(d)(2)(A)(i) and (ii) of the FCRA. A licensee that shares information for this reason may choose to provide an opt-out.

(v) For our affiliates' everyday business purposes – information about creditworthiness. This reason incorporates sharing information pursuant to Section 603(d)(2)(A)(iii) of the FCRA. A licensee that shares information for this reason must provide an opt-out.

(vi) For our affiliates to market to you. This reason incorporates sharing information specified in Section 624 of the FCRA. This reason may be omitted from the disclosure table when: the licensee does not have affiliates (or does not disclose personal information to its affiliates); the licensee's affiliates do not use personal information in a manner that requires an opt-out; or the licensee provides the affiliate marketing notice separately. Licensees that include this reason must provide an opt-out of indefinite duration. A licensee that is required to provide an

© 2026 National Association of Insurance Commissioners

affiliate marketing opt-out, but does not include that opt-out in the Model Form under this part, must comply with Section 624 of the FCRA and [insert citation for statute or regulation that parallels NAIC *Privacy of Consumer Information Act*], with respect to the initial notice and opt-out and any subsequent renewal notice and opt-out. A licensee not required to provide an opt-out under this subparagraph may elect to include this reason in the Model Form.

(vii) For nonaffiliates to market to you. This reason incorporates sharing described in [insert citation for sections of statute or regulation sections that parallel Sections 11 and 16(B) of NAIC *Privacy of Consumer Information Act*]. A licensee that shares personal information for this reason must provide an opt-out.

(e) To limit our sharing. A licensee must include this section of the Model Form only if it provides an opt-out. The word "choice" may be written in either the singular or plural, as appropriate. Licensees must select one or more of the applicable opt-out methods described: telephone, such as by a toll-free number; a web site; or use of a mail-in opt-out form. Licensees may include the word "toll-free" before telephone, as appropriate. A licensee that allows consumers to opt out online must provide either a specific web address that takes consumers directly to the opt-out page or a general web address that provides a clear and conspicuous direct link to the opt-out page. The opt-out choices made available to the consumer who contacts the licensee through these methods must correspond accurately to the "Yes" responses in the third column of the disclosure table. In the part entitled "Please note," licensees may insert a number that is 30 days or greater in the space marked "[30]." Instructions on voluntary or state privacy law opt-out information are in Paragraph 2(g)(v) of these Instructions.

(f) Questions box. Customer service contact information must be inserted as appropriate where [phone number] or [web site] appear. Licensees may elect to provide either a phone number, such as a toll-free number, or a web address, or both. Licensees may include the words "toll-free" before the telephone number, as appropriate.

(g) Mail-in opt-out form. Licensees must include this mail-in form only if they state in the "To limit our sharing" box that consumers can opt out by mail. The mail-in form must provide opt-out options that correspond accurately to the "Yes" responses in the third column of the disclosure table. Licensees that require consumers to provide only name and address may omit the section identified as "[account #]." Licensees that require additional or different information, such as a random opt-out number or a truncated account number to implement an opt-out election should modify the "[account #]" reference accordingly. This includes licensees that require customers consumers with multiple accounts to identify each account to which the opt-out should apply. A licensee must enter its opt-out mailing address in the far right of this form (see version 3); or below the form (see version 4). The reverse side of the mail-in opt-out form must not include any content of the Model Form.

(i) Joint accountholder. Only licensees that provide their joint accountholders the choice to opt out for only one accountholder, in accordance with Paragraph 3(a)(5) of these Instructions, must include in the far left column of the mail-in form the following statement:

If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.

□ Apply my choice(s) only to me.

The word "choice" may be written in either the singular or plural, as appropriate. Licensees that provide insurance products or services, provide this option, and elect to use the Model Form may substitute the word "policy" for "account" in this statement. Licensees that do not provide this option may eliminate this left column from the mail-in form.

(ii) FCRA Section 603(d)(2)(A)(iii) opt-out. If the licensee shares personal information pursuant to Section

© 2026 National Association of Insurance Commissioners

603(d)(2)(A)(iii) of the FCRA, it must include in the mail-in opt-out form the following statement:

□ Do not share information about my creditworthiness with your affiliates for their everyday business purposes.

(iii) FCRA Section 624 opt-out. If the licensee uses Section 624 of the FCRA, in accord with paragraph 2(d)(6) of these Instructions, it must include in the mail-in opt-out form the following statement:

□ Do not allow your affiliates to use my personal information to market to me.

(iv) Nonaffiliate opt-out. If the licensee shares personal information pursuant to [insert citation for section of statute or regulation that parallels Section 16(B) of NAIC *Privacy of Consumer InformationAct*], it must include in the mail-in opt-out form the following statement:

□ Do not share my personal information with nonaffiliates to market their products and services to me.

(v) Additional opt-outs. Licensees that use the disclosure table to provide opt-out options beyond those required by Federal law must provide those opt-outs in this section of the Model Form. A licensee that chooses to offer an opt-out for its own marketing in the mail-in opt-out form must include one of the two following statements:

□ Do not share my personal information to market to me. or

□ Do not use my personal information to market to me.

A licensee that chooses to offer an opt-out for joint marketing must include the following statement:

□ Do not share my personal information with other financial institutions to jointly market to me.

(h) Barcodes. A licensee may elect to include a barcode and/or "tagline" (an internal identifier) in 6-point type at the bottom of page one, as needed for information internal to the licensee, so long as these do not interfere with the clarity or text of the form.

3. Page Two

(a) General Instructions for the Questions. Certain Questions on the Model Form may be customized as follows:

(i) "Who is providing this notice?" This question may be omitted where only one licensee provides the Model Form and that licensee is clearly identified in the title on Page One. Two or more licensees or financial institutions that jointly provide the Model Form must use this question to identify themselves as required by [insert citation for section of statute or regulation that parallels Section 15(E) of NAIC model *Privacy of Consumer Information Act*]. Where the list of licensees or financial institutions exceeds four (4) lines, the licensee must describe in the response to this question the general types of licensees or financial institutions jointly providing the notice and must separately identify those licensees or financial institutions, in minimum 8-point font, directly following the "Other important information" box, or, if that box is not included in the licensee's form, directly following the "Definitions." The list may appear in a multi- column format.

(ii) "How does [name of licensee] protect my personal information?" The licensee may only provide additional information pertaining to its safeguards practices following the designated response to this question. Such information may include information about the licensee's use of cookies or other measures it uses to

© 2026 National Association of Insurance Commissioners

safeguard personal information. Licensees are limited to a maximum of 30 additional words.

(iii) "How does [name of licensee] collect my personal information?" Licensees must use five (5) of the following terms to complete the bulleted list for this question: open an account; deposit money; pay your bills; apply for a loan; use your credit or debit card; seek financial or tax advice; apply for insurance; pay insurance premiums; file an insurance claim; seek advice about your investments; buy securities from us; sell securities to us; direct us to buy securities; direct us to sell your securities; make deposits or withdrawals from your account; enter into an investment advisory contract; give us your income information; provide employment information; give us your employment history; tell us about your investment or retirement portfolio; tell us about your investment or retirement earnings; apply for financing; apply for a lease; provide account information; give us your contact information; pay us by check; give us your wage statements; provide your mortgage information; make a wire transfer; tell us who receives the money; tell us where to send the money; show your government-issued ID; show your driver's license; order a commodity futures or option trade.

Licensees that collect personal information from their affiliates and/or credit bureaus must include the following statement after the bulleted list: "We also collect your personal information from others, such as credit bureaus, affiliates, or other companies." Licensees that do not collect personal information from their affiliates or credit bureaus but do collect information from other companies must include the following statement instead: "We also collect your personal information from other companies." Only licensees that do not collect any personal information from affiliates, credit bureaus, or other companies can omit both statements.

(iv) "Why can't I limit all sharing?" Licensees that describe state privacy law provisions in the "Other important information" box must use the bracketed sentence: "See below for more on your rights under state law." Other licensees must omit this sentence.

(v) "What happens when I limit sharing for an account I hold jointly with someone else?" Only licensees that provide opt-out options must use this question. Other licensees must omit this question. Licensees must choose one of the following two statements to respond to this question: "Your choices will apply to everyone on your account." or "Your choices will apply to everyone on your account—unless you tell us otherwise." Licensees may substitute the word "policy" for "account" in these statements.

(b) General Instructions for the Definitions. The licensee must customize the space below the responses to the three definitions in this section. This specific information must be in italicized lettering to set off the information from the standardized definitions.

(i) Affiliates. As required by [insert citation for section of statute or regulation that parallels Section 9(A)(3) of NAIC *Privacy of Consumer Information Act*], where [affiliate information] appears, the licensee must:

(a) If it has no affiliates, state: "[name of licensee] has no affiliates";

(b) If it has affiliates but does not share personal information with them, state: "[name of licensee] does not share with our affiliates"; or

(c) If it shares with its affiliates, state, as applicable: "Our affiliates include companies with a [common corporate identity of licensee] name; financial companies such as [insert illustrative list of companies]; nonfinancial companies, such as [insert illustrative list of companies]; and others, such as [insert illustrative list]."

(ii) Nonaffiliates. As required by [insert citation for section of statute or regulation that parallels Section 9)(A)(3) of NAIC *Privacy of Consumer InformationAct*], where [nonaffiliate information] appears, the licensee must:

© 2026 National Association of Insurance Commissioners

(a) If it does not share with nonaffiliated third parties, state: "[name of licensee] does not share with nonaffiliates so they can market to you"; or

(b) If it shares with nonaffiliated third parties, state, as applicable: "Nonaffiliates we share with can include [list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations]."

(iii) Joint Marketing. As required by [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*], where [joint marketing] appears, the licensee must:

(a) If it does not engage in joint marketing, state: "[name of licensee] doesn't jointly market"; or

(b) If it shares personal information for joint marketing, state, as applicable: "Our joint marketing partners include [list categories of companies such as credit card companies]."

(c) General instructions for the "Other important information" box. This box is optional. The space provided for information in this box is not limited, and an additional page may be used if necessary. Only the following types of information can appear in this box:

(i) State and/or international privacy law information; and/or

(ii) A form by which the consumer may acknowledge receipt of the notice.

Chronological Summary of Actions (all references are to the Proceedings of the NAIC)

2000 Proc. 3rd Quarter 7, 10, 14-36, 904 (adopted).
2002 Proc. 3rd Quarter12, 13, 71, 72-73 (amended).
2017 Spring National Meeting (amended).

© 2026 National Association of Insurance Commissioners

Version 1:
Model Form with No Opt-Out

Rev. [insert date]

FACTS	**WHAT DOES** [Name of Licensee] **DO WITH YOUR PERSONAL INFORMATION?**
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores] When you are *no longer* our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

Questions?	Call [phone number] or go to [web site]

© 2026 National Association of Insurance Commissioners

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Version 2: Model Form with Opt-Out by Telephone and/or Online

Rev. [insert date]

FACTS	WHAT DOES [NAME OF LICENSEE] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

To limit our sharing	■ Call [phone number] —our menu will prompt you through your choice(s) **or** ■ Visit us online: [web site] **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

© 2026 National Association of Insurance Commissioners

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Rev. [insert date

Version 3: Model Form with Mail-in Opt-Out Form

FACTS	WHAT DOES [NAME OF LICENSEE] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

© 2026 National Association of Insurance Commissioners

Page 2

To limit our sharing	■ Call [phone number] —our menu will prompt you through your choice(s) ■ Visit us online: [web site] or ■ Mail the form below **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

Mail-in Form

Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless your mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me.	
	Name	
	Address	
	City, State, Zip	
	[Account #]	
Mail To:	[Name of Licensee] [Address] [City], [ST] [ZIP]	

© 2026 National Association of Insurance Commissioners

Page 3

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Version 4: Optional Mail-in Form

Mail-in Form	
Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me. **Name** **Address** **City, State, Zip** **[Account #]**
Mail To:	[Name of Licensee], [Address 1], [Address 2], [City], [ST] [ZIP]

© 2026 National Association of Insurance Commissioners

American Land Title Association (ALTA):

PRIVACY OF CONSUMER ~~FINANCIAL AND HEALTH~~ INFORMATION ~~REGULATION~~ACT

Table of Contents

ARTICLE I. GENERAL PROVISIONS

Section 1. ~~Authority~~ Purpose
Section 2. ~~Purpose and~~ Scope and Compliance
Section 3. Rule of Construction
Section 4. Definitions

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS~~PRIVACY AND OPT OUT NOTICES FOR FINANCIAL INFORMATION~~

Section 5. Third-Party Service Provider Arrangements~~Initial Privacy Notice to Consumers Required~~

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7~~6~~. ~~Annual Privacy~~ Initial and Subsequent Delivery Notice of Information Practices to ~~Customers~~ Consumers Required
Section 8~~7~~. ~~Information to be Included in Privacy Notices~~Annual Notice of Information Practices to ~~Customers~~Consumers Required
Section 9~~8~~. ~~Form of Opt Out Notice to Consumers and Opt Out Methods~~Information to be Included in Notices of Information Practices
Section 10~~9~~. ~~Revised Privacy Notices~~Short Form Initial Notice of Information Practices
Section 11~~0~~. Form of Opt-In Notice to Consumers and Opt-In Methods~~Privacy Notices to Group Policyholders~~
Section 12~~1~~. ~~Delivery~~Form of Opt-Out Notice to Consumers and Opt-Out Methods
Section 13. Revised Notice of Information Practices
Section 14. Notice of Information Practices to Group Policyholders
Section 15. Delivery

ARTICLE ~~VIII~~. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL ~~FINANCIAL~~ INFORMATION

Section 16~~2~~. General Rules for Use and Disclosure of Nonpublic Personal Information~~Limitation on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties~~
Section 17~~3~~. Limits on Redisclosure and Reuse of Nonpublic Personal ~~Financial~~ Information
Section 18~~4~~. Limits on Sharing Access ~~Account~~ Number or Access Code Information for Marketing Purposes
Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted Advertising
Section 20. Limits on Sale of Nonpublic Personal Information
Section 21. Limits on Disclosure of Sensitive Personal Information

© 2026~~17~~ National Association of Insurance Commissioners

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL ~~FINANCIAL~~ INFORMATION

Section 22~~15~~. Exception to Opt Out Requirements for Disclosure of Nonpublic Personal ~~Financial~~ Information for Service Providers and Joint Marketing
Section 23~~16~~. Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal ~~Financial~~ Information for Processing and Servicing Transactions
Section 24~~17~~. Other Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Information

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 25~~18~~. When Authorization Required for Disclosure of Nonpublic Personal Health Information
Section 26~~19~~. Authorizations
Section 27~~0.~~ Authorization Request Delivery
Section 28~~1~~. Relationship to Federal Rules
Section 29~~2~~. Relationship to State Laws

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 30~~23~~. Protection of Fair Credit Reporting Act
Section 31~~24~~. Nondiscrimination
Section 32~~25~~. Violation
Section 33~~26~~. Severability
Section 34. Individual Remedies
Section 35~~27~~. Effective Date
~~Appendix A Sample Clauses~~
~~Appendix B Federal Model Privacy Form~~

APPENDICES

Appendix A Sample Clauses
Appendix B Federal Model Privacy Form
Model Law Forms

© 202617 National Association of Insurance Commissioners

American Land Title Association (ALTA):

ARTICLE I. GENERAL PROVISIONS

~~**Section 1. Authority**~~

~~This regulation is promulgated pursuant to the authority granted by Sections [insert applicable sections] of the Insurance Law.~~

Section ~~2~~1. Purpose ~~and Scope~~

~~A.~~ Purpose. This Act~~regulation~~ governs the treatment of nonpublic personal health information and nonpublic personal ~~financial~~ information about individuals by all licensees of the state insurance department. This Act~~regulation~~:

A.~~(1)~~ Requires a licensee to provide notice to individuals about its privacy policies and practices;

B.~~(2)~~ Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal ~~financial~~ information about individuals to affiliates and nonaffiliated third parties; and

C.~~(3)~~ Provides methods for individuals to prevent a licensee from disclosing that information.

Drafting Note: Whether this model is adopted as an Act or Regulation will depend upon individual state law. If a state adopts the model as an Act, reference to the model as an Act should be updated throughout the model.

Section 2. Scope and Compliance

Commented [CC1]: We recommend the NAIC adopt a small business exemption with a defined revenue or data-volume threshold drawn from an existing, complete framework.

A.~~B.~~ Scope. This Act~~regulation~~ applies to:

(1) Nonpublic personal ~~financial~~ information about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. This ~~regulation~~ Act does not apply to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes; and

(2) All nonpublic personal health information.

B.~~C.~~ Compliance. A licensee domiciled in this state that is in compliance with this Act ~~regulation~~ in a state that has not enacted laws or regulations that meet the requirements of Title V of the Gramm-Leach-Bliley Act (PL 102-106) may nonetheless be deemed to be in compliance with Title V of the Gramm-Leach-Bliley Act in the other state.

Drafting Note: Subsection B~~C~~ is intended to give licensees some guidance for complying with Title V of the Gramm-Leach-Bliley Act in those states that do not have laws or regulations that meet GLBA's privacy requirements.

© 2026~~17~~ National Association of Insurance Commissioners

Section 3. Rule of Construction

The examples in this Actregulation, the sample clauses in Appendix A, and the Federal Model Privacy Form in Appendix B of this Actregulation are not exclusive. Compliance with an example, use of a sample clause, or the Federal Privacy Model Form, to the extent applicable, constitutes compliance with this Actregulation.

Licensees may rely on use of the Federal Privacy Form in Appendix B, consistent with the attached instructions, as a safe harbor of compliance with the Notice of Information Practicesprivacy notice content requirements of this regulationAct.

Use of the Federal Model Privacy Form is not required. Licensees may continue to use other types of privacy notices, including notices that contain the examples in this regulation Act and/or the sample clauses in Appendix A, provided that such notices accurately describe the Licensee's privacy practices and otherwise meet the notice content requirements of this regulationAct. However, while Licensees may continue to use privacy notices that contain the examples in this regulation and/or the sample clauses in Appendix A, Licensees may not rely on use of privacy notices with the sample clauses in Appendix A as a safe harbor of compliance with the notice content requirements of this regulation after July 1, 2019.

Drafting Note: Safe harbor of compliance with this regulation Act for use of sample clauses in Appendix A sunsets on July 1, 2019.

Section 4. Definitions

As used in this Actregulation, unless the context requires otherwise:

A. "Affiliate" means a company that controls, is controlled by or is under common control with another company.

B. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

CB. (1) "Clear and conspicuous" means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) Examples.

(a) Reasonably understandable. A licensee makes its notice reasonably understandable if it:

(i) Presents the information in the notice in clear, concise sentences, paragraphs and sections;

(ii) Uses short explanatory sentences or bullet lists whenever possible;

(iii) Uses definite, concrete, everyday words and active voice whenever possible;

© 20267 National Association of Insurance Commissioners

American Land Title Association (ALTA):

(iv) Avoids multiple negatives;

(v) Avoids legal and highly technical business terminology whenever possible; and

(vi) Avoids explanations that are imprecise and readily subject to different interpretations.

(b) Designed to call attention. A licensee designs its notice to call attention to the nature and significance of the information in it if the licensee:

(i) Uses a plain-language heading to call attention to the notice;

(ii) Uses a typeface and type size that are easy to read;

(iii) Provides wide margins and ample line spacing;

(iv) Uses boldface or italics for key words; and

(v) In a form that combines the licensee's notice with other information, uses distinctive type size, style, and graphic devices, such as shading or sidebars.

(c) Notices on web sites. If a licensee provides a notice on a web page, the licensee designs its notice to call attention to the nature and significance of the information in it if the licensee uses text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks or sound) do not distract attention from the notice, and the licensee either:

(i) Places the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(ii) Places a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

DC. "Collect" means to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

ED. "Commissioner" means the chief insurance regulatory official ~~commissioner~~ of the state.

Drafting Note: Use the title of the chief insurance regulatory official wherever the term "commissioner" appears. If the jurisdiction of certain health licensees, such as health maintenance organizations, lies with some state agency other than the insurance department, or if there is dual regulation, a state should add language referencing that agency to ensure the appropriate coordination of responsibilities.

F~~E~~. "Company" means a corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.

G~~F~~. (1) "Consumer" means an individual who seeks to obtain, obtains or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, and about whom the licensee has nonpublic personal information, or that individual's legal representative.

(2) Examples.

(a) An individual who provides nonpublic personal information to a licensee in connection with obtaining or seeking to obtain financial, investment or economic advisory services relating to an insurance product or service is a consumer regardless of whether the licensee establishes an ongoing advisory relationship.

(b) An applicant for insurance prior to the inception of insurance coverage is a licensee's consumer.

(c) An individual who is a consumer of another financial institution is not a licensee's consumer solely because the licensee is acting as agent for, or provides processing or other services to, that financial institution.

(d) An individual is a licensee's consumer if:

(i) (I) The individual is a beneficiary of a life insurance policy underwritten by the licensee;

(II) The individual is a claimant under an insurance policy issued by the licensee;

(III) The individual is an insured or an annuitant under an insurance policy or an annuity, respectively, issued by the licensee; or

(IV) The individual is a mortgagor of a mortgage covered under a mortgage insurance policy; and

(ii) The licensee discloses nonpublic personal ~~financial~~ information about the individual to a nonaffiliated third party other than as permitted under Sections ~~15, 16 and 17~~22, 23, and 24 of this ~~regulation~~Act.

(e) Provided that the licensee provides the initial, annual and revised notices under Sections ~~10~~ 7, 8, and 13 of this ~~regulation~~ Act to the plan sponsor, group or blanket insurance policyholder or group annuity contractholder, or workers' compensation policyholder, and further provided that the licensee does not disclose to a nonaffiliated third party nonpublic personal financial information about an individual described in Item (i), (ii) or (iii), other than as permitted under Sections ~~15, 16 and 17~~22, 23, or 24 of this ~~regulation~~Act, such an individual is not the consumer of the licensee solely because he or she is:

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

(i) A participant or a beneficiary of an employee benefit plan that the licensee administers or sponsors or for which the licensee acts as a trustee, insurer or fiduciary;

(ii) Covered under a group or blanket insurance policy or group annuity contract issued by the licensee; or

(iii) A claimant covered by a workers' compensation plan.

Drafting Note: In states where the workers' compensation self-insurance or workers' compensation state fund coverage is outside the commissioner's jurisdiction, regulators may wish to urge the applicable agency or agencies to promulgate a regulation similar to this ~~regulation~~ Act in order to ensure parity in treatment of workers' compensation plans and to ensure that all workers covered by such plans have privacy protections.

(f) (i) The individuals described in Subparagraph (e)(i) through (iii) of this paragraph are consumers of a licensee if the licensee does not meet all the conditions of Subparagraph (e).

(ii) In no event shall the individuals, solely by virtue of the status described in Subparagraph (e)(i) through (iii) above, be deemed to be ~~customers~~ consumers for purposes of this ~~regulation~~Act.

(g) An individual is not a licensee's consumer solely because he or she is a beneficiary of a trust for which the licensee is a trustee.

(h) An individual is not a licensee's consumer solely because he or she has designated the licensee as trustee for a trust.

H~~G~~. "Consumer reporting agency" has the same meaning as in Section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

I~~H~~. "Control" means:

(1) Ownership, control or power to vote twenty-five percent (25%) or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

(2) Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or

(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the commissioner determines.

~~I. "Customer" means a consumer who has a customer relationship with a licensee.~~

~~J. (1) "Customer relationship" means a continuing relationship between a consumer and a licensee under which the licensee provides one or more insurance products or services to the consumer that are to be used primarily for personal, family or household purposes.~~

~~(2) Examples.~~

Commented [CC2]: 15 USC 6803's notice obligation attaches to a customer relationship. Current state insurance privacy laws distinguish between a consumer and a customer. Eliminating the concept of a customer from this proposed model removes a very important distinction to the title insurance industry, which has a customer relationship with its typical customers of limited duration. It would also impose a subjective and onerous obligation on the insurance trades that is not present in the implementing GLBA regulations for any other financial services trade by requiring annual privacy notices to every "prospective" customer of an insurance company until data deletion is fully achieved. This could lead to confusion for consumers whose limited interaction with an insurance company results in years of unsolicited mailings from an insurance company that they never had a customer relationship with.

© 2026~~17~~ National Association of Insurance Commissioners

~~(a) A consumer has a continuing relationship with a licensee if:~~

~~(i) The consumer is a current policyholder of an insurance product issued by or through the licensee; or~~

~~(ii) The consumer obtains financial, investment or economic advisory services relating to an insurance product or service from the licensee for a fee.~~

~~(b) A consumer does not have a continuing relationship with a licensee if:~~

~~(i) The consumer applies for insurance but does not purchase the insurance;~~

~~(ii) The licensee sells the consumer airline travel insurance in an isolated transaction;~~

~~(iii) The individual is no longer a current policyholder of an insurance product or no longer obtains insurance services with or through the licensee;~~

~~(iv) The consumer is a beneficiary or claimant under a policy and has submitted a claim under a policy choosing a settlement option involving an ongoing relationship with the licensee;~~

~~(v) The consumer is a beneficiary or a claimant under a policy and has submitted a claim under that policy choosing a lump sum settlement option;~~

~~(vi) The customer's policy is lapsed, expired or otherwise inactive or dormant under the licensee's business practices, and the licensee has not communicated with the customer about the relationship for a period of twelve (12) consecutive months, other than annual privacy notices, material required by law or regulation, communication at the direction of a state or federal authority, or promotional materials;~~

~~(vii) The individual is an insured or an annuitant under an insurance policy or annuity, respectively, but is not the policyholder or owner of the insurance policy or annuity; or~~

~~(viii) For the purposes of this regulation, the individual's last known address according to the licensee's records is deemed invalid. An address of record is deemed invalid if mail sent to that address by the licensee has been returned by the postal authorities as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.~~

J. "De-identified data" means information that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual.

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

K. (1) "Financial institution" means any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 1843(k)(4)(B) ~~4(k)~~ of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial institution does not include:

(a) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 *et seq.*);

(b) The Federal Agricultural Mortgage Corporation or any entity charged and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*); or

(c) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as the institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

L. (1) "Financial product or service" means a product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 1843(k)(4)(B) ~~4(k)~~ of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.

~~M. "Health care" means:~~

~~(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, services, procedures, tests or counseling that:~~

~~(a) Relates to the physical, mental or behavioral condition of an individual; or~~

~~(b) Affects the structure or function of the human body or any part of the human body, including the banking of blood, sperm, organs or any other tissue; or~~

~~(2) Prescribing, dispensing or furnishing to an individual drugs or biologicals, or medical devices or health care equipment and supplies.~~

~~N. "Health care provider" means a physician or other health care practitioner licensed, accredited or certified to perform specified health services consistent with state law, or a health care facility.~~

MP. ~~(1)~~ "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.

~~(2) Insurance service includes a licensee's evaluation, brokerage or distribution of information that the licensee collects in connection with a request or an application from a consumer for a insurance product or service.~~

~~Q~~N. (1) "Licensee" means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Insurance Law of this state, [and health maintenance organizations holding a certificate of authority pursuant to Section [insert section] of this state's Public Health Law].

Drafting Note: Add bracketed language if HMOs are licensed under other than insurance statutes and cite appropriate state law.

(2) A licensee is not subject to the notice and opt out requirements for nonpublic personal ~~financial~~ information set forth in Articles I, II, III and IV of this ~~regulation~~ Act if the licensee is an employee, agent or other representative of another licensee ("the principal") and:

(a) The principal otherwise complies with, and provides the notices required by, the provisions of this ~~regulation~~Act; and

(b) The licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates in a manner permitted by this ~~regulation~~Act.

(3) (a) Subject to Subparagraph (b), "licensee" shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only in regard to the excess lines placements placed pursuant to Section [insert section] of this state's laws.

(b) An excess lines broker or excess lines insurer shall be deemed to be in compliance with the notice and opt out requirements for nonpublic personal ~~financial~~ information set forth in Articles I, II, III and IV of this ~~regulation~~ Act provided:

(i) The broker or insurer does not disclose nonpublic personal information of a consumer ~~or a customer~~ to nonaffiliated third parties for any purpose, including joint servicing or marketing under Section 22~~15~~ of this ~~regulation~~Act, except as permitted by Section 23~~16~~ or 24~~17~~ of this ~~regulation~~Act; and

(ii) The broker or insurer delivers a notice to the consumer at the time a ~~customer~~ consumer relationship is established on which the following is printed in 16-point type:

NOTICE OF INFORMATION PRACTICES~~PRIVACY NOTICE~~

"Neither the U.S. brokers that handled this insurance nor the insurers that have underwritten this insurance will disclose nonpublic personal information concerning the buyer to nonaffiliates of the brokers or insurers except as permitted by law."

© 202617 National Association of Insurance Commissioners

American Land Title Association (ALTA):

Drafting Note: References to "excess lines broker" and "excess lines insurer" should be changed as necessary to correspond with the applicable terms used in each state.

~~R~~O. (1) "Nonaffiliated third party" means any person except:

(a) A licensee's affiliate; or

(b) A person employed jointly by a licensee and any company that is not the licensee's affiliate (but nonaffiliated third party includes the other company that jointly employs the person).

(2) Nonaffiliated third party includes any company that is an affiliate solely by virtue of the direct or indirect ownership or control of the company by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

P. "Nonpublic personal h~~H~~ealth information" means any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of an individual;

(2) The provision of health care to an individual; or

(3) Payment for the provision of health care to an individual.

Q~~S~~. "Nonpublic personal information" means ~~nonpublic personal financial information and nonpublic personal health information.~~any personally identifiable information that is linked or reasonably linkable to an identified natural person. Nonpublic personal information does not include de-identified data or publicly available information.

~~T. (1) "Nonpublic personal financial information" means:~~

~~(a) Personally identifiable financial information; and~~

~~(b) Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.~~

~~(2) Nonpublic personal financial information does not include:~~

~~(a) Health information;~~

~~(b) Publicly available information, except as included on a list described in Subsection T(1)(b) of this section; or~~

~~(c) Any list, description or other grouping of consumers (and publicly available~~

~~information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.~~

~~(3) Examples of lists.~~

~~(a) Nonpublic personal financial information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information that is not publicly available, such as account numbers.~~

~~(b) Nonpublic personal financial information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived in whole or in part using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.~~

~~U. "Nonpublic personal health information" means health information:~~

~~(1) That identifies an individual who is the subject of the information; or~~

~~(2) With respect to which there is a reasonable basis to believe that the information could be used to identify an individual.~~

R~~V~~. (1) "Personally identifiable ~~financial~~ information" means any information:

(a) A consumer provides to a licensee to obtain an insurance product or service from the licensee;

(b) About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

(c) The licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.

(2) Examples.

(a) Information included. Personally identifiable ~~financial~~ information includes:

(i) Information a consumer provides to a licensee on an application to obtain an insurance product or service;

(ii) Account balance information and payment history;

(iii) The fact that an individual is or has been one of the licensee's consumers~~ustomers~~ or has obtained an insurance product or service from the licensee;

(iv) Any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer;

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

(v) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;

(vi) Any information the licensee collects through an Internet cookie (an information-collecting device from a web server); and

(vii) Information from a consumer report.

(b) Information not included. Personally identifiable ~~financial~~ information does not include:

~~(i) Health information;~~

(i~~i~~) A list of names and addresses of customers of an entity that is not a financial institution; and

(ii~~i~~) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.

S~~X~~. "Opt in" means an affirmative direction by a consumer that authorizes a licensee to disclose the consumer's information.

T~~X~~. "Opt out" means a direction by a consumer that the licensee may not disclose nonpublic personal information about the consumer to a nonaffiliated third party, except as permitted under Sections 22,23, or 24 ~~15, 16, 17, and 18~~.

U~~W~~. (1) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

(a) Federal, state or local government records;

(b) Widely distributed media; or

(c) Disclosures to the general public that are required to be made by federal, state or local law.

(2) Reasonable basis. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

(a) That the information is of the type that is available to the general public; and

(b) Whether an individual can direct that the information not be made available to the general public and, if so, that the licensee's consumer has not done so.

Commented [CC3]: New privacy laws, like CCPA, provide a different definition of "publicly available information." Care should be taken to utilize the same definition of "publicly available information" as is used in state comprehensive data privacy laws to minimize compliance burdens of managing to multiple statutory definitions and consumer confusion as to application of their privacy rights.

(3) Examples.

(a) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(b) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(c) Reasonable basis.

(i) A licensee has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(ii) A licensee has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the licensee has located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

V. "Reasonable opportunity" means any of the following:

(1) ~~(a)~~ The licensee mails the notices required to the consumer and allows the consumer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within sixty (60) days from the date the licensee mailed the notices;

(2) ~~(b)~~ Where a consumer agrees to receive the notices required by this Act electronically in accordance with UETA [insert state electronic transactions act statute], the licensee allows the consumer to opt out by any reasonable means at any time; or

(3) ~~(c)~~ For an isolated transaction, such as providing the consumer with an insurance quote, the licensee provides the notices required by this Act at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction.

X. -"Sale" or "selling" means the exchange of nonpublic personal information for monetary or other valuable consideration. A licensee does not sell nonpublic personal information when:

(1) The disclosure is to a third party for the purpose of or in support of providing a product or service requested by the consumer.

~~(1)~~(2) A licensee provides information to or receives anything of value from an insurance

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

support organization, statistical agent, or reinsurer;

~~(2)~~(3) A licensee provides nonpublic personal information to an affiliate or to a financial institution with which the licensee performs joint marketing;

~~(3)~~(4) The business transfers to a third party the nonpublic personal information as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction in which the party assumes control of all or part of the licensee's assets; or

(5) A consumer uses or directs the business to (i) disclose nonpublic personal information; or (ii) interact with one or more third parties including but not limited to referrals to other licensees.

Y. "Sensitive Personal Information" means personally identifiable "nonpublic personal information" about a consumer that includes:

(1) Racial or ethnic origin, religious beliefs, sexual orientation, or citizenship or citizenship status; or

(2) Genetic information or biometric data that may be processed for the purpose of uniquely identifying an individual.

Z. (1) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests.

(2) "Targeted advertising" does not include:

(a) Online advertisements based on activities within a Licensee's own websites or online applications;

(b) Online advertisements based on the context of a consumer's current search query, visit to a website, or online application;

(c) Online advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(d) Processing Nonpublic Personal Information solely for measuring or reporting advertising performance, reach, or frequency.

AA. "Third party service provider" or "third party" means a person or entity not otherwise defined as a licensee or affiliate of a licensee that:

(1) Provides services to the licensee; and

(2) Maintains, processes or otherwise is permitted access to nonpublic personal information through its provisions of services to the licensee.

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS ~~PRIVACY AND OPT-OUT NOTICES FOR FINANCIAL INFORMATION~~

Section 5. Third-Party Service Provider Arrangements

A. Contract Requirements.

A licensee that discloses a consumer's nonpublic personal information to a third-party service provider shall enter into a written contract with the third-party service provider that:

(1) Prohibits the third-party service provider from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless processing is necessary to comply with the law or a valid and binding order of a governmental body, in which case the third-party service provider must notify the licensee within 48 hours unless prohibited by law;

(2) Requires the third-party service provider to delete, destroy, de-identify or return all nonpublic personal information to the licensee when requested by the licensee; or to delete nonpublic personal information after it is no longer necessary to fulfill a legal requirement or to meet the record retention requirements of the licensee or third-party service provider, and to notify the licensee of the action taken;

(3) Requires the third-party service provider to notify the licensee if it can no longer comply with its obligations under this contract and provides the licensee with a right to terminate the contract;

(4) Requires that any contract between a third-party service provider and a subcontractor with access to a consumer's nonpublic personal information must contain provisions no less protective of nonpublic personal information than those contained in the third-party service provider's agreement with the licensee;

(5) Requires the third-party service provider to provide assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act;

(6) Requires the third-party service provider to implement and maintain administrative, technical, and physical data security practices to protect the nonpublic personal information from unauthorized access, destruction, use, modification, or disclosure;

(7) Requires the third-party service provider to notify the licensee of a failure to meet the obligations of Subsections (1) to (6) above within 48 hours of discovery by the third-party service provider.

B. A licensee that discloses a consumer's nonpublic personal information to a third-party service provider remains fully responsible for compliance with this Act and the handling of nonpublic personal information.

Commented [CC4]: We strongly recommend the NAIC to take a risk-based approach to third party service provider oversight and its third party contracts, as previously done with Model Law 668. Imposing prescriptive requirements for insurer contracts has the effect of limiting insurance companies' ability to contract in ways detrimental to the insurance company and their serviced customers. Certain large service providers will not negotiate contract terms with clients, though these providers may be better positioned to protect consumer data than smaller vendors who would agree to these terms but be less resourced to adequately protect consumer data. Certain of these requirements would also disallow an insurer from negotiating more restrictive contract terms (an incident notice period of less than 48 hours, for example, or the disallowance of subcontractor data processing).

Additionally, we recommend a safe harbor for licensees whose existing contracts already meet MDL-668, CCPA, or a comparable framework, so insurers aren't forced to renegotiate agreements that already provide equivalent protection.

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

A. A consumer may file the following requests with a licensee, which shall be processed in accordance with the following standards:

(1) Within 45 days of receiving an authenticated request from a consumer for their nonpublic personal information, a licensee shall disclose:

(a) All nonpublic personal information about the consumer that is maintained by the licensee or any contracted third-party service provider; and

(b) A list of all third-party service providers to whom the licensee disclosed the consumer's nonpublic personal information.

(2) A licensee shall not be required to disclose the following:

(a) A consumer's Social Security Number, driver's license number or other government-issued identification number, financial account number(s), any health insurance or medical identification number, any account password(s), security questions and answers, unique biometric data or other information that could create a high risk of identity theft. The licensee may instead disclose the types of nonpublic personal information maintained by listing each type of nonpublic personal information it has about the consumer;

(b) Duplicative nonpublic personal information, if it is described in a manner reasonably understandable by the consumer and the consumer is offered an opportunity to review the nonpublic personal information for inconsistencies; or

(c) Information that is outside the scope of the request, if the consumer has requested only specified items or categories of information.

B. Correction of nonpublic personal information.

(1) A consumer may make an authenticated request for the correction of their nonpublic personal information by filing a request with the licensee that:

(a) Identifies the specific nonpublic personal information the consumer wishes to correct; and

(b) Provides an explanation of why the nonpublic personal information is incorrect.

(2) Within 45 days of receipt of the request under this subsection, a licensee shall take one of the following actions and notify the consumer:

(a) Correct the nonpublic personal information in dispute as requested by the consumer;

Commented [CC5]: In the context of a real estate transaction, this would have to be a transaction by transaction analysis, potentially, which would take considerable time and resources for response.

Commented [CC6]: Other information could also carry high risk if disclosed, such as the address for those protected by address confidentiality programs. Disclosure of categories would be more protective against risk to the consumer and would allow for more timely response.

We recommend broadening the standard beyond identity theft to cover information that poses a risk of harm to the consumer more generally, and lean more heavily on the category-based disclosure approach already available for the enumerated list rather than requiring case-by-case identification of every high-risk data type.

© 2026~~17~~ National Association of Insurance Commissioners

(b) Delete the nonpublic personal information in dispute; or

(~~b~~c) Deny the request and provide:

(i) The basis for refusal to correct the nonpublic personal information as requested;

(ii) Information about how the consumer may appeal the denial; and

(iii) An explanation of how the appeal will be reviewed and how the consumer will be notified of the decision on appeal.

(3) A licensee may deny a request for correction if:

(a) The nonpublic personal information is accurate and complete and if the licensee provides a process for appeal of the decision; or

(b) The nonpublic personal information that is the subject of the request was not created by the licensee, unless there is a reasonable basis to believe that the originator of the nonpublic personal information is no longer available to act on the requested correction, and the consumer has independently demonstrated the information is incorrect.

C. Deletion of nonpublic personal information.

(1) Within 45 days of an authenticated request from a consumer, a licensee shall delete the nonpublic personal information about the consumer that is maintained by the licensee or direct a third-party service provider to delete the nonpublic personal information on the licensee's behalf.

(2) The licensee is not required to delete nonpublic personal information if:

(a) The licensee is required by law or regulation to retain the nonpublic personal information;

(b) The nonpublic personal information may be necessary to perform the contract or service requested by or benefiting the consumer;

(c) The information is necessary to comply with a legal obligation; or

(d) The information is maintained in reasonable anticipation of a claim or civil or criminal proceeding.

(3) A licensee may delay fulfilling a consumer's request, up to 45 days, to delete nonpublic personal information stored on an archived or backup system. A licensee must notify the consumer of such delay.

D. Request and Response Procedures

Commented [CC7]: Application backups are designed to restore an entire system to a known point in time after a failure, cyberattack, or other disaster. They are not designed to function as searchable databases from which individual records can be selectively removed.

Modifying backups would undermine their integrity and disaster recovery function.

When a backup is created, the backup software captures a snapshot of large amounts of data and stores that information in compressed, indexed, and often encrypted backup files, individual customer records are not typically stored as separate, independently editable files. As a result, deleting a single customer's information from a backup is usually not technically feasible without restoring the backup, modifying the restored environment, and then creating a completely new backup. Even then, altering backup data can compromise the integrity and reliability of the backup and may prevent the organization from demonstrating that the backup accurately reflects the system's state at the time it was created.

Organizations typically address deletion requests by removing the information from active production systems and ensuring that it is not restored into production from backups except where necessary for disaster recovery. Backup copies containing the information should be allowed to expire according to the established retention period.

We recommend additionally adding explicit language preserving information used to detect, investigate, prevent, or document fraud, misrepresentation, unauthorized transactions, or other illegal activity

© 20~~17~~26 National Association of Insurance Commissioners

American Land Title Association (ALTA):

(1) Except as provided in Subsection D(1)(b), a licensee shall respond to requests submitted under this section within 45 days in the following manner:

(a) A licensee may use its secure communications portal to authenticate requests from consumers holding current accounts with the licensee, unless the licensee has reason to believe the request has been submitted through an account that has been compromised. Otherwise, the licensee may use methods that are commercially reasonable, but not unduly burdensome, to authenticate the identity of the person making the request and to verify that this person is either:

(i) The consumer;

(ii) A person acting with the consumer's written authorization, including but not limited to a valid power of attorney;

(iii) The parent or legal guardian of a consumer who is a minor, except where the information relates to health insurance claims in circumstances where the child has a legal right to obtain the services in question without the parent's or guardian's consent;

(iv) The legal guardian or other person authorized by law to act on behalf of an incapacitated consumer; or

(v) The personal representative or other person authorized by law to act on behalf of a deceased consumer.

(b) A licensee is required to notify the consumer if either of the following prevents the licensee from complying with the request:

(i) The specific nonpublic personal information at issue is not locatable or retrievable by the licensee; or

Drafting Note: Examiners should review licensees' notifications to consumers regarding nonpublic personal information that is not locatable or retrievable by the licensee and its justifications for irretrievability during Market Conduct and/or IT Exams.

(ii) The licensee is unable to verify the request after requesting that the consumer provide additional information necessary to authenticate the identity of the consumer and authenticate the consumer's request.

(c) If a licensee declines the consumer's request, the licensee shall inform the consumer of the basis for declining the request and provide instructions for how to request review of the decision.

(2) There shall be no cap on the number of requests to correct or delete nonpublic personal information.

Commented [CC8]: If requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, a business may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The business shall bear the burden of demonstrating that any verifiable consumer request is manifestly unfounded or excessive.

(3) If a consumer disagrees with a licensee's refusal to correct or delete nonpublic personal information per the consumer's request, the consumer shall be permitted to file with the licensee:

© 2026~~17~~ National Association of Insurance Commissioners

(a) A concise statement setting forth why the consumer disagrees with the licensee's refusal and what the consumer thinks is the correct, relevant or fair information; and

(b) The licensee shall maintain the statement with the disputed nonpublic personal information and allow anyone reviewing the disputed nonpublic personal information to be made aware of the dispute and have access to the consumer's statement.

Commented [CC9]: We would like to understand the intent behind what this provision is meant to address because systems in which consumer data resides most likely are not designed to allow for added statements or documents from a consumer as proposed, so this as drafted could potentially pose practical challenges.

© 20267 National Association of Insurance Commissioners

American Land Title Association (ALTA):

ARTICLE IV.~~—~~ NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7~~8~~5. Initial and Subsequent Delivery Notice of Information Practices~~Privacy Notice~~ to Consumers Required

A. Initial Delivery of Notice~~notice requirement~~. A licensee shall provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to~~:~~ all consumers no later than when the licensee obtains access to the consumer's nonpublic personal information, except that a licensee may provide the initial notice within a reasonable time after access to the consumer's nonpublic personal information if:

(1) Obtaining access to the consumer's nonpublic personal information is not at the consumer's election and the licensee follows the Notice of Information Practices previously sent to the consumer; or

(2) Providing notice when the licensee obtains access to the consumer's nonpublic personal i~~n~~formation would substantially delay the consumer's transaction and the consumer agrees to receive the notice at a later time.

Commented [CC10]: Requiring the licensee to capture the consumer's agreement to delay notice, which assumes a level of direct contact that may not exist if the licensee couldn't manage to send the notice itself in the first place. In a lot of title insurance transactions companies don't have that contact at all, the order comes through a realtor, attorney, or lender acting on the consumer's behalf. We recommend the second exception also cover notice provided to or acknowledged by the consumer's authorized representative, rather than requiring direct consumer contact.

B. Subsequent Delivery of Notice

When a consumer with an existing relationship with a licensee obtains a new insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, the licensee satisfies the initial notice requirements of Subsection A of this section as follows:

(1) The licensee may provide a revised notice, under Section 13 , that covers the consumer's new insurance product or service; or

(2) If the initial, revised or annual notice that the licensee most recently provided to that consumer was accurate with respect to the new insurance product or service, the licensee does not need to provide a new notice of information practices under Subsection A of this section.

C. For purposes of this section:

(1) "Not at consumer's election" includes the scenario where a licensee acquires or is assigned a consumer's policy from another financial institution or residual market mechanism and the consumer does not have a choice about the licensee's acquisition or assignment.

(2) "Substantially delay the consumer's transaction" includes the scenario where the licensee and the individual agree over the telephone or electronically to enter into a consumer relationship involving prompt delivery of the insurance product or service but does not include the scenario where the relationship is initiated in person at the licensee's office or through other means by which the consumer may view the notice, such as on a website.

~~(1) Customer. An individual who becomes the licensee's customer, not later than when the licensee establishes a customer relationship, except as provided in Subsection E of this~~

section; and

(2) Consumer. A consumer, before the licensee discloses any nonpublic personal financial information about the consumer to any nonaffiliated third party, if the licensee makes a disclosure other than as authorized by Sections 16 and 17.

B. When initial notice to a consumer is not required. A licensee is not required to provide an initial notice to a consumer under Subsection A(2) of this section if:

(1) The licensee does not disclose any nonpublic personal financial information about the consumer to any nonaffiliated third party, other than as authorized by Sections 16 and 17, and the licensee does not have a customer relationship with the consumer; or

(2) A notice has been provided by an affiliated licensee, as long as the notice clearly identifies all licensees to whom the notice applies and is accurate with respect to the licensee and the other institutions.

C. When the licensee establishes a customer relationship.

(1) General rule. A licensee establishes a customer relationship at the time the licensee and the consumer enter into a continuing relationship.

(2) Examples of establishing customer relationship. A licensee establishes a customer relationship when the consumer:

(a) Becomes a policyholder of a licensee that is an insurer when the insurer delivers an insurance policy or contract to the consumer, or in the case of a licensee that is an insurance producer or insurance broker, obtains insurance through that licensee; or

(b) Agrees to obtain financial, economic or investment advisory services relating to insurance products or services for a fee from the licensee.

D. Existing customers. When an existing customer obtains a new insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, the licensee satisfies the initial notice requirements of Subsection A of this section as follows:

(1) The licensee may provide a revised policy notice, under Section 9, that covers the customer's new insurance product or service; or

(2) If the initial, revised or annual notice that the licensee most recently provided to that customer was accurate with respect to the new insurance product or service, the licensee does not need to provide a new privacy notice under Subsection A of this section.

E. Exceptions to allow subsequent delivery of notice.

(1) A licensee may provide the initial notice required by Subsection A(1) of this section within a reasonable time after the licensee establishes a customer relationship if:

(a) Establishing the customer relationship is not at the customer's election; or

© 20267 National Association of Insurance Commissioners

American Land Title Association (ALTA):

~~(b) Providing notice not later than when the licensee establishes a customer relationship would substantially delay the customer's transaction and the customer agrees to receive the notice at a later time.~~

~~(2) Examples of exceptions.~~

~~(a) Not at customer's election. Establishing a customer relationship is not at the customer's election if a licensee acquires or is assigned a customer's policy from another financial institution or residual market mechanism and the customer does not have a choice about the licensee's acquisition or assignment.~~

~~(b) Substantial delay of customer's transaction. Providing notice not later than when a licensee establishes a customer relationship would substantially delay the customer's transaction when the licensee and the individual agree over the telephone to enter into a customer relationship involving prompt delivery of the insurance product or service.~~

~~(c) No substantial delay of customer's transaction. Providing notice not later than when a licensee establishes a customer relationship would not substantially delay the customer's transaction when the relationship is initiated in person at the licensee's office or through other means by which the customer may view the notice, such as on a web site.~~

~~F. Delivery. When a licensee is required to deliver an initial privacy notice by this section, the licensee shall deliver it according to Section 11. If the licensee uses a short-form initial notice for non-customers according to Section 7D, the licensee may deliver its privacy notice according to Section 7D(3).~~

Section ~~6~~8. Annual ~~Privacy~~ Notice of Information Practices to ~~Customers~~ Consumers Required

~~A. (1)~~ General rule. A licensee shall provide a clear and conspicuous notice to consumers~~ustomers~~ that accurately reflects its privacy policies and practices ~~not less than annually during the continuation of the customer relationship. Annually means~~ at least once in any period of twelve (12) consecutive months. ~~during which that relationship exists.~~ A licensee may define the twelve-consecutive-month period, but the licensee shall apply it to the consumer~~ustomer~~ on a consistent basis.

A.~~(2)~~ Example. A licensee provides a notice annually if it defines the twelve-consecutive-month period as a calendar year and provides the annual notice to the consumer~~ustomer~~ once in each calendar year following the calendar year in which the licensee provided the initial notice. For example, if a consumer~~ustomer~~ opens an account on any day of year 1, the licensee shall provide an annual notice to that consumer~~ustomer~~ by December 31 of year 2.

(1) Exceptions. ~~to general rule.~~

(1) A licensee that provides nonpublic personal information to nonaffiliated third parties only in accordance with Sections ~~15, 16, or 17~~22, 23, or 24 and has not changed its policies and practices with regard to disclosing ~~n~~Nonpublic Ppersonal Iinformation from the policies and practices that were disclosed in the most recent disclosure sent to consumers in accordance with this section or Section 7~~5~~ shall not be required to provide an annual

Commented [CC11]: Based on the definition of "consumer" (anyone who applied for or received an insurance product, or is a former policyholder, would be a "consumer"), which could pose practical challenges. In cases where the title insurance industry retain data for any order opened for 7 to 10 years (or longer), the industry would have to send participants in failed transactions privacy notices annually for at least that long.

We recommend first, restore the customer/consumer distinction and define "customer" as a consumer with an ongoing relationship with the licensee, then limit the Section 8 annual notice obligation to customers specifically rather than consumers generally. Second, add a specific carve-out for continuation of coverage under an existing policy since that does not constitute an ongoing business relationship unless or until there is a claim, renewal, or modification.

© 2026~~17~~ National Association of Insurance Commissioners

disclosure under this section until such time as the licensee fails to comply with any criteria described in this paragraph.

(2) A licensee is not required to provide notice if the licensee no longer has access to the consumer's nonpublic personal information.

(2) For the purposes of this Act, a licensee no longer has an obligation to continue to notify a consumer if the licensee's records do not contain a valid address. An address is deemed invalid if electronic or regular mail sent to that address by the licensee has been returned as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.

~~C. (1) Termination of customer relationship. A licensee is not required to provide an annual notice to a former customer. A former customer is an individual with whom a licensee no longer has a continuing relationship.~~

~~(2) Examples.~~

~~(a) A licensee no longer has a continuing relationship with an individual if the individual no longer is a current policyholder of an insurance product or no longer obtains insurance services with or through the licensee.~~

~~(b) A licensee no longer has a continuing relationship with an individual if the individual's policy is lapsed, expired or otherwise inactive or dormant under the licensee's business practices, and the licensee has not communicated with the customer about the relationship for a period of twelve (12) consecutive months, other than to provide annual privacy notices, material required by law or regulation, or promotional materials.~~

~~(c) For the purposes of this regulation, a licensee no longer has a continuing relationship with an individual if the individual's last known address according to the licensee's records is deemed invalid. An address of record is deemed invalid if mail sent to that address by the licensee has been returned by the postal authorities as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.~~

~~(d) A licensee no longer has a continuing relationship with a customer in the case of providing real estate settlement services, at the time the customer completes execution of all documents related to the real estate closing, payment for those services has been received, or the licensee has completed all of its responsibilities with respect to the settlement, including filing documents on the public record, whichever is later.~~

~~D. Delivery. When a licensee is required by this section to deliver an annual privacy notice, the licensee shall deliver it according to Section 11.~~

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

Section 97. Information to be Included in ~~Privacy~~ Notices of Information Practices

A. General rule. The initial, annual and revised ~~privacy notices~~ Notice of Information Practices that a licensee provides under Sections ~~5~~7,~~ 6~~8, and ~~3~~139 shall include each of the following items of information, in addition to any other information the licensee wishes to provide, that applies to the licensee and to the consumers to whom the licensee sends its ~~privacy notice:~~ Notice of Information Practices:

~~(1) The categories of nonpublic personal financial information that the licensee collects;~~

~~(2) The categories of nonpublic personal financial information that the licensee discloses;~~

~~(3) The categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information, other than those parties to whom the licensee discloses information under Sections 16 and 17;~~

~~(4) The categories of nonpublic personal financial information about the licensee's former customers that the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information about the licensee's former customers, other than those parties to whom the licensee discloses information under Sections 16 and 17;~~

~~(5) If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under Section 15 (and no other exception in Sections 16 and 17 applies to that disclosure), a separate description of the categories of information the licensee discloses and the categories of third parties with whom the licensee has contracted;~~

(1) The categories of nonpublic personal information that the licensee collects, including, but not limited to, whether information is collected from the consumer, through the consumer's transactions with affiliates or nonaffiliated third parties, or consumer reporting agencies;

(2) The categories of nonpublic personal information that the licensee discloses, including at least one example in each category. Categories may include, but are not limited to, application information, transaction information, or consumer reports;

(3) The categories of affiliates and nonaffiliated third parties, and the types of business in which they engage, to whom the licensee discloses nonpublic personal information, other than those parties to whom the licensee discloses information under Sections ~~20 and 21~~22, 23, and 24. The types of businesses may be described in general terms only if the licensee uses illustrative examples of each significant line of business;

(~~4~~6) An explanation of the consumer's right under Section 12~~A~~ to opt out of the disclosure of nonpublic personal ~~financial~~ information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;

(5) An explanation of the consumer's rights with regard to the sale of nonpublic personal information and disclosure of sensitive personal information pursuant to Sections 20 and 21;

Commented [CC12]: We recommend the Act to provide a complete list of expected categories. Without a complete list of expected categories, a title-specific notice either has to over-include every possible source or risk being wrong for any given transaction.

Commented [CC13]: A single, shared notice model assumes one company with one set of sharing relationships, but title and escrow operations often sit inside a holding company where different entities share with different affiliated and nonaffiliated parties depending on their own business line. As drafted, a consolidated notice either has to list every possible relationship across the corporate family, most of which won't apply to any given entity's actual customers, or risk being inaccurate. We recommend allowing entity-specific or business-line-specific notices within a holding company structure, rather than requiring one notice to accurately describe sharing practices across the entire corporate family.

(6) A description of the consumer's options to request access, correction, or deletion of nonpublic personal information about the consumer as established under this Act and the instructions for exercising such options;

(7) Any disclosures that the licensee makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);

(8) The licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; by~~and~~

(a) Describing in general terms who is authorized to have access to the information; and

(b) Stating whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance with the licensee's policy. The licensee is not required to describe technical information about the safeguards it uses; and

~~(9)~~(c) Any disclosure that the licensee makes ~~under Subsection B of this section.~~ as authorized under Section 22, 23, or 24~~21~~, except that the licensee is not required to list those exceptions in the initial or annual Notice of Information Practices required by Sections ~~9~~7 and ~~10~~8. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.

~~B. Description of parties subject to exceptions. If a licensee discloses nonpublic personal financial information as authorized under Sections 16 and 17, the licensee is not required to list those exceptions in the initial or annual privacy notices required by Sections 5 and 6. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.~~

B. The licensee's notice may include:

(1) Categories of nonpublic personal information that the licensee reserves the right to disclose in the future, but does not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the right in the future to disclose, but to whom the licensee does not currently disclose, nonpublic personal information.

C. Exceptions:~~Examples.~~

If a licensee does not disclose, and does not reserve the right to disclose, nonpublic personal information about consumers to affiliates or nonaffiliated third parties except as authorized under Sections ~~20 and 21~~22, 23, or 24, the licensee shall state that in its notice, in addition to the information it shall provide under Subsections A(1) and A(8) and Subsection B of this section.

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

D. Sample Clauses and Federal Model Privacy Form.

(1) Licensees are not required to use any prescribed clauses or model form.

(2) The commissioner may determine that a Licensee's use of any of the following constitutes compliance with this Act:

(a) Sample clauses illustrating some of the notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner;

(b) Model forms illustrating notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner; or

(c) The Federal Model Privacy Forms are included in Appendix A and Appendix B, of this Act.

~~(1) Categories of nonpublic personal financial information that the licensee collects. A licensee satisfies the requirement to categorize the nonpublic personal financial information it collects if the licensee categorizes it according to the source of the information, as applicable:~~

~~(a) Information from the consumer;~~

~~(b) Information about the consumer's transactions with the licensee or its affiliates;~~

~~(c) Information about the consumer's transactions with nonaffiliated third parties; and~~

~~(d) Information from a consumer reporting agency.~~

~~(2) Categories of nonpublic personal financial information a licensee discloses.~~

~~(a) A licensee satisfies the requirement to categorize nonpublic personal financial information it discloses if the licensee categorizes the information according to source, as described in Paragraph (1), as applicable, and provides a few examples to illustrate the types of information in each category. These might include:~~

~~(i) Information from the consumer, including application information, such as assets and income and identifying information, such as name, address and social security number;~~

~~(ii) Transaction information, such as information about balances, payment history and parties to the transaction; and~~

~~(iii) Information from consumer reports, such as a consumer's creditworthiness and credit history.~~

(b) A licensee does not adequately categorize the information that it discloses if the licensee uses only general terms, such as transaction information about the consumer.

(c) If a licensee reserves the right to disclose all of the nonpublic personal financial information about consumers that it collects, the licensee may simply state that fact without describing the categories or examples of nonpublic personal information that the licensee discloses.

(3) Categories of affiliates and nonaffiliated third parties to whom the licensee discloses.

(a) A licensee satisfies the requirement to categorize the affiliates and nonaffiliated third parties to which the licensee discloses nonpublic personal financial information about consumers if the licensee identifies the types of businesses in which they engage.

(b) Types of businesses may be described by general terms only if the licensee uses a few illustrative examples of significant lines of business. For example, a licensee may use the term financial products or services if it includes appropriate examples of significant lines of businesses, such as life insurer, automobile insurer, consumer banking or securities brokerage.

(c) A licensee also may categorize the affiliates and nonaffiliated third parties to which it discloses nonpublic personal financial information about consumers using more detailed categories.

(4) Disclosures under exception for service providers and joint marketers. If a licensee discloses nonpublic personal financial information under the exception in Section 15 to a nonaffiliated third party to market products or services that it offers alone or jointly with another financial institution, the licensee satisfies the disclosure requirement of Subsection A(5) of this section if it:

(a) Lists the categories of nonpublic personal financial information it discloses, using the same categories and examples the licensee used to meet the requirements of Subsection A(2) of this section, as applicable; and

(b) States whether the third party is:

(i) A service provider that performs marketing services on the licensee's behalf or on behalf of the licensee and another financial institution; or

(ii) A financial institution with whom the licensee has a joint marketing agreement.

(5) Simplified notices. If a licensee does not disclose, and does not wish to reserve the right to disclose, nonpublic personal financial information about customers or former customers to affiliates or nonaffiliated third parties except as authorized under Sections 16 and 17, the licensee may simply state that fact, in addition to the information it shall provide under Subsections A(1), A(8), A(9) and Subsection B of this section.

© 20267 National Association of Insurance Commissioners

American Land Title Association (ALTA):

~~(6) Confidentiality and security. A licensee describes its policies and practices with respect to protecting the confidentiality and security of nonpublic personal financial information if it does both of the following:~~

~~(a) Describes in general terms who is authorized to have access to the information; and~~

~~(b) States whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance with the licensee's policy. The licensee is not required to describe technical information about the safeguards it uses.~~

~~D. Short-form initial notice with opt out notice for non-customers.~~

~~(1) A licensee may satisfy the initial notice requirements in Sections 5A(2) and 8C for a consumer who is not a customer by providing a short-form initial notice at the same time as the licensee delivers an opt out notice as required in Section 8.~~

~~(2) A short-form initial notice shall:~~

~~(a) Be clear and conspicuous;~~

~~(b) State that the licensee's privacy notice is available upon request; and~~

~~(c) Explain a reasonable means by which the consumer may obtain that notice.~~

~~(3) The licensee shall deliver its short-form initial notice according to Section 10. The licensee is not required to deliver its privacy notice with its short-form initial notice. The licensee instead may simply provide the consumer a reasonable means to obtain its privacy notice. If a consumer who receives the licensee's short-form notice requests the licensee's privacy notice, the licensee shall deliver its privacy notice according to Section 11.~~

~~(4) Examples of obtaining privacy notice. The licensee provides a reasonable means by which a consumer may obtain a copy of its privacy notice if the licensee:~~

~~(a) Provides a toll-free telephone number that the consumer may call to request the notice; or~~

~~(b) For a consumer who conducts business in person at the licensee's office, maintains copies of the notice on hand that the licensee provides to the consumer immediately upon request.~~

~~E. Future disclosures. The licensee's notice may include:~~

~~(1) Categories of nonpublic personal financial information that the licensee reserves the right to disclose in the future, but does not currently disclose; and~~

~~(2) Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the right in the future to disclose, but to whom the licensee does not currently disclose, nonpublic personal financial information.~~

~~F. Sample Clauses and Federal Model Privacy Form. Sample clauses illustrating some of the notice content required by this section and the Federal Model Privacy Form are included in Appendix A and Appendix B, respectively, of this regulation.~~

Section 10. Short Form Initial Notice of Information Practices

A. A licensee may satisfy the initial notice requirements in Sections 7A and 13A by providing a Short Form Initial Notice of Information Practices at the same time the licensee delivers an opt-out notice as required in Section 12 if:

(1) The licensee provides the consumer a reasonable means to obtain its Notice of Information Practices; and

(2) The licensee provides the Notice of Information Practices upon request.

B. A Short Form Initial Notice of Information Practices shall meet all of the following requirements.

(1) Be clear and conspicuous;

(2) State that the licensee's Notice of Information Practices is available upon request;

(3) Explain the reasonable means to obtain the licensee's Notice of Information Practices;

(4) Contain contact information for the commissioner; and

(5) Describe how the consumer can request access to or correction of their nonpublic personal information.

C. For purposes of this section "reasonable means to obtain the licensee's Notice of Information Practices" includes:

(1) Providing a toll-free telephone number that the consumer may call to request the notice;

(2) Providing a website or other electronic medium that is easily accessible by the consumer; or

(3) Maintaining copies of the notice at the licensee's place of business to be provided upon request.

Section 11~~8~~. Form of Opt-In~~Out~~ Notice to Consumers and Opt-In~~Out~~ Methods

A. ~~(1) Form of opt-out notice.~~ If a licensee is required to provide an opt-in ~~-out~~ notice under Sections ~~12A22~~20 or ~~23~~21, it shall provide a clear and conspicuous notice to each of its consumers that accurately explains the ~~right~~ information proposed to be disclosed, the use of that information, and the consumer's option to opt in to that use~~.out under that section.~~ The notice shall state:

(1)~~a)~~ ~~That T~~the licensee discloses or reserves the right to disclose nonpublic personal ~~financial~~ information about its consumer to a nonaffiliated third party;

Commented [CC14]: As drafted, this could create a burden on national or multi-state licensee as they would be required to list every relevant state commissioner's contact information on a short-form notice. We recommend either limiting this to the commissioner of the consumer's home state, or allowing a single reference to where the full list can be found, such as a website, rather than requiring every applicable commissioner's contact information in the notice itself.

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

(2b) ~~That T~~the consumer has the ~~right~~ option to opt in to ~~out of~~ that disclosure; and

(3) A reasonable means by which the consumer may exercise the option to opt in~~out right~~.

B. The licensee shall not disclose that information to a nonaffiliated third party unless the consumer has affirmatively opted in to the use.

C. The opt-in must be an affirmative act by the consumer. The licensee cannot deem a failure to respond as an opt-in or use pre-checked boxes.

D. The opt-in should be obtained separately from any other communication or consent.

E. The opt-in may be revoked at any time by the consumer.

~~(2) Examples.~~

~~(a) Adequate opt out notice. A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal financial information to a nonaffiliated third party if the licensee:~~

~~(i) Identifies all of the categories of nonpublic personal financial information that it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to which the licensee discloses the information, as described in Section 7A(2) and (3), and states that the consumer can opt out of the disclosure of that information; and~~

~~(ii) Identifies the insurance products or services that the consumer obtains from the licensee, either singly or jointly, to which the opt out direction would apply.~~

~~(b) Reasonable opt out means. A licensee provides a reasonable means to exercise an opt out right if it:~~

~~(i) Designates check-off boxes in a prominent position on the relevant forms with the opt out notice;~~

~~(ii) Includes a reply form together with the opt out notice;~~

~~(iii) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the licensee's web site, if the consumer agrees to the electronic delivery of information; or~~

~~(iv) Provides a toll-free telephone number that consumers may call to opt out.~~

~~(c) Unreasonable opt out means. A licensee does not provide a reasonable means of opting out if:~~
~~(i) The only means of opting out is for the consumer to write his or her own letter to exercise that opt out right; or~~

(ii) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the licensee provided with the initial notice but did not include with the subsequent notice.

(d) Specific opt out means. A licensee may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

B. Same form as initial notice permitted. A licensee may provide the opt out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 5.

C. Initial notice required when opt out notice delivered subsequent to initial notice. If a licensee provides the opt out notice later than required for the initial notice in accordance with Section 5, the licensee shall also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.

D. Joint relationships.

(1) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt out notice. The licensee's opt out notice shall explain how the licensee will treat an opt out direction by a joint consumer (as explained in Paragraph (5) of this subsection).

(2) Any of the joint consumers may exercise the right to opt out. The licensee may either:

(a) Treat an opt out direction by a joint consumer as applying to all of the associated joint consumers; or

(b) Permit each joint consumer to opt out separately.

(3) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all of the joint consumers.

(4) A licensee may not require all joint consumers to opt out before it implements any opt out direction.

(5) Example. If John and Mary are both named policyholders on a homeowner's insurance policy issued by a licensee and the licensee sends policy statements to John's address, the licensee may do any of the following, but it shall explain in its opt out notice which opt out policy the licensee will follow:

(a) Send a single opt out notice to John's address, but the licensee shall accept an opt out direction from either John or Mary.

(b) Treat an opt out direction by either John or Mary as applying to the entire policy. If the licensee does so and John opts out, the licensee may not require Mary to opt out as well before implementing John's opt out direction.

(c) Permit John and Mary to make different opt out directions. If the licensee does so:

© 20267 National Association of Insurance Commissioners

American Land Title Association (ALTA):

~~(i) It shall permit John and Mary to opt out for each other;~~

~~(ii) If both opt out, the licensee shall permit both of them to notify it in a single response (such as on a form or through a telephone call); and~~

~~(iii) If John opts out and Mary does not, the licensee may only disclose nonpublic personal financial information about Mary, but not about John and not about John and Mary jointly.~~

~~E. Time to comply with opt out. A licensee shall comply with a consumer's opt out direction as soon as reasonably practicable after the licensee receives it.~~

~~F. Continuing right to opt out. A consumer may exercise the right to opt out at any time.~~

~~G. Duration of consumer's opt out direction.~~

~~(1) A consumer's direction to opt out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.~~

~~(2) When a customer relationship terminates, the customer's opt out direction continues to apply to the nonpublic personal financial information that the licensee collected during or related to that relationship. If the individual subsequently establishes a new customer relationship with the licensee, the opt out direction that applied to the former relationship does not apply to the new relationship.~~

~~H. Delivery. When a licensee is required to deliver an opt out notice by this section, the licensee shall deliver it according to Section 11.~~

Section 12. Form of Opt-Out Notice to Consumers and Opt-Out Methods

A. (1) If a licensee is required to provide an opt-out notice, it shall provide a clear and conspicuous notice to each consumer that accurately explains the right to opt out under that section. To the extent applicable, the notice shall state:

(a) That the licensee discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;

(b) That the consumer has the right to opt out of that disclosure; and

(c) A reasonable means by which the consumer may exercise the opt-out right.

(2) Requirements

(a) A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if the licensee:

(i) Identifies all of the categories of nonpublic personal information it discloses or reserves the right to disclose, and all of the categories of

nonaffiliated third parties to whom the licensee discloses the information, as described in Section ~~11~~9A(2) and (3), and states the consumer can opt out of the disclosure of that information; and

(ii) Identifies the insurance products or services the consumer obtains from the licensee, either singly or jointly, to which the opt-out would apply.

(b) A licensee provides a reasonable means to exercise an opt-out right if it:

(i) Designates check-off boxes in a prominent position on the relevant forms with the opt-out notice;

(ii) Includes a reply form together with the opt–out notice;

(iii) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the licensee's website, if the consumer agrees to the electronic delivery of information; or

(iv) Provides a toll-free telephone number that consumers may call to opt out.

(c) A licensee does not provide a reasonable means of opting out if:

(i) The only means of opting out is for the consumer to write a letter to the licensee to exercise their opt-out right; or

(ii) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the licensee provided with the initial notice but did not include with the subsequent notice.

(d) A licensee may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

B. A licensee may provide the opt-out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 7.

C. If a licensee provides the opt-out notice after it provides the initial notice, the licensee shall include a copy of the initial notice with the opt-out notice in writing or, if the consumer agrees, electronically.

D. Joint relationships.

(1) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt-out notice. The licensee's opt-out notice shall explain how the licensee will treat an opt-out direction by a joint consumer (as explained in Paragraph (2) of this subsection).

(2) Any of the joint consumers may exercise the right to opt out. The licensee may either:

(a) Treat an opt-out direction by a joint consumer as applying to all of the associated joint consumers; or

(b) Permit each joint consumer to opt out separately.

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

(3) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all the joint consumers.

(4) A licensee may not require all joint consumers to opt out before it implements any opt-out direction.

E. A licensee shall comply with a consumer's opt-out direction as soon as reasonably practicable but no later than 10 days after the licensee receives it.

F. A consumer may exercise the right to opt out at any time. A consumer's direction to opt-out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.

Section 139. Revised ~~Privacy~~ Notice of Information Practices~~s~~

A. ~~General rule.~~Except as otherwise authorized in this Act~~regulation~~, a licensee shall not, directly or through an affiliate, disclose any nonpublic personal ~~financial~~ information about a consumer to a nonaffiliated third party other than as described in the initial notice that the licensee provided to that consumer under Section ~~5~~7, unless:

(1) The licensee has provided to the consumer a clear and conspicuous revised notice that accurately describes its policies and practices;

(2) The licensee has provided to the consumer a new opt-out notice;

(3) The licensee has given the consumer a reasonable opportunity, before the licensee discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(4) The consumer does not opt out.

B. Examples.

(1) Except as otherwise permitted by Sections 1~~9~~5, 20~~16~~ and 21~~17~~, a licensee shall provide a revised notice before it:

(a) Discloses a new category of nonpublic personal ~~financial~~ information to any nonaffiliated third party; or

(b) Discloses nonpublic personal ~~financial~~ information to a new category of nonaffiliated third party.~~; or~~

~~(c) Discloses nonpublic personal financial information about a former customer to a nonaffiliated third party, if that former customer has not had the opportunity to exercise an opt out right regarding that disclosure.~~

(2) A revised notice is not required if the licensee discloses nonpublic personal ~~financial~~ information to a new nonaffiliated third party that the licensee adequately described in its prior notice.

~~C. Delivery. When a licensee is required to deliver a revised privacy notice by this section, the licensee shall deliver it according to Section 11.~~

© 20<u>26</u>~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

Section 14~~0~~. ~~Privacy~~ Notice~~s~~ of Information Practices to Group Policyholders

Unless a licensee is providing notices of information practices~~privacy notices~~ directly to covered individuals described in Section 4~~F~~(G)2)(e)(i), (ii) or (iii), a licensee shall provide initial, annual and revised notices to the plan sponsor, group or blanket insurance policyholder or group annuity contract holder, or workers' compensation policyholder, in the manner described in Sections ~~9~~7~~5~~ through 13~~9~~ of this Act~~regulation~~, describing the licensee's privacy practices with respect to nonpublic personal information about individuals covered under the policies, contracts or plans. Compliance with this section satisfies the licensees initial, annual and renewal Notice of Information Practices as required by Sections 7 and 8 and delivery provisions of Section 15.

Section 15~~1~~. Delivery

A. ~~How to provide notices.~~ A licensee shall provide any notices that this Act~~regulation~~ requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer interacts with the licensee online or in some other electronic fashion, ~~agrees,~~ electronically.

B. (1) ~~Examples of reasonable expectation of actual notice.~~ A licensee may reasonably expect that a consumer will receive actual notice if the licensee:

(a) Hand-delivers a printed copy of the notice to the consumer;

(b) Mails a printed copy of the notice to the last known address of the consumer separately, or in a policy, billing or other written communication;

(c) For a consumer who conducts transactions electronically, in accordance with UETA (insert state electronic transactions act statute), posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service;

(i) The notice should be posted in a manner that enables a consumer to print or save it using programs or apps that are widely available and free of charge.

(ii) Notice is available electronically as long as it is in force.

(d) For an isolated transaction with a consumer, such as the licensee providing an insurance quote or selling the consumer travel insurance, posts the notice and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular insurance product or service.

(e) Provides the notice by any other means authorized by the commissioner.

(2) Examples of unreasonable expectation of actual notice. A licensee may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:

(a) Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or

(b) Sends the notice via electronic mail to a consumer who does not otherwise communicate with ~~obtain an insurance product or service from~~ the licensee electronically.

C. ~~Annual notices only.~~ A licensee may reasonably expect that a consumer~~ustomer~~ will receive actual notice of the licensee's ~~annual privacy n~~Notice ~~if:~~ of Information Practices if:

(1) The consumer~~ustomer~~ uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or

(2) The consumer~~ustomer~~ has requested that the licensee refrain from sending any information regarding the consumer~~ustomer~~ relationship, and the licensee's current privacy notice remains available to the consumer~~ustomer~~ upon request.

D. A licensee may not provide any notice required by this Act solely by orally explaining the notice, either in person or over the telephone.

Commented [CC15]: We recommend an exception allowing oral notice when provided as a reasonable accommodation, in addition to a written or otherwise documented notice, rather than leaving the prohibition absolute.

E. A licensee may provide a joint notice from the licensee and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the licensee and the other institutions. A licensee also may provide a notice on behalf of another financial institution.

F. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of Sections 7A, 8A and 13A, respectively, by providing one notice to those consumers jointly.

~~D. Oral description of notice insufficient. A licensee may not provide any notice required by this regulation solely by orally explaining the notice, either in person or over the telephone.~~

~~E. Retention or accessibility of notices for customers.~~

~~(1) For customers only, a licensee shall provide the initial notice required by Section 5A(1), the annual notice required by Section 6A, and the revised notice required by Section 9 so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.~~

~~(2) Examples of retention or accessibility. A licensee provides a privacy notice to the customer so that the customer can retain it or obtain it later if the licensee:~~

~~(a) Hand delivers a printed copy of the notice to the customer;~~

~~(b) Mails a printed copy of the notice to the last known address of the customer; or~~

~~(c) Makes its current privacy notice available on a web site (or a link to another web site) for the customer who obtains an insurance product or service electronically and agrees to receive the notice at the web site.~~

~~F. Joint notice with other financial institutions. A licensee may provide a joint notice from the~~

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

licensee and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the licensee and the other institutions. A licensee also may provide a notice on behalf of another financial institution.

G. Joint relationships. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of Sections 5A, 6A and 9A, respectively, by providing one notice to those consumers jointly.

ARTICLE V~~III~~. LIMITS ON DISCLOSURES OF NONPUBLIC~~FINANCIAL~~ PERSONAL INFORMATION

Section 16. General Rules for Use and Disclosure of Nonpublic Personal Information

A. Use and Disclosure

(1) A licensee may use and disclose nonpublic personal information about a consumer for purposes of processing a business transaction requested or authorized by the consumer.

(2) A licensee may disclose nonpublic personal information with affiliates, provided the affiliates' use and disclosure comply with this Act.

(3) A licensee shall not disclose nonpublic personal information to a nonaffiliated third party except as permitted by this Act.

(4) This section applies to nonpublic personal information collected before and after a consumer exercises an opt-out right under Section 19 or an opt-in right under Sections 20 and 21.

(5) If a consumer submits an opt-out request during a transaction and the requested information is necessary to complete that transaction, the licensee shall:

(a) Inform the consumer that the transaction cannot be completed without the information; and

(b) Confirm whether the consumer wishes to proceed.

B. Limits on Disclosure**.** Except as provided by Section 16A(1), before disclosing a consumer's nonpublic personal information to a nonaffiliated third party, whether directly or through an affiliate, a licensee shall:

(1) Provide the initial notice required by Section 7;

(2) Provide a clear and conspicuous notice to the consumer that details:

(a) The consumer's right to opt out of disclosure for targeted advertising under Section 19;

(b) The consumer's option to opt in to the sale of nonpublic personal information under Section 20; or

(c) The consumer's option to opt in to the disclosure of sensitive personal information Section 21.

(3) Provide a reasonable opportunity for the consumer to exercise any applicable opt-out right before disclosure; and

(4) Obtain and document the consumer's opt-in or opt-out election, as applicable.

~~**Section 12. Limits on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties**~~

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

A. (1) Conditions for disclosure. Except as otherwise authorized in this regulation, a licensee may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party unless:

(a) The licensee has provided to the consumer an initial notice as required under Section 5;

(b) The licensee has provided to the consumer an opt out notice as required in Section 8;

(c) The licensee has given the consumer a reasonable opportunity, before it discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(d) The consumer does not opt out.

(2) Opt out definition. Opt out means a direction by the consumer that the licensee not disclose nonpublic personal financial information about that consumer to a nonaffiliated third party, other than as permitted by Sections 15, 16 and 17.

(3) Examples of reasonable opportunity to opt out. A licensee provides a consumer with a reasonable opportunity to opt out if:

(a) By mail. The licensee mails the notices required in Paragraph (1) of this subsection to the consumer and allows the consumer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within thirty (30) days from the date the licensee mailed the notices.

(b) By electronic means. A customer opens an on-line account with a licensee and agrees to receive the notices required in Paragraph (1) of this subsection electronically, and the licensee allows the customer to opt out by any reasonable means within thirty (30) days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.

(c) Isolated transaction with consumer. For an isolated transaction such as providing the consumer with an insurance quote, a licensee provides the consumer with a reasonable opportunity to opt out if the licensee provides the notices required in Paragraph (1) of this subsection at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.

B. Application of opt out to all consumers and all nonpublic personal financial information.

(1) A licensee shall comply with this section, regardless of whether the licensee and the consumer have established a customer relationship.

(2) Unless a licensee complies with this section, the licensee may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer that the licensee has collected, regardless of whether the licensee collected it before or after receiving the direction to opt out from the consumer.

~~C. Partial opt out. A licensee may allow a consumer to select certain nonpublic personal financial information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out.~~

Section 1~~7~~3. Limits on Rediscloure and Reuse of Nonpublic Personal ~~Financial~~ Information

A. ~~(1) Information the licensee receives under an exception.~~ If a licensee receives nonpublic personal ~~financial~~ information from a nonaffiliated third-party service provider~~financial institution~~ under an exception in ~~Sections~~ 2016 ~~or 17~~ ~~or~~ Article VI of this Act~~regulation~~, ~~the licensee's disclosure and use of that information is limited as follows:~~

~~(a) The licensee may disclose the information to the affiliates of the financial institution from which the licensee received the information;~~

~~(b) The licensee may disclose the information to its affiliates, but the licensee's affiliates may, in turn, disclose and use the information only to the extent that the licensee may disclose and use the information; and~~

~~(a)~~ t~~T~~he licensee may use and disclose the information ~~pursuant to an exception in Sections 16 or 17 of this regulation,~~ in the ordinary course of business to carry out the activity covered by the exception under which the licensee received the information.

~~(2) Example. If a licensee receives information from a nonaffiliated financial institution for claims settlement purposes, the licensee may disclose the information for fraud prevention, or in response to a properly authorized subpoena. The licensee may not disclose that information to a third party for marketing purposes or use that information for its own marketing purposes.~~

B. (1) ~~Information a licensee receives outside of an exception.~~ If a licensee receives nonpublic personal ~~financial~~ information from a nonaffiliated third-party service provider~~financial institution~~ other than under an exception in ~~Sections~~ 20 ~~or~~ Article VI~~16 or 17~~ of this Act~~regulation~~, the licensee may disclose the information only to the following, provided the disclosure is consistent with this Act:

(a) ~~To the A~~affiliates of the third party-service provider~~financial institution~~ from which the licensee received the information; and

(b) ~~To its A~~affiliates of the licensee who may~~, but its affiliates may, in turn,~~ disclose the information only to the extent that the ~~licensee may disclose the information;~~disclosure would be permissible by the licensee pursuant to this Act. ~~and~~

~~(c) To any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which the licensee received the information.~~

(2) Example. If a licensee obtains a customer list from a nonaffiliated third-party service provider~~financial institution~~ outside of the exceptions in ~~Sections 16 or 17:~~20 ~~or~~ Article VI:

Commented [CC16]: Under existing law it is the responsibility of the party providing the information to ensure compliance via the contract process. The concept of this Section works in 672 because both entities are financial institutions subject to the same data use requirements. Expansion is problematic given the jurisdiction of the regulator and varying data use requirements. Contracts terms protect consumers when regulators do not have jurisdiction to enforce rules related to third parties.

Commented [CC17]: This section swallows the whole unintentionally through reference to third party service providers and use of the phrase "other than under an exception in Article VI of this Act." Licensees could receive personal information from a vendor necessary to effect a transaction and this would limit the licensees ability to use or share it for that purpose.

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

(a) The licensee may use that list for its own purposes~~; and~~ consistent with this Act; and

(b) The licensee may disclose that list to another nonaffiliated third-party service provider only as permitted by this Act.~~if the financial institution from which the licensee purchased the list could have lawfully disclosed the list to that third party. That is, the licensee may disclose the list in accordance with the privacy policy of the financial institution from which the licensee received the list, as limited by the opt-out direction of each consumer whose nonpublic personal financial information the licensee intends to disclose, and the licensee may disclose the list in accordance with an exception in Sections 16 or 17, such as to the licensee's attorneys or accountants.~~

C. ~~Information a licensee discloses under an exception.~~ If a licensee discloses nonpublic personal ~~financial~~ information to a nonaffiliated third-party service provider under an exception in S~~ections 16 or 17 20 or~~ Article VI of this Act~~of this regulation~~, the third party-service provider: ~~may disclose and use that information only as follows:~~

(1) ~~The third party~~ M~~m~~ay disclose the information to the licensee's affiliates; and

~~(2) The third party may disclose the information to its affiliates, but its affiliates may, in turn, disclose and use the information only to the extent that the third party may disclose and use the information; and~~

(2~~3~~) ~~The third party~~ M~~m~~ay disclose and use the information ~~pursuant to an exception in Sections 16 or 17~~ in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

D. ~~Information a licensee discloses outside of an exception.~~ If a licensee discloses nonpublic personal ~~financial~~ information to a nonaffiliated third-party service provider other than under an exception in ~~Sections 20 16 or 17 or~~ Article VI of this Act~~regulation~~, the third-party service provider may disclose the information only:

(1) To the licensee's affiliates~~;~~ who may disclose the information only to the extent that it would be permissible for the licensee to disclose the information pursuant to this Act: and

~~(2) To the third party's affiliates, but the third party's affiliates, in turn, may disclose the information only to the extent the third party can disclose the information; and~~

(2~~3~~) To any other person, if the disclosure would be lawful if the licensee made it directly to that person.

Section 1814. Limits on Sharing Access Number or Access Code~~Account Number~~ Information for Marketing Purposes

A. ~~General prohibition on disclosure of account numbers.~~ A licensee shall not, directly or through an affiliate, disclose, other than to a consumer reporting agency, a policy number or similar form of access number or access code for a consumer's policy or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

B. Exceptions. Subsection A of this section does not apply if a licensee discloses a policy number or similar form of access number or access code:

(1) To the licensee's service provider solely in order to perform marketing for the licensee's own products or services, as long as the service provider is not authorized to directly initiate charges to the account;

(2) To a licensee who is a producer solely in order to perform marketing for the licensee's own products or services; or

(3) To a participant in an affinity or similar program where the participants in the program are identified to the consumer~~ustomer~~ when the consumer~~ustomer~~ enters into the program.

(4) Where the policy number, or similar form of access number or access code, is in an encrypted form, as long as the licensee does not provide a means to decode the access number or access code.

~~C. Examples.~~

~~(1) Policy number. A policy number, or similar form of access number or access code, does not include a number or code in an encrypted form, as long as the licensee does not provide the recipient with a means to decode the number or code.~~

~~(2) Policy or transaction account. For the purposes of this section, a policy or transaction account is an account other than a deposit account or a credit card account. A policy or transaction account does not include an account to which third parties cannot initiate charges.~~

Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted ~~Marketing~~ Advertising

A. Except as otherwise authorized in this Act, a licensee may not, directly or through any affiliate, disclose for the purpose of targeted advertising any nonpublic personal information about a consumer to a nonaffiliated third party unless the consumer has been provided clear and conspicuous notice and a reasonable opportunity to opt out of targeted advertising in accordance with the requirements of Section 12 of this Act.

B. A licensee shall act on a consumer's request to opt out within 15 days of receipt.

C. A licensee is under no obligation to obtain additional information to execute the opt-out request.

© 20261~~7~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

D. A licensee may not solicit the consumer to change their election to opt -out for twelve months.

Commented [CC18]: This time period seems very long, given how frequently consumers visit websites.

E. A consumer has the right to opt out at any time.

Section 20. Limits on Sale of Nonpublic Personal Information

Before a licensee may sell nonpublic personal information:

A. The licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

B. The consumer must affirmatively opt in to the sale of their nonpublic personal information.

Section 21. Limits on Disclosure of Sensitive Personal Information

A. Except as provided by Subsection B below, a licensee may disclose a consumer's sensitive personal information only for those purposes and uses identified in Article VI and as expressly permitted or required by Article VI or other provisions of this Act.

B. Before a licensee may disclose a consumer's sensitive personal information for purposes other than those specified in subsection A of this section:

(1) A licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

(2) The consumer must affirmatively opt in to disclosure of their sensitive personal information.

© 20262~~17~~ National Association of Insurance Commissioners

ARTICLE ~~I~~V[I]. EXCEPTIONS TO LIMITS ON DISCLOSURES OF ~~FINANCIAL~~ NONPUBLIC PERSONAL INFORMATION

Section 2~~2~~5. Exception to Opt-Out Requirements for Disclosure of Nonpublic Personal ~~Financial~~ Information for Service Providers and Joint Marketing

A. General rule.

(1) The opt-out requirements in Sections 12~~-8~~ and ~~16~~2~~-~~19 do not apply when a licensee provides nonpublic personal ~~financial~~ information to a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf, if the licensee:

(a) Provides the initial notice in accordance with Section ~~9~~5~~-~~7; and

(b) Enters into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in Sections ~~25~~16 ~~or 26~~17~~-~~23 or 24 in the ordinary course of business to carry out those purposes.

(2) Example. If a licensee discloses nonpublic personal ~~financial~~ information under this section to a financial institution with which the licensee performs joint marketing, the licensee's contractual agreement with that institution meets the requirements of Paragraph (1)(b) of this subsection if it prohibits the institution from disclosing or using the nonpublic personal ~~financial~~ information except as necessary to carry out the joint marketing or under an exception in Sections ~~25~~16 ~~or 26~~17~~-~~23 or 24 in the ordinary course of business to carry out that joint marketing.

B. Service may include joint marketing. The services a nonaffiliated third party performs for a licensee under Subsection A of this section may include marketing of the licensee's own products or services or marketing of financial products or services offered pursuant to joint agreements between the licensee and one or more financial institutions.

C. Definition of "joint agreement." For purposes of this section, "joint agreement" means a written contract pursuant to which a licensee and one or more financial institutions jointly offer, endorse or sponsor a financial product or service.

Section 2~~3~~1~~6~~. Exceptions to Notice and Opt-Out Requirements for Disclosure of Nonpublic Personal ~~Financial~~ Information for Processing and Servicing Transactions

A. Exceptions for processing transactions at consumer's request. The requirements for initial notice in Section ~~9~~7~~5~~A(2), the opt-out in Sections 12~~8~~ and ~~16~~2~~-~~19, and service providers and joint marketing in Section ~~24~~15~~-~~22 do not apply if the licensee discloses nonpublic personal ~~financial~~ information as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Servicing or processing an insurance product or service that a consumer requests or authorizes;

Commented [CC19]: Requested by the consumer, but section 22 states that a licensee can share with a service provider only if it provides the initial notice required by section 7. We suggest cross-reference the exception within Section 22 directly, or clarify which provision controls when the two conflict.

© 20~~17~~26 National Association of Insurance Commissioners

American Land Title Association (ALTA):

(2) Maintaining or servicing the consumer's account with a licensee, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity;

(3) A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer; or

(4) Reinsurance or stop loss or excess loss insurance.

B. "Necessary to effect, administer or enforce a transaction" means that the disclosure is:

(1) Required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or

(2) Required, or is a usual, appropriate or acceptable method:

(a) To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer's account in the ordinary course of providing the insurance product or service;

(b) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

(c) To provide a confirmation, statement or other record of the transaction, or information on the status or value of the insurance product or service to the consumer or the consumer's agent or broker;

(d) To accrue or recognize incentives or bonuses associated with the transaction that are provided by a licensee or any other party;

(e) To underwrite insurance at the consumer's request or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects or as otherwise required or specifically permitted by federal or state law; or

(f) In connection with:

(i) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited or otherwise paid using a debit, credit or other payment card, check or account number, or by other payment means;

(ii) The transfer of receivables, accounts or interests therein; or

(iii) The audit of debit, credit or other payment information.

© 2026~~17~~ National Association of Insurance Commissioners

Section 2417. Other Exceptions to Notice and Opt-Out Requirements for Disclosure of Nonpublic Personal ~~Financial~~ Information

A. Exceptions to opt out requirements. The requirements for initial notice to consumers in Section 957A(2), the opt--out in Sections 128 and 1692, and service providers and joint marketing in Section 24195122 do not apply when a licensee discloses nonpublic personal ~~financial~~ information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

(2) (a) To protect the confidentiality or security of a licensee's records pertaining to the consumer, service, product or transaction;

(b) To protect against or prevent actual or potential fraud or unauthorized transactions;

(c) For required institutional risk control or for resolving consumer disputes or inquiries;

(d) To persons holding a legal or beneficial interest relating to the consumer; or

(e) To persons acting in a fiduciary or representative capacity on behalf of the consumer;

(f) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted nonpublic personal information.

Commented [CC20]: We suggest restoring "information systems" back into the definition of exemptions. Since security incident impacts are not limited to data impacts, we suggest there is no reason to limit this use case to preventing security incidents that could impact personal information.

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating a licensee, persons that are assessing the licensee's compliance with industry standards, and the licensee's attorneys, accountants and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the federal Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, the Securities and Exchange Commission, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance authority, and the Federal Trade Commission), self-regulatory organizations or for an investigation on a matter related to public safety;

(5) (a) To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or

(b) From a consumer report reported by a consumer reporting agency;

© 20267 National Association of Insurance Commissioners

American Land Title Association (ALTA):

(6) In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal ~~financial~~ information concerns solely consumers of the business or unit;

(7) (a) To comply with federal, state or local laws, rules and other applicable legal requirements;

(b) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities; or

(c) To respond to judicial process or government regulatory authorities having jurisdiction over a licensee for examination, compliance or other purposes as authorized by law; or

(8) For purposes related to the replacement of a group benefit plan, a group health plan, a group welfare plan or a workers' compensation plan.

B. Example of revocation of consent. A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under Section ~~12~~8F.~~.~~12F.

Drafting Note: Because the notice requirements of this Act ~~regulation~~ could be a financial burden on a company in liquidation or receivership and negatively impact the ability of the liquidator or receiver to pay claims, regulators may want to consider adding an additional exception providing that licensees in liquidation or receivership are not subject to the notice provisions of this ~~.~~ Act~~regulation~~.

© 2026~~17~~ National Association of Insurance Commissioners

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 2518. When Authorization Required for Disclosure of Nonpublic Personal Health Information

A. A licensee shall not disclose nonpublic personal health information about a consumer ~~or customer~~ unless an authorization is obtained from the consumer ~~or customer~~ whose nonpublic personal health information is sought to be disclosed.

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee: ~~claims administration; claims adjustment and management; detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity; underwriting; policy placement or issuance; loss control; ratemaking and guaranty fund functions; reinsurance and excess loss insurance; risk management; case management; disease management; quality assurance; quality improvement; performance evaluation; provider credentialing verification; utilization review; peer review activities; actuarial, scientific, medical or public policy research; grievance procedures; internal administration of compliance, managerial, and information systems; policyholder service functions; auditing; reporting; database security; administration of consumer disputes and inquiries; external accreditation standards; the replacement of a group benefit plan or workers compensation policy or program; activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit; any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services; disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes; and any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.~~

(1) Claims administration any processing~~claims~~;

(2) Claims adjustment and management;

(3) Detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity;

(4) Underwriting;

(5) Policy placement or issuance;

(6) Loss control;

(7) Ratemaking and guaranty fund functions;

(8) Reinsurance and excess loss insurance;

(9) Risk management;

© 20~~17~~26 National Association of Insurance Commissioners

American Land Title Association (ALTA):

(10) Case management;

(11) Disease management;

(12) Quality assurance;

(13) Quality improvement;

(14) Performance evaluation;

(15) Provider credentialing verification;

(16) Utilization review;

(17) Peer review activities;

(18) Actuarial, scientific, medical or public policy research;

(19) Grievance procedures;

(20) Internal administration of compliance, managerial, and information systems;

(21) Policyholder service functions;

(22) Auditing;

(23) Reporting;

(24) Database security;

(25) Administration of consumer disputes and inquiries;

(26) External accreditation standards;

(27) The replacement of a group benefit plan or workers' compensation policy or program;

(28) Activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit;

(29) Any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services or other applicable laws;

(30) Disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes including subrogation, and

(31) Any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with the legal process.

C. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable

Section ~~19~~26. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article VII shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer ~~or customer~~ who is the subject of the nonpublic personal health information;

(2) A general description of the types of nonpublic personal health information to be disclosed;

(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

~~-~~(4) The signature, including electronic signatures, of the consumer ~~or customer~~ who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer ~~or customer~~ may revoke the authorization at any time and the procedure for making a revocation.

(6) Any additional information necessary to comply with HIPAA or any other applicable law.

B. An authorization for the purposes of this Article VII shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer ~~or customer~~ who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article VII at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

E. A signed copy of the authorization shall be provided to the consumer.

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

Section 27.0. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer ~~or a customer~~ as part of an opt-out notice pursuant to Section ~~15~~12, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer ~~or customer~~ or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section ~~18~~25A.

Section 28~~1~~. Relationship to Federal Rules

A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

This Act shall not apply to nonprofits, such as the National Association of Insurance Commissioners or the National Insurance Crime Bureau, when processing or sharing information solely for investigating criminal or fraudulent insurance acts. ~~Irrespective of whether a licensee is subject to the federal Health Insurance Portability and Accountability Act privacy rule as promulgated by the U.S. Department of Health and Human Services [insert cite] (the "federal rule"), if a licensee complies with all requirements of the federal rule except for its effective date provision, the licensee shall not be subject to the provisions of this Article V.~~

~~**Drafting Note:** The drafters note that the effective date of this Act regulation is July 1, 2001. The HHS regulation is anticipated to be promulgated in late 2000, thereby becoming effective in late 2002. As of July 1, 2001, if the licensee is in compliance with all requirements of the HHS regulation except its effective date provision, the licensee is not subject to the provisions of this articlethis Article. If the licensee comes into compliance with the HHS regulation after that date, the licensee is no longer subject to the provisions of this aArticle as of the date the licensee comes into compliance with the HHS regulation.~~

Section 29~~2~~. Relationship to State Laws

Nothing in ~~this articlethis~~ Article shall preempt or supersede ~~supercede~~ existing state law related to medical records, consumer data privacy, health or insurance information privacy.

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 3023. Protection of Fair Credit Reporting Act

Nothing in this ~~regulation~~ Act shall be construed to modify, limit or supersede the operation of the ~~federal~~ Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and no inference shall be made ~~drawn on the basis of the provisions of this regulation~~ Act regarding whether information is transaction or experience information under Section 603 of that Act.

Section 3124. Nondiscrimination

A. A licensee shall not unfairly discriminate against any consumer ~~or customer~~ because that consumer ~~or customer~~ has opted out from the disclosure of his or her nonpublic personal ~~financial~~ information pursuant to the provisions of this ~~regulation~~Act.

B. A licensee shall not unfairly discriminate against a consumer ~~or customer~~ because that consumer ~~or customer~~ has not granted authorization for the disclosure of his or her nonpublic personal health information pursuant to the provisions of this ~~regulation~~Act.

Section 3225. Violation

Drafting Note: Cite state unfair trade practices act or other applicable state law.

Section 3326. Severability

If any section or portion of a section of this ~~regulation~~ Act or its applicability to any person or circumstance is held invalid by a court, the remainder of the ~~regulation~~ Act or the applicability of the provision to other persons or circumstances shall not be affected.

Section 34. Individual Remedies

This Act may not be construed to create or imply a private cause of action for violation of its provisions, nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Section 3527. Effective Date

A. Effective date. This Act~~regulation~~ has been~~is~~ effective since November 13, 2000. The amendments to this Act are effective [Insert Effective Date]. In order to provide sufficient time for licensees to establish policies and systems to comply with the amendments~~requirements~~ to~~of~~ this ~~regulation~~Act, the commissioner has extended the time for compliance with the~~is~~ amendments to this Act~~regulation~~ until [Insert Compliance Date]~~July 1, 2001~~.

B. ~~(1)~~ By [Insert Compliance Date], a licensee shall provide an initial notice, as required by Section 7, to any existing consumer who has not previously received a notice that complies with the amendments to this Act. ~~Notice requirement for consumers who are the licensee's customers on the compliance date. By July 1, 2001, a licensee shall provide an initial notice, as required by Section 5, to consumers who are the licensee's customers on July 1, 2001.~~

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

~~(2) Example. A licensee provides an initial notice to consumers who are its customers on [Insert Date]July 1, 2001, if, by that date, the licensee has established a system for providing an initial notice to all new customers and has mailed the initial notice to all the licensee's existing customers.~~

C. Two-year grandfathering of service agreements. Until [Insert Compliance Date]~~July 1, 2002~~, a contract that a licensee has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf satisfies the provisions of Section ~~15~~22A(1)(b) of this ~~regulation~~Act, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the licensee entered into the agreement on or before [Insert Compliance Date]~~July 1, 2000~~.

Commented [CC21]: We suggest a general 2-plus year compliance runway from each state's enactment date, rather than the current draft's narrower two-year grandfather limited to existing vendor contracts. This would ensure the minimization of compliance risks and regulatory burdens when adapting to the new rules.

APPENDIX A – SAMPLE CLAUSES

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A-1–Categories of information a licensee collects (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section ~~7A~~9A(1) to describe the categories of nonpublic personal information the licensee collects.

Sample Clause A-1:

We collect nonpublic personal information about you from the following sources:

Information we receive from you on applications or other forms;
Information about your transactions with us, our affiliates or others; and
Information we receive from a consumer reporting agency.

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-1 expires on July 1, 2019.~~

A-2–Categories of information a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use one of these clauses, as applicable, to meet the requirement of Section ~~7A~~9A(2) to describe the categories of nonpublic personal information the licensee discloses. The licensee may use these clauses if it discloses nonpublic personal information other than as permitted by the exceptions in Sections ~~15~~22, ~~16~~ 23 and ~~17~~24.

Sample Clause A-2, Alternative 1:

We may disclose the following kinds of nonpublic personal information about you:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premiums, and payment history"]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your creditworthiness and credit history"].

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-2, Alternative 1 expires on July 1, 2019.~~

Sample Clause A-2, Alternative 2:

We may disclose all of the information that we collect, as described [describe location in the notice, such as "above" or "below"].

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-2, Alternative 2 expires on July 1, 2019.~~

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

A-3–Categories of information a licensee discloses and parties to whom the licensee discloses (institutions that do not disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirements of Sections ~~7A~~9A(2) and~~,~~ (3)~~, and (4)~~ to describe the categories of nonpublic personal information ~~about customers and former customers that~~ the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses. A licensee may use this clause if the licensee does not disclose nonpublic personal information to any party, other than as permitted by the exceptions in Sections ~~16~~ 23 and ~~17~~24.

Sample Clause A-3:

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-3 expires on July 1, 2019.~~

A-4–Categories of parties to whom a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section ~~7A~~9A(3) to describe the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information. This clause may be used if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections ~~15~~22, ~~16~~ 23 and ~~17~~24~~, as well as when permitted by the exceptions in Sections 16 and 17~~.

Sample Clause A-4:

We may disclose nonpublic personal information about you to the following types of third parties:

Financial service providers, such as [provide illustrative examples, such as "life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents"];

Non-financial companies, such as [provide illustrative examples, such as "retailers, direct marketers, airlines, and publishers"]; and

Others, such as [provide illustrative examples, such as "non-profit organizations"].

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-4 expires on July 1, 2019.~~

A-5–Service provider/joint marketing exception
A licensee may use one of these clauses, as applicable, to meet the requirements of Section ~~7A~~9A(~~5~~2) related to the exception for service providers and joint marketers in Section ~~15~~22. If a licensee discloses nonpublic personal information under this exception, the licensee shall describe the categories of nonpublic personal information the licensee discloses and the categories of third parties with which the licensee has contracted.

Sample Clause A-5, Alternative 1:

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premium, and payment history"]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your creditworthiness and credit history"].

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-5, Alternative 1 expires on July 1, 2019.~~

Sample Clause A-5, Alternative 2:

We may disclose all of the information we collect, as described [describe location in the notice, such as "above" or "below"] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-5, Alternative 2 expires on July 1, 2019.~~

A-6–Explanation of opt- out right (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section ~~7A~~9A(~~6~~4) to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. The licensee may use this clause if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections ~~15~~22, ~~16~~23 and ~~17~~24.

Sample Clause A-6:

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [describe a reasonable means of opting out, such as "call the following toll-free number: (insert number)].

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-6 expires on July 1, 2019.~~

A-7–Confidentiality and security (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section ~~7A~~9A(8) to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A-7:

We restrict access to nonpublic personal information about you to [provide an appropriate description, such as "those employees who need to know that information to provide products or services to you"]. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-7 expires on July 1, 2019.~~

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

APPENDIX B – FEDERAL MODEL PRIVACY FORM

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the Federal Model Privacy Form, if the Form is accurate for each institution that uses the Form. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A. General Instructions

1. How the Model Privacy Form is used.

(a) The Model Form may be used, at the option of a "licensee"~~)~~, including a group of licensees or other financial institutions that use a common privacy notice, to meet the content requirements of the privacy notice and opt-out notice set forth in [insert citation for sections of statute or regulation sections that parallel Sections ~~7~~ 9and ~~8~~ 11 of the NAIC *Privacy of Consumer ~~Financial and Health~~ Information ~~Act~~Regulation*]

(b) The Model Form is a standardized form, including page layout, content, format, style, pagination, and shading. Licensees seeking to obtain the safe harbor through use of the Model Form may modify it only as described in these Instructions.

(c) Note that disclosure of certain information, such as assets, income, and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act (FCRA), codified at 15 U.S.C. §§ 1681-1681x, such as a requirement to permit a consumer to opt out of disclosures to affiliates, or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.

(d) The word "consumer~~ustomer~~" may be replaced by the word "member," whenever it appears in the Model Form, as appropriate.

2. The Contents of the Model Privacy Form

The Model Form consists of two pages, which may be printed on both sides of a single sheet of paper or may appear on two separate pages. Where a licensee provides a long list of licensees or financial institutions at the end of the Model Form in accordance with Instruction B3(a)(i), or provides additional information in accordance with Instruction B3(c) and such list or additional information exceeds the space available on Page Two of the Model Form, such list or additional information may extend to a third page.

(a) Page One. The first page consists of the following components:

(1) Date last revised (upper right-hand corner)
(2) Title
(3) Key frame (Why? What? How?)
(4) Disclosure table ("Reasons we can share your personal information")
(5) "To limit our sharing" box, as needed, for the licensee's opt-out information
(6) "Questions" box, for customer service contact information
(7) Mail-in opt-out form, as needed

(b) Page Two. The second page consists of the following components:

© 2026~~17~~ National Association of Insurance Commissioners

(1) Heading (Page 2)
(2) Frequently Asked Questions ("Who we are" and "What we do")
(3) Definitions
(4) "Other important information" box, as needed

3. The format of the Model Privacy Form.

The format of the Model Form may be modified only as described below.

(a) Easily readable type font. Licensees that use the Model Form must use an easily readable type font. While a number of factors together produce easily readable font, licensees are required to use a minimum of 10-point font (unless otherwise expressly permitted in these Instructions) and sufficient spacing between lines.

(b) Logo. A licensee may include a corporate logo on any page of the notice, so long as it does not interfere with the readability of the Model Form or the space constraints of each page.

(c) Page size and orientation. Each page of the Model Form must be printed in portrait orientation, the size of which must be sufficient to meet the layout and minimum font size requirements, with sufficient white space on the top, bottom, and sides of the content.

(d) Color. The Model Form must be printed on white or light color paper (such as cream) with black or other contrasting ink color. Spot color may be used to achieve visual interest, so long as the color contrast is distinctive and the color does not detract from the readability of the Model Form. Logos may also be printed in color.

(e) Languages. The Model Form may be translated into languages other than English.

B. Information Required in the Model Privacy Form

The information in the Model Form may be modified only as described below:

1. Name of licensee or group of affiliated licensees or institutions providing the notice
Insert the name of the licensee providing the notice, or a common identity of the affiliated licensees or financial institutions jointly providing the notice on the form, wherever [name of licensee] appears.

2. Page One

(a) Last revised date. The licensee must insert in the upper right-hand corner the date on which the notice was last revised. The information shall appear in minimum 8-point font as "rev. [month/year]" using either the name or number of the month, such as "rev. July 2016" or "rev. 7/16."

(b) General instructions for the "What?" box

(i) The bulleted list identifies the types of personal information that the licensee collects and shares. All licensees must use the term "Social Security Number" in the first bullet.

(ii) A licensee must use five (5) of the following terms, to complete the bulleted list: income; account balances; payment history; transaction history; transaction or loss history; credit history; credit scores; assets; investment experience; credit-based insurance scores; insurance claim history; medical information; overdraft

© 20~~17~~26 National Association of Insurance Commissioners

American Land Title Association (ALTA):

history; purchase history; account transactions; risk tolerance; medical-related debts; credit card or other debt; mortgage rates and payments; retirement assets; checking account information; employment information; wire transfer instructions.

(c) General instructions for the disclosure table. The left column lists reasons for sharing or using personal information. Each reason correlates to a specific legal provision described in Paragraph 2(d) of this Instruction. In the middle column, each licensee must provide a "Yes" or "No" response that accurately reflects its information-sharing policies and practices with respect to the reason listed on the left. In the right column, each licensee must provide in each box one of the following three (3) responses, as applicable, that reflects whether a consumer can limit such sharing:

"Yes," if it is required to or voluntarily provides an opt-out; "No," if it does not provide an opt-out; or

"We don't share," if it answers "No" in the middle column.

Only the sixth row ("For our affiliates to market to you") may be omitted at the option of the licensee. See Paragraph 2(d)(6) of this instruction.

(d) Specific disclosures and corresponding legal provisions

(i) For our everyday business purposes. This reason incorporates sharing information under [insert citation for sections of statute or regulation sections that parallel Sections ~~16~~ 23 and ~~17~~ 24 of NAIC model *Privacy of Consumer ~~Financial and Health~~ Information ~~Regulation~~Act*] and with service providers pursuant to [insert citation for section of statute or regulation that parallels Section ~~15~~ 22 of NAIC *Privacy of Consumer ~~Financial and Health~~ Information Act~~Regulation~~*] other than the disclosures described in Paragraphs (2)(d)(ii) or (2)(d)(iii) of this instruction.

(ii) For our marketing purposes. This reason incorporates sharing information with service providers by a licensee for its own marketing pursuant to [insert citation for section of statute or regulation that parallels Section ~~15~~ 22 of NAIC *Privacy of Consumer ~~Financial and Health~~Information ~~Regulation~~Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iii) For joint marketing with other financial companies. This reason incorporates sharing information under joint marketing agreements between 2 or more licensees or financial institutions and with any service provider used in conjunction with such agreement pursuant to [insert citation for section of statute or regulation that parallels Section ~~15~~ 22 of NAIC *Privacy of Consumer ~~Financial and Health~~Information ~~Regulation~~Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iv) For our affiliates' everyday business purposes – information about transactions and experiences. This reason incorporates sharing information specified in Sections 603(d)(2)(A)(i) and (ii) of the FCRA. A licensee that shares information for this reason may choose to provide an opt-out.

(v) For our affiliates' everyday business purposes – information about creditworthiness. This reason incorporates sharing information pursuant to Section 603(d)(2)(A)(iii) of the FCRA. A licensee that shares information for this reason must provide an opt-out.

(vi) For our affiliates to market to you. This reason incorporates sharing information specified in Section 624 of the FCRA. This reason may be omitted from the disclosure table when: the licensee does not have affiliates (or does not disclose personal information to its affiliates); the licensee's affiliates do not use personal information in a manner that requires an opt-out; or the licensee provides the affiliate marketing notice separately. Licensees

© 2026~~17~~ National Association of Insurance Commissioners

that include this reason must provide an opt-out of indefinite duration. A licensee that is required to provide an affiliate marketing opt-out, but does not include that opt-out in the Model Form under this part, must comply with Section 624 of the FCRA and [insert citation for statute or regulation that parallels NAIC *Privacy of Consumer ~~Financial and Health~~ Information Act~~Regulation~~*], with respect to the initial notice and opt-out and any subsequent renewal notice and opt-out. A licensee not required to provide an opt-out under this subparagraph may elect to include this reason in the Model Form.

(vii) For nonaffiliates to market to you. This reason incorporates sharing described in [insert citation for sections of statute or regulation sections that parallel Sections ~~8~~ 11 and ~~12(A)~~16(B) of NAIC *Privacy of Consumer ~~Financial and Health~~ Information Act~~Regulation~~*]. A licensee that shares personal information for this reason must provide an opt-out.

(e) To limit our sharing. A licensee must include this section of the Model Form only if it provides an opt-out. The word "choice" may be written in either the singular or plural, as appropriate. Licensees must select one or more of the applicable opt-out methods described: telephone, such as by a toll-free number; a web site; or use of a mail-in opt-out form. Licensees may include the word "toll-free" before telephone, as appropriate. A licensee that allows consumers to opt out online must provide either a specific web address that takes consumers directly to the opt-out page or a general web address that provides a clear and conspicuous direct link to the opt-out page. The opt-out choices made available to the consumer who contacts the licensee through these methods must correspond accurately to the "Yes" responses in the third column of the disclosure table. In the part entitled "Please note," licensees may insert a number that is 30 days or greater in the space marked "[30]." Instructions on voluntary or state privacy law opt-out information are in Paragraph 2(g)(v) of these Instructions.

(f) Questions box. Customer service contact information must be inserted as appropriate where [phone number] or [web site] appear. Licensees may elect to provide either a phone number, such as a toll-free number, or a web address, or both. Licensees may include the words "toll-free" before the telephone number, as appropriate.

(g) Mail-in opt-out form. Licensees must include this mail-in form only if they state in the "To limit our sharing" box that consumers can opt out by mail. The mail-in form must provide opt-out options that correspond accurately to the "Yes" responses in the third column of the disclosure table. Licensees that require consumers to provide only name and address may omit the section identified as "[account #]." Licensees that require additional or different information, such as a random opt-out number or a truncated account number to implement an opt-out election should modify the "[account #]" reference accordingly. This includes licensees that require customers consumers with multiple accounts to identify each account to which the opt-out should apply. A licensee must enter its opt-out mailing address in the far right of this form (see version 3); or below the form (see version 4). The reverse side of the mail-in opt-out form must not include any content of the Model Form.

(i) Joint accountholder. Only licensees that provide their joint accountholders the choice to opt out for only one accountholder, in accordance with Paragraph 3(a)(5) of these Instructions, must include in the far left column of the mail-in form the following statement:

If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.

□ Apply my choice(s) only to me.

The word "choice" may be written in either the singular or plural, as appropriate. Licensees that provide insurance products or services, provide this option, and elect to use the Model Form may substitute the word "policy" for "account" in this statement. Licensees that do not provide this option may eliminate this left column from the mail-in form.

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

(ii) FCRA Section 603(d)(2)(A)(iii) opt-out. If the licensee shares personal information pursuant to Section 603(d)(2)(A)(iii) of the FCRA, it must include in the mail-in opt-out form the following statement:

□ Do not share information about my creditworthiness with your affiliates for their everyday business purposes.

(iii) FCRA Section 624 opt-out. If the licensee uses Section 624 of the FCRA, in accord with paragraph 2(d)(6) of these Instructions, it must include in the mail-in opt-out form the following statement:

□ Do not allow your affiliates to use my personal information to market to me.

(iv) Nonaffiliate opt-out. If the licensee shares personal information pursuant to [insert citation for section of statute or regulation that parallels Section ~~12(A)~~16(B) of NAIC *Privacy of Consumer ~~Financial and Health~~ Information ~~Act~~Regulation*], it must include in the mail-in opt-out form the following statement:

□ Do not share my personal information with nonaffiliates to market their products and services to me.

(v) Additional opt-outs. Licensees that use the disclosure table to provide opt-out options beyond those required by Federal law must provide those opt-outs in this section of the Model Form. A licensee that chooses to offer an opt-out for its own marketing in the mail-in opt-out form must include one of the two following statements:

□ Do not share my personal information to market to me. or

□ Do not use my personal information to market to me.

A licensee that chooses to offer an opt-out for joint marketing must include the following statement:

□ Do not share my personal information with other financial institutions to jointly market to me.

(h) Barcodes. A licensee may elect to include a barcode and/or "tagline" (an internal identifier) in 6-point type at the bottom of page one, as needed for information internal to the licensee, so long as these do not interfere with the clarity or text of the form.

3. Page Two

(a) General Instructions for the Questions. Certain Questions on the Model Form may be customized as follows:

(i) "Who is providing this notice?" This question may be omitted where only one licensee provides the Model Form and that licensee is clearly identified in the title on Page One. Two or more licensees or financial institutions that jointly provide the Model Form must use this question to identify themselves as required by [insert citation for section of statute or regulation that parallels Section ~~11(F)~~15(E) of NAIC model *Privacy of Consumer ~~Financial and Health~~ Information ~~Act~~Regulation*]. Where the list of licensees or financial institutions exceeds four (4) lines, the licensee must describe in the response to this question the general types of licensees or financial institutions jointly providing the notice and must separately identify those licensees or financial institutions, in minimum 8-point font, directly following the "Other important information" box, or, if that box is not included in the licensee's form, directly following the "Definitions." The list may appear in a multi- column format.

© 2026~~17~~ National Association of Insurance Commissioners

(ii) "How does [name of licensee] protect my personal information?" The licensee may only provide additional information pertaining to its safeguards practices following the designated response to this question. Such information may include information about the licensee's use of cookies or other measures it uses to safeguard personal information. Licensees are limited to a maximum of 30 additional words.

(iii) "How does [name of licensee] collect my personal information?" Licensees must use five (5) of the following terms to complete the bulleted list for this question: open an account; deposit money; pay your bills; apply for a loan; use your credit or debit card; seek financial or tax advice; apply for insurance; pay insurance premiums; file an insurance claim; seek advice about your investments; buy securities from us; sell securities to us; direct us to buy securities; direct us to sell your securities; make deposits or withdrawals from your account; enter into an investment advisory contract; give us your income information; provide employment information; give us your employment history; tell us about your investment or retirement portfolio; tell us about your investment or retirement earnings; apply for financing; apply for a lease; provide account information; give us your contact information; pay us by check; give us your wage statements; provide your mortgage information; make a wire transfer; tell us who receives the money; tell us where to send the money; show your government-issued ID; show your driver's license; order a commodity futures or option trade.

Licensees that collect personal information from their affiliates and/or credit bureaus must include the following statement after the bulleted list: "We also collect your personal information from others, such as credit bureaus, affiliates, or other companies." Licensees that do not collect personal information from their affiliates or credit bureaus but do collect information from other companies must include the following statement instead: "We also collect your personal information from other companies." Only licensees that do not collect any personal information from affiliates, credit bureaus, or other companies can omit both statements.

(iv) "Why can't I limit all sharing?" Licensees that describe state privacy law provisions in the "Other important information" box must use the bracketed sentence: "See below for more on your rights under state law." Other licensees must omit this sentence.

(v) "What happens when I limit sharing for an account I hold jointly with someone else?" Only licensees that provide opt-out options must use this question. Other licensees must omit this question. Licensees must choose one of the following two statements to respond to this question: "Your choices will apply to everyone on your account." or "Your choices will apply to everyone on your account—unless you tell us otherwise." Licensees may substitute the word "policy" for "account" in these statements.

(b) General Instructions for the Definitions. The licensee must customize the space below the responses to the three definitions in this section. This specific information must be in italicized lettering to set off the information from the standardized definitions.

(i) Affiliates. As required by [insert citation for section of statute or regulation that parallels Section ~~7~~9(A)(3) of NAIC *Privacy of Consumer ~~Financial and Health~~ Information ~~Regulation~~Act*], where [affiliate information] appears, the licensee must:

(a) If it has no affiliates, state: "[name of licensee] has no affiliates";

(b) If it has affiliates but does not share personal information with them, state: "[name of licensee] does not share with our affiliates"; or

(c) If it shares with its affiliates, state, as applicable: "Our affiliates include companies with a [common corporate identity of licensee] name; financial companies such as [insert illustrative list of companies]; nonfinancial companies, such as [insert illustrative list of companies]; and others, such as [insert illustrative list]."

© 2026~~17~~ National Association of Insurance Commissioners

American Land Title Association (ALTA):

(ii) Nonaffiliates. As required by [insert citation for section of statute or regulation that parallels Section ~~7(C)~~(9)(A)(3) of NAIC *Privacy of Consumer ~~Financial and Health~~ Information ~~Act~~Regulation*], where [nonaffiliate information] appears, the licensee must:

(a) If it does not share with nonaffiliated third parties, state: "[name of licensee] does not share with nonaffiliates so they can market to you"; or

(b) If it shares with nonaffiliated third parties, state, as applicable: "Nonaffiliates we share with can include [list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations]."

(iii) Joint Marketing. As required by [insert citation for section of statute or regulation that parallels Section ~~15~~ 22 of NAIC *Privacy of Consumer ~~Financial and Health~~ Information Act~~Regulation~~*], where [joint marketing] appears, the licensee must:

(a) If it does not engage in joint marketing, state: "[name of licensee] doesn't jointly market"; or

(b) If it shares personal information for joint marketing, state, as applicable: "Our joint marketing partners include [list categories of companies such as credit card companies]."

(c) General instructions for the "Other important information" box. This box is optional. The space provided for information in this box is not limited, and an additional page may be used if necessary. Only the following types of information can appear in this box:

(i) State and/or international privacy law information; and/or

(ii) A form by which the consumer may acknowledge receipt of the notice.

Chronological Summary of Actions (all references are to the Proceedings of the NAIC)

2000 Proc. 3rd Quarter 7, 10, 14-36, 904 (adopted).
2002 Proc. 3rd Quarter12, 13, 71, 72-73 (amended).
2017 Spring National Meeting (amended).

© 2026~~17~~ National Association of Insurance Commissioners

Version 1:
Model Form with No Opt-Out

Rev. [insert date]

FACTS	WHAT DOES [Name of Licensee] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores] When you are *no longer* our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

Questions?	Call [phone number] or go to [web site]

© 20~~26~~17 National Association of Insurance Commissioners

American Land Title Association (ALTA):

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026~~17~~ National Association of Insurance Commissioners

Version 2: Model Form with Opt-Out by Telephone and/or Online

Rev. [insert date]

FACTS	WHAT DOES [NAME OF LICENSEE] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

To limit our sharing	■ Call [phone number] —our menu will prompt you through your choice(s) **or** ■ Visit us online: [web site] **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

© 20267 National Association of Insurance Commissioners

American Land Title Association (ALTA):

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

Rev. [insert date

Version 3: Model Form with Mail-in Opt-Out Form

FACTS	WHAT DOES **[NAME OF LICENSEE]** DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ▪ Social Security number and [income] ▪ [account balances] and [payment history] ▪ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

© 20267 National Association of Insurance Commissioners

American Land Title Association (ALTA):

Page 2

To limit our sharing	▪ Call [phone number] —our menu will prompt you through your choice(s) ▪ Visit us online: [web site] or ▪ Mail the form below **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

Mail-in Form

Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless your mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me.	
	Name	
	Address	
	City, State, Zip	
	[Account #]	
Mail To:	[Name of Licensee] [Address] [City], [ST] [ZIP]	

© 2026~~17~~ National Association of Insurance Commissioners

Page 3

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ▪ [open an account] or [deposit money] ▪ pay your bills] or [apply for a loan] ▪ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ▪ sharing for affiliates' everyday business purposes—information about your creditworthiness ▪ affiliates from using your information to market to you ▪ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ▪ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ▪ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ▪ *[joint marketing information]*
Other important information	
[insert other important information]	

© 20267 National Association of Insurance Commissioners

American Land Title Association (ALTA):

Version 4: Optional Mail-in Form

Mail-in Form	
Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me. **Name** **Address** **City, State, Zip** **[Account #]**
Mail To:	[Name of Licensee], [Address 1], [Address 2], [City], [ST] [ZIP]

American Property Casualty Insurance Association℠
INSURING AMERICA apci.org

September 22, 2026

RE: *APCIA Comments on Revised Privacy of Consumer Financial and Health Information Regulation (#672)*

Dear Chair Dwyer and Members of the Privacy Protections (H) Working Group:

Thank you for the opportunity to provide comments on the Privacy Protections (H) Working Group's revised draft of the Privacy of Consumer Financial and Health Information Regulation (#672). APCIA appreciates the significant time, effort, and thoughtful consideration the Working Group has devoted to this project over the course of several years. We value the Working Group's collaborative approach and its commitment to ensuring that stakeholder perspectives are heard and considered throughout the drafting process.

APCIA strongly supports the protection of consumer privacy and recognizes the importance of periodically modernizing regulatory frameworks to reflect evolving technologies, consumer expectations, and business practices. We share the Working Group's goal of developing a modernized privacy framework that promotes consumer trust while providing clear, practical, and workable standards for insurers.

The revised draft represents an important milestone in this effort and reflects significant progress over the course of the Working Group's deliberations. At the same time, members continue to identify several areas where additional refinement is needed to ensure the model is clear, workable, and capable of implementation across the insurance industry. In particular, members have raised concerns regarding: (1) foundational definitions and the resulting scope of the model; (2) the operational feasibility of access, correction, and deletion rights; (3) third-party service provider requirements and related liability standards; (4) the treatment of sale, targeted advertising, and sensitive personal information; (5) harmonization with existing privacy frameworks and insurance regulatory requirements; and (6) implementation timelines necessary to operationalize the proposed changes.

While the revised draft reflects substantial progress, members continue to view several foundational provisions, particularly those related to definitions and scope, as critical issues that merit careful consideration given their impact throughout the remainder of the model.

Many of these concerns stem from the fact that the definitions drive the rest of the model. Decisions about scope, who is covered, and what information is protected have downstream impacts throughout the framework. For that reason, we believe it is important to get those foundational provisions right before the model is finalized.

Privacy is an important matter, and any insurance-specific privacy framework should account for the unique nature of insurance operations, align with the broader regulatory landscape governing financial institutions, and appropriately reflect existing state and federal requirements. Modernization and workability are not competing objectives. A successful model should provide meaningful consumer

protections while remaining practical, reasonable, and capable of implementation across a diverse insurance marketplace.

APCIA believes this draft provides a strong foundation for continued discussion and refinement. We appreciate the opportunity to provide feedback and look forward to continuing to work with the Working Group and interested stakeholders to develop a framework that protects consumers, supports regulatory consistency, and can be successfully implemented by the industry.

To assist the Working Group's review, APCIA has organized member feedback according to the structure of the draft. Where appropriate, APCIA has also included selected drafting suggestions in the attached appendix to illustrate potential approaches for addressing several of the concerns identified below. While not every concern identified during member review is reflected below, the comments focus on the areas that generated the most significant feedback and where members believe additional refinement would improve clarity, workability, and implementation.

Detailed Comments and Recommendations

As discussed above, APCIA supports the goal of modernizing Model #672 and strengthening consumer privacy protections. The comments below focus on several overarching themes that consistently emerged during member review, including: (1) foundational definitions and scope; (2) consumer rights provisions; (3) third-party service provider requirements; (4) sale, targeted advertising, and sensitive data provisions; (5) harmonization with existing privacy and insurance regulatory frameworks; and (6) implementation and transition considerations. Across nearly every topic area, implementation and transition planning will be critical considerations given the breadth of the proposed changes. These issues are discussed in greater detail below and organized according to the structure of the draft.

Consumer (Article 1; Section 4)

> The draft substantially expands the definition of "consumer" beyond the longstanding GLBA consumer/customer framework. This definition change is one of the most consequential revisions in the draft because it expands obligations throughout the model, including notice requirements, access rights, correction rights, and deletion rights. By eliminating the distinction between consumers and customers, the definition appears to encompass former customers, claimants, insureds who did not purchase the policy, beneficiaries, quote applicants, and other individuals with indirect relationships to a licensee. This expansion would significantly increase privacy notice obligations and the population eligible to exercise consumer rights, while creating substantial new compliance obligations and operational burdens with limited corresponding consumer benefit. The practical impact of this change extends throughout the model. For example, annual notice obligations and other ongoing compliance requirements could apply to individuals who do not maintain a customer relationship with the insurer, including certain applicants, claimants, beneficiaries, and other third parties. In many cases, insurers may not possess or maintain contact

information for these individuals. The treatment of claimants is particularly unclear and appears broader than may have been intended. As drafted, the definition could be read to include claimants under commercial auto or commercial general liability policies, rather than being limited to workers' compensation claimants. Clarification is needed regarding which categories of claimants are intended to be covered. Additionally, several operative provisions continue to reference concepts associated with a customer relationship, creating potential inconsistencies within the draft following removal of the customer definition.

The draft's elimination of the longstanding consumer/customer distinction raises not only operational concerns but also drafting concerns. Several provisions throughout the draft continue to rely on concepts traditionally tied to an ongoing customer relationship. Preserving the consumer/customer framework would improve consistency throughout the model and better align notice, access, and other obligations with established GLBA principles. The removal of the customer framework also appears to create tension throughout the draft between obligations intended for individuals who maintain an ongoing insurance relationship and those that would now apply to a much broader population. As a result, provisions that historically operated within a customer-based framework may now have significantly different implications for claimants, beneficiaries, applicants, and other individuals who do not have an ongoing relationship with the insurer.

Beyond the operational implications, this issue goes to the fundamental scope of the model. The consumer/customer distinction has long served as a cornerstone of both GLBA and Model #672, helping to define when privacy obligations attach and what information-sharing expectations consumers should reasonably have. Moving away from that framework would represent a significant policy shift and should be carefully evaluated given the downstream effects throughout the model.

Suggested Revision: Retain the existing Model #672 consumer/customer framework, including restoring the customer and customer relationship concepts that currently form the basis for several operative provisions throughout the draft. At a minimum, narrow the definition of consumer, clarify that any reference to claimants is limited to workers' compensation claimants (if that is the intended scope), clarify the treatment of beneficiaries, and limit obligations where the licensee does not have sufficient contact information or does not maintain an ongoing relationship with the individual. APCIA has included illustrative drafting suggestions in the attached appendix reflecting one potential approach to restoring the consumer/customer framework and clarifying the scope of covered individuals.

Personally Identifiable Information (PII) (Article 1; Section 4)

The definition appears broader than information that is actually identifiable to a specific individual and includes examples that may not independently identify a consumer. Several examples appear more consistent with personal information than personally identifiable information. As drafted, the definition could substantially expand the scope of regulated data beyond existing insurance and financial privacy frameworks. It may also extend beyond insurer-consumer interactions and potentially encompass information relating to business contacts, witnesses, third parties, or other individuals who are not traditionally viewed as consumers under insurance privacy frameworks.

Suggested Revision: Require a clear nexus between the information and an identifiable individual. Reevaluate examples such as payment history, account balance information, and customer status to ensure they are only included when linked to a specific consumer.

Nonpublic Personal Information (Article 1; Section 4)

The proposed definition is broader than the existing GLBA-based framework and may result in nearly all information collected by insurers being treated as nonpublic personal information. The draft also removes longstanding concepts regarding publicly available information. As drafted, the definition could extend beyond traditional insurer-consumer relationships and potentially capture information relating to business contacts, witnesses, public officials, service providers, or other individuals who are not the intended subjects of an insurance privacy framework. Significantly, the current definition departs significantly from the GLBA framework and may require extensive new data mapping and classification efforts without providing corresponding consumer value.

Suggested Revision: Retain the existing Model #672 definition or otherwise align the definition more closely with GLBA. Restore exclusions for publicly available information and clarify that publicly available names and addresses, as well as certain business or employment relationship information, are not NPI.

Sale (Article 1; Section 4)

The proposed definition of "sale" may be overly broad. The inclusion of "valuable consideration" could create uncertainty regarding common insurance, marketing, analytics, and service-provider arrangements, including lead generation, comparative raters, embedded insurance models, and marketing partnerships. As drafted, the definition may capture activities that consumers would not reasonably view as a sale of information.

Suggested Revision: Limit "sale" to exchanges involving monetary consideration. Clarify that customary insurance, marketing, analytics, distribution, and service-provider arrangements are not considered sales, or provide insurance-specific exclusions and examples.

Undefined terms (Article 1; Section 4)

APCIA also encourages the Working Group to review the draft for terms that carry operational significance but are currently undefined or inconsistently used. Several undefined relationship-based concepts, including "existing consumer," have significant implications for notice obligations, consumer rights, and implementation requirements throughout the draft. Greater definitional clarity would improve consistency and facilitate implementation.

Suggested Revision: Define key operational terms, including, but not limited to, “customer,” “existing consumer,” “existing customer,” "genetic information," "processing," "affirmative act," and "data integrity," or otherwise clarify how those terms should be interpreted and applied.

Harmonization (Overarching Concern)

The draft departs in significant ways from GLBA, existing Model #672, state comprehensive privacy laws, and other established privacy frameworks. While modernization is important and appropriate, members are concerned that the cumulative effect of the proposed changes could result in a largely standalone insurance privacy framework that differs significantly from the frameworks consumers, insurers, and regulators have relied upon for many years. Modernization should build upon proven privacy principles and established consumer expectations, not create a separate regime that increases complexity for consumers and regulated entities without clear corresponding benefits.

Suggested Revision: Align definitions, consumer rights provisions, consent mechanisms, and service-provider obligations with established frameworks where possible to reduce fragmentation and improve the likelihood of broad adoption.

Third-Party Service Providers (Article II; Section 5)

APCIA members consistently identified the third-party service provider provisions as one of their top concerns. The draft would require substantial changes to existing vendor, MGA, TPA, reinsurer, and other third-party relationships and, in some cases, would impose obligations that may be outside a licensee's practical control. Several provisions also appear to require insurers to impose requirements on subcontractors and downstream entities with whom they have no direct contractual relationship. These provisions raise practical concerns regarding contractual privity, enforceability, and the allocation of responsibility between insurers and third-party service providers. In addition, the provision making a licensee fully responsible for third-party service provider compliance departs from the risk-based oversight approaches reflected in many existing legal and regulatory frameworks and may effectively require insurers to assume responsibility for activities outside their direct control.

Importantly, many insurers have already undertaken significant contract remediation efforts to comply with comprehensive state privacy laws and other regulatory requirements. Requiring broad re-papering of existing agreements may create substantial costs and operational burdens,

particularly where existing contracts already contain robust privacy, confidentiality, and security provisions.

Suggested Revisions: APCIA recommends a more traditional, risk-based approach to third-party oversight that recognizes the practical limits of a licensee's control over independent service providers. The draft should clarify the treatment of MGAs, TPAs, reinsurers, and similar entities, avoid imposing contractual requirements that may not be commercially negotiable, and provide a practical transition framework that allows existing agreements to be updated through ordinary renewal and renegotiation cycles rather than requiring large-scale contract remediation efforts.

48-Hour Notification Requirement (Article II; Section 5)

The proposed 48-hour requirement conflicts with timelines found in several existing regulatory frameworks and would require substantial renegotiation of existing vendor agreements. Members question whether a fixed 48-hour timeline is appropriate in a privacy model, particularly where no actual breach of nonpublic information has occurred. The requirement could result in significant implementation costs and contract renegotiation efforts without a clear consumer benefit.

Suggested Revision: Replace the 48-hour requirement with a "without unreasonable delay" or "promptly" standard consistent with other privacy and cybersecurity frameworks.

Implementation Period (Article II; Section 5)

Implementation is one of the most significant concerns raised by members. Compliance would require extensive updates to privacy notices, consumer rights processes, governance programs, technology systems, vendor contracts, training programs, and operational procedures. In many cases, insurers would be required to build entirely new request-management, consent-management, tracking, and governance capabilities that do not exist under the current GLBA-based framework. Implementation considerations should therefore remain a central factor in evaluating whether particular requirements provide sufficient consumer benefit to justify the substantial systems, governance, operational, and contractual changes they would require. APCIA also encourages the Working Group to ensure that service-provider provisions appropriately accommodate common operational activities such as security, fraud prevention, debugging, service improvements, and other routine functions that are generally recognized in existing privacy frameworks.

Suggested Revision: Provide no less than 24 months for implementation of substantive requirements and at least five years to bring existing third-party service provider contracts into compliance through ordinary renewal and renegotiation cycles. Include a prospective implementation approach that applies new contractual requirements to new agreements and renewals rather than requiring broad remediation of potentially thousands of existing contracts.

Consumer Requests (Article III)

APCIA members support providing consumers meaningful rights to access, correct, and delete personal information. However, several aspects of Section 6 depart from existing privacy frameworks and would be difficult to operationalize in an insurance context. Primarily, the expanded consumer definition significantly broadens the population eligible to submit requests, creating operational and litigation risks that were not contemplated under the traditional consumer/customer framework. Members support the overall objectives of this section but believe targeted revisions are necessary to improve workability while preserving meaningful consumer rights. Several provisions should be clarified to ensure that correction and deletion obligations apply to information under the licensee's control and maintained within reasonably accessible operational systems. Further, several provisions also appear to assume that licensees maintain direct relationships and complete data visibility for all individuals covered by the expanded consumer definition, which may not be the case for claimants, beneficiaries, or other individuals with indirect relationships to the insurer.

Suggested Revision: APCIA recommends targeted revisions to improve the workability of Section 6 while preserving meaningful consumer rights. At a minimum, the Working Group should clarify that obligations apply to information under a licensee's control and maintained within reasonably accessible operational systems, establish reasonable lookback periods and request limits, replace vendor-specific disclosures with categories of recipients, and expand exceptions for claims administration, fraud prevention, litigation, regulatory compliance, record retention, and other core insurance functions. These revisions would better align the draft with existing privacy frameworks while addressing significant operational and implementation concerns. APCIA has also included selected drafting suggestions in the appendix addressing several of these issues, including request limits, lookback periods, vendor disclosures, and operational exceptions

Unlimited Lookback (Article III, Section 6)

Without a defined lookback period, consumers could request information spanning decades of insurance transactions. Such requests may be difficult or impossible to fulfill accurately and would create substantial operational burdens without providing additional meaningful consumer benefit.

Suggested Revision: Limit access requests to information collected within the preceding one or two years, consistent with other privacy frameworks.

Request Limits (Article III, Section 6)

The absence of limits on access, correction, and deletion requests creates the potential for repetitive, harassing, or duplicative requests. Most state privacy frameworks recognize the need for reasonable limitations on consumer requests.

Suggested Revision: Limit access, correction and deletion requests to two requests per consumer per calendar year or permit denial of repetitive or manifestly excessive requests.

Vendor Lists (Article III, Section 6)

Requiring disclosure of every third-party service provider would be operationally difficult and is unlikely to provide meaningful value to consumers. APCIA is not aware of comparable requirements in other privacy frameworks that require disclosure of every individual service provider rather than categories of recipients. Requiring disclosure of specific vendors may also raise confidentiality and cybersecurity concerns, particularly where those vendors perform security-related functions. Consistent with other privacy frameworks, categories of recipients would be more useful to consumers and substantially easier to administer.

Suggested Revision: Replace specific vendor identification with categories of third parties or service providers.

Deletion Exceptions (Article III, Section 6)

The current deletion exceptions do not adequately account for insurance-specific legal, regulatory, and operational obligations. Insurers frequently retain information to defend claims, satisfy regulatory requirements, comply with statutes of limitation, conduct actuarial analysis, maintain reserves, and ensure cybersecurity. Additionally, access, correction, and deletion rights should not interfere with fraud prevention, fraud investigations, litigation, or evidentiary preservation obligations. Appropriate exceptions are needed to ensure consumer rights cannot be used in a manner that compromises ongoing investigations or undermines legitimate fraud-detection activities.

Suggested Revision: Expand the deletion exceptions to expressly recognize the legal, regulatory, and operational obligations unique to the insurance industry. At a minimum, the exceptions should encompass claims administration, fraud prevention and detection, cybersecurity, actuarial analysis, reserving, litigation and dispute resolution, compliance with statutes of limitation, regulatory examinations, record-retention obligations, and backup and disaster recovery systems. These activities are essential to insurers' ability to meet legal and regulatory requirements, manage risk, protect consumers, and ensure the ongoing integrity and resiliency of insurance operations.

Appeals Process (Article III; Section 6)

The mandatory appeals process for denied correction and deletion requests may create significant operational burdens while providing limited consumer benefit, particularly where information must be retained to satisfy legal, regulatory, actuarial, claims, fraud prevention, or cybersecurity obligations. Requirements to maintain statements of disagreement alongside retained information could create ongoing recordkeeping and systems challenges for insurers.

Suggested Revision: Align the appeals process with existing privacy frameworks and eliminate requirements that would require insurers to maintain indefinite dispute-management records.

Privacy Notices (Article IV; Section 7 and 8)

The combination of the expanded consumer definition and new notice requirements could create significant operational challenges. As drafted, it is unclear whether notices must continue indefinitely for individuals whose information is retained, even where the relationship ended years earlier. In some circumstances, notice obligations could extend indefinitely simply because information is retained for legal, regulatory, or claims-related purposes, even though the underlying relationship ended years earlier.

Additionally, expanding notice obligations to individuals who do not have an ongoing customer relationship may create confusion rather than transparency. For example, claimants, beneficiaries, quote applicants, or other individuals may receive notices from companies with which they do not believe they have a relationship, potentially creating confusion rather than transparency. The expanded definition of consumer may also create unique challenges in the context of beneficiaries, including situations where required notices could create confusion regarding the individual's status or relationship to a policy.

Questions also remain regarding former customers, indirect data collection, claimants, and individuals for whom contact information is unavailable. In some cases, insurers may not possess the contact information necessary to satisfy notice obligations for individuals who do not have a direct customer relationship with the insurer.

APCIA members are also concerned that the proposed notice trigger, tied to when a licensee "obtains access" to nonpublic personal information, creates significant uncertainty regarding when notice obligations arise. The shift from a customer-relationship trigger to an "access to information" trigger represents a significant policy change that could substantially expand notice obligations beyond traditional insurance relationships and longstanding consumer expectations. Insurers routinely receive information from agents, brokers, producers, claimants, service providers, and other third parties. Without additional clarification, the provision could significantly expand notice obligations beyond traditional customer relationships and ordinary consumer expectations.

Suggested Revision: Retain the existing customer-relationship based approach or clarify that notice obligations are tied to the establishment of a customer relationship rather than mere access to information. Clarify when website notices satisfy notice requirements and establish reasonable standards for delivery attempts and undeliverable notices.

Opt-In Framework (Articles V-VII)

The layered combination of opt-outs, targeted advertising requirements, opt-in requirements for sales, and opt-in requirements for sensitive information creates a fragmented consent framework that may be difficult for consumers to understand and challenging for insurers to operationalize. In addition, the breadth of the proposed definition of "sale" may create uncertainty regarding common insurance, marketing, analytics, and service-provider arrangements, making it difficult to determine which consent framework applies in a given circumstance. As drafted, the definition may also encompass activities that consumers would not reasonably view as a sale of information, increasing the risk of consumer confusion while requiring insurers to implement complex and potentially overlapping consent-management processes.

Consumers have long interacted with insurance privacy notices through established GLBA-based mechanisms, and significant departures from those approaches should be carefully evaluated. The proposed framework would likely require new notice structures, consent-management systems, tracking capabilities, and operational workflows that do not exist under the current model. The introduction of multiple consent standards within a single framework could create confusion regarding consumer rights while requiring insurers to build entirely new compliance processes that differ substantially from existing privacy practices.

Suggested Revision: Align the framework more closely with existing state privacy laws and GLBA principles. Reevaluate opt-in requirements for sales of information, particularly where disclosures involve customary insurance, marketing, or distribution activities.

Operational Processing Exceptions (Article VI, Section 24)

The operational exceptions should better reflect core insurance functions. Without additional exceptions, insurers may face uncertainty regarding routine activities that are essential to underwriting, claims administration, fraud detection, cybersecurity, regulatory compliance, and other core insurance operations.

Suggested Revision: Add explicit exceptions for core insurance operations, including claims management, fraud prevention, cybersecurity, regulatory examinations, enterprise investigations, AI and model governance, actuarial analysis, reserving, death matching, and compliance activities. These exceptions would better align the model with routine insurance operations and reduce uncertainty regarding permissible processing activities.

Effective Date (Article VIII; Section 35)

APCIA members consistently identified implementation as one of their top concerns and, in many cases, their top concern. The scope of the proposed changes extends well beyond updating privacy notices and would require modifications to systems, workflows, vendor management programs, consumer rights processes, governance structures, training materials, and existing contractual

arrangements. Several provisions would require insurers to build new consumer-rights processes, consent-management workflows, vendor-management controls, tracking systems, and operational capabilities that do not exist under the current framework. In addition, the term "existing consumer" is undefined and could create significant notice obligations for individuals with whom insurers no longer maintain an active relationship.

Suggested Revision: Clarify the implementation provisions by defining the term "existing consumer" and limiting ongoing notice obligations to individuals with active customer relationships. Given the breadth of the proposed changes, the model should provide no less than 24 months for implementation of substantive requirements and permit compliance through ordinary contract renewal and renegotiation cycles. APCIA also recommends grandfathering existing third-party service provider agreements for up to five years to allow insurers and vendors sufficient time to incorporate new requirements in a practical and orderly manner.

Additional Observations

The concerns described above represent the issues that generated the most significant and consistent feedback during APCIA's review. However, a number of additional drafting, operational, and implementation questions remain that are not addressed in detail here, including notice requirements, consent mechanisms, consumer rights administration, operational exceptions, service-provider provisions, and other technical implementation considerations. APCIA elected to focus these comments on the issues believed to have the greatest impact on the overall scope, structure, and workability of the model.

APCIA also notes that many of the issues identified throughout the draft are interconnected. Changes to definitions, scope, notice obligations, consumer rights, consent requirements, and third-party service provider obligations can substantially affect the implementation and operation of other provisions. For that reason, members believe it is important to evaluate future revisions holistically rather than on a section-by-section basis.

Because many provisions are dependent upon the foundational definitions, scope, consumer rights framework, consent structure, and third-party service provider requirements, APCIA believes additional work and stakeholder review will be necessary before the model is ready to advance. Addressing these foundational issues will place the Working Group in a better position to evaluate the remaining drafting and implementation questions and develop the most effective and workable version of the model. APCIA remains committed to engaging constructively throughout that process and welcomes the opportunity to review future drafts and provide additional drafting suggestions, implementation recommendations, and technical feedback as the Working Group continues its deliberations.

Conclusion

APCIA supports the objective of modernizing Model #672 and believes there is a meaningful opportunity to create a framework that strengthens consumer privacy while remaining practical and effective for the insurance marketplace. Privacy protections should provide meaningful consumer benefits, avoid unintended consequences, and allow insurers to continue providing affordable, accessible, and innovative products and services.

The comments above reflect recurring themes identified consistently across member review, particularly with respect to definitions and scope, consumer rights, third-party service provider requirements, harmonization, and implementation. While APCIA supports the objective of modernization, we continue to believe additional refinement is needed to ensure the framework can be implemented effectively and consistently across the insurance industry. We generally support a modernized insurance privacy framework that builds upon established privacy principles and existing consumer expectations rather than creating a substantially new and separate regulatory regime.

APCIA appreciates the Working Group's continued engagement and looks forward to working collaboratively toward a final framework that achieves those objectives.

Thank you,

Kristin Abbott
Sr. Director & Counsel, Privacy and Cyber Issues

APCIA Appendix: Suggested Redlines

To assist with the Working Group's review, APCIA has included this appendix containing selected drafting suggestions for several of the issues discussed above. These examples are intended to be illustrative rather than exhaustive and should not be viewed as APCIA's only potential approach to resolving the concerns identified in these comments.

Redlined text is presented for ease of reference. Text shown in red strikethrough indicates language APCIA recommends deleting, while text shown in green underline indicates language APCIA recommends adding.

Consumer/Customer (Article 1; Section 4)

- "Customer" means a consumer who has a continuing relationship with a licensee.
- "Customer relationship" means a continuing relationship between a consumer and a licensee under which the licensee provides one or more insurance products or services to the consumer.
- "Consumer" means an individual who seeks to obtain, obtains, or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family, or household purposes. A beneficiary shall not be deemed a consumer unless and until the beneficiary initiates a claim or otherwise directly engages with the licensee regarding policy benefits. For purposes of ongoing notice obligations and consumer rights under this Act, customer status shall be determined separately pursuant to the definition of customer.
- "Existing consumer" means an individual with whom the licensee maintains an active customer relationship as of the compliance date.
    - Alternative suggestion: "For purposes of Section 35, existing consumer shall be limited to individuals with an active customer relationship as of the compliance date.
- Revise references throughout the draft to distinguish between consumers and customers consistent with current Model #672.

Sale (Article 1; Section 4)

- ~~"Sale" means the exchange of nonpublic personal information for monetary or other valuable consideration.~~
- "Sale" means the exchange of nonpublic personal information for monetary consideration. Sale does not include disclosures to service providers, vendors, analytics providers, marketing partners, affiliates, reinsurers, insurance support organizations, comparative raters, or other entities acting on behalf of or in support of insurance operations.

Third-Party Service Providers (Article II; Section 5)

- ~~A licensee remains fully responsible for compliance…~~

- A licensee shall exercise reasonable oversight of third-party service providers and maintain policies and procedures designed to ensure compliance with this Act.

48-Hour Notification Requirement (Article II; Section 5)

- ~~within 48 hours~~
- promptly and without unreasonable delay

Implementation Period (Article II; Section 5)

- Existing third-party service provider agreements shall be deemed compliant until the earlier of:
  - renewal of the agreement; or
  - five years after the effective date.

Reasonably Accessible Systems (Article III, Section 6)

- A licensee shall not be required to retrieve, modify, delete, or disclose nonpublic personal information that is not maintained within a reasonably accessible operational system.

Unlimited Lookback (Article III, Section 6)

- The licensee shall not be required to provide information collected more than two years prior to receipt of the request.

Request Limits (Article III, Section 6)

- ~~There shall be no cap on the number of requests.~~
- A consumer shall be permitted to submit no more than two correction or deletion requests per calendar year.
- A licensee may decline requests that are duplicative, repetitive, or manifestly excessive.

Claims, Fraud, and Investigative Activities Exception (Article III, Section 6)

- A licensee shall not be required to disclose, correct, or delete nonpublic personal information where such action would materially interfere with claims administration, claims handling, fraud prevention or detection, litigation, regulatory investigations, dispute resolution, or the preservation of evidence.

Vendor Lists (Article III, Section 6(A)(1)(b))

- ~~A list of all third-party service providers to whom the licensee disclosed the consumer's nonpublic personal information.~~
- The categories of third-party service providers to whom the licensee disclosed the consumer's nonpublic personal information.

Deletion Exceptions (Article III, Section 6(C)(2))

- Add to deletion exceptions:
  The information is necessary for:
  - claims administration;
  - fraud prevention or detection;
  - cybersecurity purposes;
  - actuarial analysis or reserving;
  - litigation, dispute resolution, or evidentiary preservation;
  - compliance with record-retention obligations;
  - backup, archival, or disaster recovery systems.

Appeals Process (Article III; Section 6)

- A licensee shall maintain any statement of disagreement for a period of five years or for such period as required by applicable record-retention requirements.
- A licensee shall not be required to maintain a statement of disagreement beyond the applicable retention period.

Privacy Notice Trigger (Article IV; Section 7)

- ~~when the licensee obtains access to the consumer's nonpublic personal information~~
- when the licensee establishes a customer relationship with the consumer
  - Alternative suggestion: when the consumer directly applies for, purchases, or obtains an insurance product or service from the licensee

Privacy Annual Notices (Article IV; Section 8)

- A licensee shall provide a clear and conspicuous notice to customers with whom it maintains an ongoing customer relationship.
- A licensee shall not be required to provide annual notices solely because it retains nonpublic personal information pursuant to legal, regulatory, litigation, claims, fraud prevention, or record-retention obligations after the end of the customer relationship.
- Replace "consumer" with "customer" wherever appropriate.

Operational Processing Exceptions (Article VI, Section 24)

- Add the following operational exceptions
  - Disclosures and processing necessary for claims handling,
  - claims adjustment,
  - fraud prevention and detection,
  - cybersecurity,

- enterprise risk management
- model governance,
- actuarial analysis,
- reserving,
- regulatory compliance,
- regulatory examinations,
- enterprise investigations,
- death matching,
- related insurance operations,
- other activities necessary to provide and administer insurance products and services.

601 Pennsylvania Avenue, NW
South Building, Suite 500
Washington, D.C. 20004

T 202.778.3200
F 202.331.7487
ahip.org

September 22, 2026

Re: Full Draft Exposure of Revised Model #672

Dear Director Dwyer:

On behalf of AHIP[1], thank you for the opportunity to provide feedback to the NAIC Privacy Protections (H) Working Group (Working Group) on the Full Draft of Revised Model #672 (Exposure) dated 7.24.2026.

Health plans have long-been leaders in developing privacy, confidentiality and cybersecurity practices to protect personal health information. As new technologies emerge and the health care system continues to evolve, AHIP and our members continue to reaffirm our commitment to enhancing patients' access to actionable information while keeping their personal data secure.

AHIP strongly appreciates the Exposure's preservation of the safe harbor for Health Insurance Portability and Accountability Act (HIPAA) covered entities. This reflects continued recognition of the importance of robust protections for patients and their health information.

AHIP respectfully submits the following recommendations, most of which are technical in nature, aimed at providing clarity for implementation purposes.

Definition of "Deidentified Data". The Working Group should amend the definition of "Deidentified Data" to recognize HIPAA's deidentification standard as a sufficient, but not exclusive, means of compliance. This would provide greater flexibility while maintaining appropriate privacy protections.

Definition of "Sale". The Working Group should clarify that activities that are subject to opt-out requirements under Section 19 are not unintentionally subjected to opt-in requirements pursuant

to the definition of "Sale". Such could be clarified by adding the following to the definition of "Sale" after (5): "(6) A licensee engages in targeted advertising as described under Section 19."

In addition, the Working Group should consider including a definition of "Sale" specifically for non-public health information that aligns with the HIPAA definition of "Sale" of Protected Health Information that reads: "a disclosure of nonpublic personal health information by a licensee or business associate in exchange for direct or indirect renumeration from or on behalf of the recipient of the nonpublic information".

Access Requests and Third-Party Disclosures. The Working Group should confirm that responses regarding third parties be provided at a categorical level rather than identifying specific third parties, as providing individualized disclosures could pose operational challenges and may be infeasible.

Targeted Marketing Opt-Outs. The Working Group should clarify that where targeted marketing occurs through digital assets, notice and opt-out mechanisms may be provided electronically.

Thank you for your work on this important issue. We appreciate the opportunity to provide these comments. Please reach out if you have any questions or would like to discuss further.

Sincerely,

LaCosta Wix
AHIP Senior Regulatory Counsel, State Affairs and Policy
lwix@ahip.org
504-579-6287

Cc: Miranda Motter, Senior Vice President, State Government Affairs and Policy

[1]AHIP is the national association whose members provide health care coverage, services, and solutions to hundreds of millions of Americans every day. We are committed to market-based solutions and public-private partnerships that make health care better and coverage more affordable and accessible for everyone. Visit www.ahip.org to learn how working together, we are Guiding Greater Health.

BlueCross BlueShield Association

750 9th Street NW
Washington, D.C. 20001-4524
202.626.4800
www.BCBS.com

Sept. 22, 2026

Director Beth Dwyer, Chair
Director Ann Gillespie, Co-Vice Chair
Victoria Hastings, Co-Vice Chair
Privacy Protections (H) Working Group
National Association of Insurance Commissioners
1100 Walnut Street, Kansas City, MO 64106-2197

Submitted via email: privacywg@naic.org

RE: Comments on the July 2026 Exposure Draft of the Privacy of Consumer Financial and Health Information Regulation #672

Dear Chair Dwyer, Co-Vice Chair Gillespie, and Co-Vice Chair Hastings:

The Blue Cross Blue Shield Association (BCBSA) appreciates the opportunity to comment on the July 2026 exposure draft of the Privacy of Consumer Financial and Health Information Regulation #672 (Draft Model). BCBSA is a national federation of independent, community-based and locally operated Blue Cross and Blue Shield companies (Plans) that collectively provide health care coverage for one in three Americans. BCBS Plans contract with 97% of hospitals and 83% of doctors across the country and serve those who are covered through Medicare, Medicaid, an employer, or purchase coverage on their own.

We appreciate the Working Group's continued engagement on this model and share the goals of consistent, meaningful protections for patients' personal information. We also appreciate the Working Group's recognition that there are important existing consumer protections under HIPAA and efforts to align with those protections and processes.

Building on that alignment, we reiterate our recommendation for the model to incorporate a full exemption from this framework for HIPAA-covered entities. We continue to urge the Working Group to exempt HIPAA-covered entities from the disclosure accounting and consumer access requirements, consistent with the existing HIPAA Privacy Rule framework. We appreciate the intent of Section 28 in the current draft to ensure all patient data is protected in some manner. However, aligning with HIPAA only when a licensee maintains all nonpublic personal information (NPI) in the same manner as protected health information (PHI) leaves the model's requirements in direct conflict with the HIPAA framework for health insurers and can unintentionally expose consumers to new privacy risk by establishing a separate regulatory compliance structure for different types of data. While states play an important role in protecting consumers, applying a separate privacy framework to HIPAA-covered entities does

not necessarily provide additional protections for consumers. Instead, overlapping requirements can create conflicting standards for the same data and activities, increasing administrative complexity without a corresponding privacy benefit. Consumer privacy is best served through a single, comprehensive, and consistently applied framework

This complexity increases the risk of errors driven by imperfect understanding of which structure applies to certain data and functions that may not naturally be bifurcated in the same way as the structures dictate and/or gaps when the two frameworks are not clearly complimentary or mutually exclusive.

For example, HIPAA requires accounting only for disclosures made without patient authorization, and expressly exempts disclosures for treatment, payment, and health care operations — the vast majority of routine Plan activity. Whereas, the NAIC model (Section 6A) requires accounting for all NPI disclosures with no equivalent carve-out for operations. When PHI and NPI are part of the same transaction, it creates a create uncertainty about whether consent must be obtained before information may be disclosed, and could potentially slow patient care coordination and access.

BCBS Plans operate under HIPAA's comprehensive and well-established privacy and security framework, which was specifically designed to protect the sensitive health information of patients. Imposing duplicative and inconsistent requirements on HIPAA-covered entities diverts resources from other risk mitigation efforts into navigating conflicting legal standards as it is largely the same resources performing both functions related to data privacy. These resources could otherwise be directed toward strengthening privacy and security safeguards, preventing fraud and abuse, improving member support, and advancing other activities that directly benefit consumers. These challenges are compounded for entities operating across multiple states and relying on integrated systems to perform regulated functions. Patients' data is ultimately better protected when there are consistent, robust and predictable standards.

We respectfully offer the comments below and reiterate a few technical considerations provided in response to the November 2024 Chairs' Draft which remain relevant. To assist the Working Group's continued consideration of these issues, Appendix A also provides proposed revisions to the Draft Model that would implement the recommendations described in this letter. BCBSA remains committed to strong, workable consumer privacy protections that complement the federal HIPAA framework. We thank the Working Group for its continued engagement and look forward to working collaboratively toward a final model that meets these goals.

* * * * *

Access, Correction, and Deletion of Nonpublic Personal Information (Section 6)

Section 6 establishes a consumer's right to request access to, correction of, and deletion of personal information maintained by the licensee or any contracted third-party service provider, with a 45-day response window. BCBSA strongly supports robust consumer access rights and

greater transparency, and we share the Working Group's goal of ensuring consumers have meaningful control over their information.

To support this goal, we recommend clarifying within the correction and deletion language that deletion rights do not extend to data that Plans must retain to administer benefits, resolve grievances and appeals, or defend against fraud — functions that ultimately protect consumers as well as the integrity of the coverage relationship and some of which are required by law. These functions depend on the availability of complete and reliable information and help Plans accurately administer coverage, close gaps in care, protect program integrity, and meet their obligations to members and regulators. In addition, health insurers operate within a highly regulated environment and are frequently required to retain records for extended periods. Applying deletion rights without appropriate exceptions could place licensees in conflict with these existing obligations and impair functions that protect consumers and the integrity of the coverage relationship.

A targeted exception along these lines would strengthen the overall framework if ultimately applicable to HIPAA-covered entities.

Limits on Targeted Advertising and Disclosure of Personal Information (Sections 19 and 21)

Sections 19 and 21 introduce new consumer consent frameworks for targeted advertising and disclosure of personal information. BCBSA supports these provisions as an important foundation for consumer trust and welcomes the Working Group's focus on consent. We recommend two clarifications to ensure the provisions work as intended for health insurers.

First, member communications are a core consumer protection function for Plans — including care gap notifications, wellness program outreach, and chronic condition management programs, value-based care initiatives, and provider quality improvement activities.

As currently drafted, the definition of "targeted advertising" in Section 19 could capture these communications because they draw on data about consumer activities. These communications are intended to improve health outcomes and support appropriate care, rather than promote products or services through commercial advertising. An explicit exclusion for outreach and coordination conducted for care management, disease management, and quality improvement purposes - which are already recognized permitted insurance functions under Section 25(B) - would preserve the provision's intended scope while protecting members' access to clinically important communications.

Second, the sensitive personal information opt-in framework in Section 21 would benefit from clarification that the use of demographic data — including race and ethnicity — for community health initiatives, disparity analysis, and population health management does not require opt-in when conducted as part of a licensee's quality improvement or care management functions.

Plans’ ability to identify disparities, develop targeted interventions, comply with evolving health equity requirements, and evaluate whether their programs are reaching members effectively

depends on the responsible use of this information. Requiring additional opt-in consent for these functions could result in incomplete data and make it more difficult to identify and address disparities. Clarification is therefore needed to ensure that the model supports, rather than inadvertently limits, responsible equity-focused work on behalf of the consumers it is intended to protect.

Previous Technical Recommendations (Sections 6-8)

In addition, we appreciate the opportunity to resurface two technical recommendations from our November 2024 comments which are applicable to the latest draft:

- First, BCBSA recommends that Section 6(A) of the model clarify that nonpublic personal information provided to a requesting consumer "must be provided in paper or electronic form, as requested by the consumer," rather than in language requiring a "format specific to the consumer and easily readable." Clear, standardized expectations for both licensees and consumers are consistent with existing notice frameworks and reduce the risk of regulatory uncertainty. We renew this recommendation and urge the Working Group to adopt this clarifying language.
- Second, BCBSA recommends clarification for Sections 7 and 8 that "separately" in the context of consumer consent means a separate document with its own signature, not a wholly separate consumer interaction. Without clarification, licensees face the risk of inconsistent regulatory interpretation across states, and consumers may experience unnecessary friction in consent processes that would otherwise be straightforward. We continue to recommend that the model define "separately" consistent with this standard.

In addition, to the comments above, please see attached Appendix A which also provides proposed revisions to the Draft Model that would implement the recommendations described in this letter.

Thank you for the opportunity to provide feedback on the Privacy of Consumer Financial and Health Information Regulation draft model regulation. If you have any questions, please contact Randi Chapman at Randi.Chapman@bcbsa.com.

Sincerely,



Clay S. McClure
Senior Director, State Affairs
Blue Cross Blue Shield Association

Appendix A: BCBSA Proposed Revisions to Model Regulation #672

The following proposed revisions are intended to implement the recommendations described in BCBSA's comment letter. Bold and underlined text indicates proposed additions, and strikethrough text indicates proposed deletions.

1. Full exemption for HIPAA-covered entities

Revise:

A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), **shall not be subject to** this Act **with respect to nonpublic personal information maintained, used, or disclosed in connection with the licensee's functions as a covered entity or business associate.**

2. Section 6.C(2): Deletion exceptions

Add to the existing list of circumstances:

"The information is reasonably necessary to administer benefits or claims; coordinate care; conduct case management, disease management, utilization management, or quality improvement; resolve grievances or appeals; detect or prevent fraud, waste, or abuse; or satisfy applicable record-retention, regulatory oversight, financial reporting, litigation-preservation, or accreditation requirements."

3. Section 4: Targeted advertising definition

Add to the existing list of activities that are not "targeted advertising":

"Communications by or on behalf of a licensee for care management, disease management, medication adherence, preventive health, wellness, utilization management, quality improvement, population health management, or other insurance functions permitted under Section 25(B)."

4. Section 21: Sensitive personal information

Revise:

“Except as provided by Subsection B below, a licensee may disclose a consumer’s sensitive personal information only for those purposes and uses identified in Article VI and as expressly permitted or required by **this Act, including the insurance functions identified in Section 25(B), such as care management, quality improvement, population health management, disparity analysis, and health equity activities**.”

Coalition Against Insurance Fraud
1012 14th Street NW, Suite 610
Washington, D.C. 20005
202.393.7330

Michelle Rafeld
Executive Director

September 17, 2026

RE: Comments regarding "Revised Model 672—Full Draft 7.24.26"

Chair Dwyer and Members of the Working Group:

The Coalition Against Insurance Fraud appreciates the opportunity to comment on the July 24, 2026, full draft of revised Model #672, the proposed *Privacy of Consumer Information Act*.

The Coalition is a national alliance that brings together insurers, insurance regulators, law enforcement and government agencies, consumer organizations, legal professionals, antifraud service providers, and other stakeholders to prevent and combat insurance fraud and protect consumers from its harm.

The Coalition applauds the Working Group's efforts to modernize consumer privacy protections and appreciates the antifraud exemptions included in the revised model. These exemptions help prevent fraudsters from exploiting consumer protections or compromising fraud investigations. In reviewing the model in its entirety, we would like to recommend the following additions to strengthen antifraud protections:

1. Add express antifraud exceptions to Section 6 for each of the new consumer rights of access in 6.A.(2)(d), correction in 6.B.(3)(c) and deletion in 6.C.(2)(e). In developing this approach, the Coalition looked to California Senate Bill 354 as an example of how to address antifraud concerns separately within each consumer right, helping prevent those rights from inadvertently revealing or compromising an ongoing investigation into suspected insurance fraud or resulting in the alteration or deletion of information that may need to be preserved, particularly at a stage before a civil or criminal proceeding might be anticipated.

2. Clarify in Section 29 that the model does not limit existing obligations, including mandatory compliance reporting, related immunity, and confidentiality protections.

Balancing consumer privacy rights with fraud prevention is consumer protection.

The Coalition's proposed additions to Model #672 are attached and shown in underlined red text. We believe these targeted clarifications will prevent misinterpretation and balance the model's consumer privacy objectives with effective antifraud protections.

Respectfully,

Brent Walker
Director of Government Relations, Coalition Against Insurance Fraud
NAIC Consumer Representative
brent@insurancefraud.org

A national coalition of consumers, government agencies and insurers dedicated to combating all forms of insurance fraud through public information and advocacy.

BOARD OF DIRECTORS

AIG • Allstate Insurance • American Council on Consumer Interests • American Family Insurance • American Fidelity • American Policyholders Association • American Property Casualty Insurance Association • Assurant • CNA • Blue Cross Blue Shield Association • California Department of Insurance • Consumer Action • Consumer Federation of America • Erie Insurance • Farmers Insurance • Florida Division of Investigative & Forensic Services • Florida Office of Insurance Consumer Advocate • Geico • Hanover Insurance • Hartford Insurance • Horace Mann • Insurance Fraud Bureau of Massachusetts • Intact Insurance • International Association of Special Investigation Units • John Hancock Financial Services • Katten Muchin Rosenman LLP • Liberty Mutual Group • Louisiana State Police • MassMutual • MetLife • National Association of Consumer Agency Administrators • National Association of Insurance Commissioners • National Association of Public Adjusters • National Council of Insurance Legislators • National Criminal Justice Association • National Fraud Information Center • National Insurance Crime Bureau • Nationwide Insurance • New Mexico Office of the Superintendent • New York Life • Northwestern Mutual • Pennsylvania Insurance Fraud • Prevention Authority • Pennsylvania Office of Attorney General • Progressive Insurance • Prudential Insurance • San Diego Office of District Attorney • Senior Medicare Patrol (SMP) • National Resource Center • ReKNOWvate • Sentry Insurance • State Farm Insurance Companies • Swiss RE • The Standard • Travelers Insurance • United Policyholders • University of New Haven • USAA • Verisk • Westfield Insurance • Zurich North America

Comments from the Coalition Against Insurance Fraud, submitted 9/17/2026

PRIVACY OF CONSUMER INFORMATION ACT

Table of Contents

ARTICLE I. GENERAL PROVISIONS

Section 1. Purpose
Section 2. Scope and Compliance
Section 3. Rule of Construction
Section 4. Definitions

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Section 5. Third-Party Service Provider Arrangements

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7. Initial and Subsequent Delivery Notice of Information Practices to Consumers Required
Section 8. Annual Notice of Information Practices to Consumers Required
Section 9. Information to be Included in Notices of Information Practices
Section 10. Short Form Initial Notice of Information Practices
Section 11. Form of Opt-In Notice to Consumers and Opt-In Methods
Section 12. Form of Opt-Out Notice to Consumers and Opt-Out Methods
Section 13. Revised Notice of Information Practices
Section 14. Notice of Information Practices to Group Policyholders
Section 15. Delivery

ARTICLE V. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 16. General Rules for Use and Disclosure of Nonpublic Personal Information
Section 17. Limits on Redisclosure and Reuse of Nonpublic Personal Information
Section 18. Limits on Sharing Access Number or Access Code Information for Marketing Purposes
Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted Advertising
Section 20. Limits on Sale of Nonpublic Personal Information
Section 21. Limits on Disclosure of Sensitive Personal Information

© 2026 National Association of Insurance Commissioners

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 22. Exception to Opt Out Requirements for Disclosure of Nonpublic Personal Information for Service Providers and Joint Marketing
Section 23. Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Information for Processing and Servicing Transactions
Section 24. Other Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Information

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 25. When Authorization Required for Disclosure of Nonpublic Personal Health Information
Section 26. Authorizations
Section 27 Authorization Request Delivery
Section 28. Relationship to Federal Rules
Section 29. Relationship to State Laws

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 30. Protection of Fair Credit Reporting Act
Section 31. Nondiscrimination
Section 32. Violation
Section 33. Severability
Section 34. Individual Remedies
Section 35. Effective Date

APPENDICES

Appendix A Sample Clauses
Appendix B Federal Model Privacy Form
Model Law Forms

ARTICLE I. GENERAL PROVISIONS

Section 1. Purpose

Purpose. This Act governs the treatment of nonpublic personal health information and nonpublic personal information about individuals by all licensees of the state insurance department. This Act:

A. Requires a licensee to provide notice to individuals about its privacy policies and practices;

B. Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal information about individuals to affiliates and nonaffiliated third parties; and

C. Provides methods for individuals to prevent a licensee from disclosing that information.

Drafting Note: Whether this model is adopted as an Act or Regulation will depend upon individual state law. If a state adopts the model as an Act, reference to the model as an Act should be updated throughout the model.

Section 2. Scope and Compliance

A. Scope. This Act applies to:

(1) Nonpublic personal information about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. This Act does not apply to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes; and

(2) All nonpublic personal health information.

B. Compliance. A licensee domiciled in this state that is in compliance with this Act in a state that has not enacted laws or regulations that meet the requirements of Title V of the Gramm-Leach-Bliley Act (PL 102-106) may nonetheless be deemed to be in compliance with Title V of the Gramm-Leach-Bliley Act in the other state.

Drafting Note: Subsection B is intended to give licensees some guidance for complying with Title V of the Gramm-Leach-Bliley Act in those states that do not have laws or regulations that meet GLBA's privacy requirements.

© 2026 National Association of Insurance Commissioners

Section 3. Rule of Construction

The examples in this Act, the sample clauses in Appendix A, and the Federal Model Privacy Form in Appendix B of this Act are not exclusive. Compliance with an example, use of a sample clause, or the Federal Privacy Model Form, to the extent applicable, constitutes compliance with this Act.

Licensees may rely on use of the Federal Privacy Form in Appendix B, consistent with the attached instructions, as a safe harbor of compliance with the Notice of Information Practices content requirements of this Act.

Use of the Federal Model Privacy Form is not required. Licensees may continue to use other types of privacy notices, including notices that contain the examples in this Act and/or the sample clauses in Appendix A, provided that such notices accurately describe the Licensee's privacy practices and otherwise meet the notice content requirements of this Act.

Section 4. Definitions

As used in this Act, unless the context requires otherwise:

A. "Affiliate" means a company that controls, is controlled by or is under common control with another company.

B. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

C. (1) "Clear and conspicuous" means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) Examples.

(a) Reasonably understandable. A licensee makes its notice reasonably understandable if it:

(i) Presents the information in the notice in clear, concise sentences, paragraphs and sections;

(ii) Uses short explanatory sentences or bullet lists whenever possible;

(iii) Uses definite, concrete, everyday words and active voice whenever possible;

(iv) Avoids multiple negatives;

(v) Avoids legal and highly technical business terminology whenever possible; and

(vi) Avoids explanations that are imprecise and readily subject to different

© 2026 National Association of Insurance Commissioners

interpretations.

(b) Designed to call attention. A licensee designs its notice to call attention to the nature and significance of the information in it if the licensee:

(i) Uses a plain-language heading to call attention to the notice;

(ii) Uses a typeface and type size that are easy to read;

(iii) Provides wide margins and ample line spacing;

(iv) Uses boldface or italics for key words; and

(v) In a form that combines the licensee's notice with other information, uses distinctive type size, style, and graphic devices, such as shading or sidebars.

(c) Notices on web sites. If a licensee provides a notice on a web page, the licensee designs its notice to call attention to the nature and significance of the information in it if the licensee uses text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks or sound) do not distract attention from the notice, and the licensee either:

(i) Places the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(ii) Places a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

D. "Collect" means to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

E. "Commissioner" means the chief insurance regulatory official of the state.

Drafting Note: Use the title of the chief insurance regulatory official wherever the term "commissioner" appears. If the jurisdiction of certain health licensees, such as health maintenance organizations, lies with some state agency other than the insurance department, or if there is dual regulation, a state should add language referencing that agency to ensure the appropriate coordination of responsibilities.

F. "Company" means a corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.

G. (1) "Consumer" means an individual who seeks to obtain, obtains or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, and about whom the licensee has nonpublic personal information, or that individual's legal representative.

 © 2026 National Association of Insurance Commissioners

(2) Examples.

(a) An individual who provides nonpublic personal information to a licensee in connection with obtaining or seeking to obtain financial, investment or economic advisory services relating to an insurance product or service is a consumer regardless of whether the licensee establishes an ongoing advisory relationship.

(b) An applicant for insurance prior to the inception of insurance coverage is a licensee's consumer.

(c) An individual who is a consumer of another financial institution is not a licensee's consumer solely because the licensee is acting as agent for, or provides processing or other services to, that financial institution.

(d) An individual is a licensee's consumer if:

(i) (I) The individual is a beneficiary of a life insurance policy underwritten by the licensee;

(II) The individual is a claimant under an insurance policy issued by the licensee;

(III) The individual is an insured or an annuitant under an insurance policy or an annuity, respectively, issued by the licensee; or

(IV) The individual is a mortgagor of a mortgage covered under a mortgage insurance policy; and

(ii) The licensee discloses nonpublic personal information about the individual to a nonaffiliated third party other than as permitted under Sections 22, 23, and 24 of this Act.

(e) Provided that the licensee provides the initial, annual and revised notices under Sections 7, 8, and 13 of this Act to the plan sponsor, group or blanket insurance policyholder or group annuity contract holder, or workers' compensation policyholder, and further provided that the licensee does not disclose to a nonaffiliated third party nonpublic personal financial information about an individual described in Item (i), (ii) or (iii), other than as permitted under Sections 22, 23, or 24 of this Act, such an individual is not the consumer of the licensee solely because he or she is:

(i) A participant or a beneficiary of an employee benefit plan that the licensee administers or sponsors or for which the licensee acts as a trustee, insurer or fiduciary;

(ii) Covered under a group or blanket insurance policy or group annuity contract issued by the licensee; or

(iii) A claimant covered by a workers' compensation plan.

© 2026 National Association of Insurance Commissioners

Drafting Note: In states where the workers' compensation self-insurance or workers' compensation state fund coverage is outside the commissioner's jurisdiction, regulators may wish to urge the applicable agency or agencies to promulgate a regulation similar to this Act in order to ensure parity in treatment of workers' compensation plans and to ensure that all workers covered by such plans have privacy protections.

(f) (i) The individuals described in Subparagraph (e)(i) through (iii) of this paragraph are consumers of a licensee if the licensee does not meet all the conditions of Subparagraph (e).

(ii) In no event shall the individuals, solely by virtue of the status described in Subparagraph (e)(i) through (iii) above, be deemed to be consumers for purposes of this Act.

(g) An individual is not a licensee's consumer solely because he or she is a beneficiary of a trust for which the licensee is a trustee.

(h) An individual is not a licensee's consumer solely because he or she has designated the licensee as trustee for a trust.

H. "Consumer reporting agency" has the same meaning as in Section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

I. "Control" means:

(1) Ownership, control or power to vote twenty-five percent (25%) or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

(2) Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or

(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the commissioner determines.

J. "De-identified data" means information that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual.

K. (1) "Financial institution" means any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 1843(k)(4)(B**)** of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial institution does not include:

(a) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 *et seq.*);

(b) The Federal Agricultural Mortgage Corporation or any entity charged and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*); or

© 2026 National Association of Insurance Commissioners

(c) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as the institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

L. (1) "Financial product or service" means a product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 1843(k)(4)(B**)** of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.

M. "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.

N. (1) "Licensee" means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Insurance Law of this state, [and health maintenance organizations holding a certificate of authority pursuant to Section [insert section] of this state's Public Health Law].

Drafting Note: Add bracketed language if HMOs are licensed under other than insurance statutes and cite appropriate state law.

(2) A licensee is not subject to the notice and opt out requirements for nonpublic personal information set forth in Articles I, II, III and IV of this Act if the licensee is an employee, agent or other representative of another licensee ("the principal") and:

(a) The principal otherwise complies with, and provides the notices required by, the provisions of this Act; and

(b) The licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates in a manner permitted by this Act.

(3) (a) Subject to Subparagraph (b), "licensee" shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only in regard to the excess lines placements placed pursuant to Section [insert section] of this state's laws.

(b) An excess lines broker or excess lines insurer shall be deemed to be in compliance with the notice and opt out requirements for nonpublic personal information set forth in Articles I, II, III and IV of this Act provided:

(i) The broker or insurer does not disclose nonpublic personal information of a consumer to nonaffiliated third parties for any purpose, including joint servicing or marketing under Section 22 of this Act, except as

© 2026 National Association of Insurance Commissioners

permitted by Section 23 or 24 of this Act; and

(ii) The broker or insurer delivers a notice to the consumer at the time a consumer relationship is established on which the following is printed in 16-point type:

NOTICE OF INFORMATION PRACTICES
"Neither the U.S. brokers that handled this insurance nor the insurers that have underwritten this insurance will disclose nonpublic personal information concerning the buyer to nonaffiliates of the brokers or insurers except as permitted by law."

Drafting Note: References to "excess lines broker" and "excess lines insurer" should be changed as necessary to correspond with the applicable terms used in each state.

O. (1) "Nonaffiliated third party" means any person except:

(a) A licensee's affiliate; or

(b) A person employed jointly by a licensee and any company that is not the licensee's affiliate (but nonaffiliated third party includes the other company that jointly employs the person).

(2) Nonaffiliated third party includes any company that is an affiliate solely by virtue of the direct or indirect ownership or control of the company by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

P. "Nonpublic personal health information" means any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of an individual;

(2) The provision of health care to an individual; or

(3) Payment for the provision of health care to an individual.

Q. "Nonpublic personal information" means any personally identifiable information that is linked or reasonably linkable to an identified natural person. Nonpublic personal information does not include de-identified data or publicly available information.

R. (1) "Personally identifiable information" means any information:

(a) A consumer provides to a licensee to obtain an insurance product or service from the licensee;

 © 2026 National Association of Insurance Commissioners

(b) About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

(c) The licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.

(2) Examples.

(a) Information included. Personally identifiable information includes:

(i) Information a consumer provides to a licensee on an application to obtain an insurance product or service;

(ii) Account balance information and payment history;

(iii) The fact that an individual is or has been one of the licensee's consumers or has obtained an insurance product or service from the licensee;

(iv) Any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer;

(v) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;

(vi) Any information the licensee collects through an Internet cookie (an information-collecting device from a web server); and

(vii) Information from a consumer report.

(b) Information not included. Personally identifiable information does not include:

(i) A list of names and addresses of customers of an entity that is not a financial institution; and

(ii) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.

S. "Opt in" means an affirmative direction by a consumer that authorizes a licensee to disclose the consumer's information.

T. "Opt out" means a direction by a consumer that the licensee may not disclose nonpublic personal information about the consumer to a nonaffiliated third party, except as permitted under Sections 22,23, or 24 .

U. (1) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

(a) Federal, state or local government records;

© 2026 National Association of Insurance Commissioners

(b) Widely distributed media; or

(c) Disclosures to the general public that are required to be made by federal, state or local law.

(2) Reasonable basis. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

(a) That the information is of the type that is available to the general public; and

(b) Whether an individual can direct that the information not be made available to the general public and, if so, that the licensee's consumer has not done so.

(3) Examples.

(a) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(b) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(c) Reasonable basis.

(i) A licensee has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(ii) A licensee has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the licensee has located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

V. "Reasonable opportunity" means any of the following:

(1) The licensee mails the notices required to the consumer and allows the consumer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within sixty (60) days from the date the licensee mailed the notices;

(2) Where a consumer agrees to receive the notices required by this Act electronically in accordance with UETA [insert state electronic transactions act statute], the licensee allows the consumer to opt out by any reasonable means at any time; or

© 2026 National Association of Insurance Commissioners

(3) For an isolated transaction, such as providing the consumer with an insurance quote, the licensee provides the notices required by this Act at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction.

X. "Sale" or "selling" means the exchange of nonpublic personal information for monetary or other valuable consideration. A licensee does not sell nonpublic personal information when:

(1) The disclosure is to a third party for the purpose of or in support of providing a product or service requested by the consumer.

(2) A licensee provides information to or receives anything of value from an insurance support organization, statistical agent, or reinsurer;

(3) A licensee provides nonpublic personal information to an affiliate or to a financial institution with which the licensee performs joint marketing;

(4) The business transfers to a third party the nonpublic personal information as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction in which the party assumes control of all or part of the licensee's assets; or

(5) A consumer uses or directs the business to (i) disclose nonpublic personal information; or (ii) interact with one or more third parties including but not limited to referrals to other licensees.

Y. "Sensitive Personal Information" means personally identifiable "nonpublic personal information" about a consumer that includes:

(1) Racial or ethnic origin, religious beliefs, sexual orientation, or citizenship or citizenship status; or

(2) Genetic information or biometric data that may be processed for the purpose of uniquely identifying an individual.

Z. (1) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests.

(2) "Targeted advertising" does not include:

(a) Online advertisements based on activities within a Licensee's own websites or online applications;

(b) Online advertisements based on the context of a consumer's current search query, visit to a website, or online application;

(c) Online advertisements directed to a consumer in response to the consumer's request for information or feedback; or

© 2026 National Association of Insurance Commissioners

(d) Processing Nonpublic Personal Information solely for measuring or reporting advertising performance, reach, or frequency.

AA. “Third party service provider” or “third party” means a person or entity not otherwise defined as a licensee or affiliate of a licensee that:

(1) Provides services to the licensee; and

(2) Maintains, processes or otherwise is permitted access to nonpublic personal information through its provisions of services to the licensee.

© 2026 National Association of Insurance Commissioners

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Section 5. Third-Party Service Provider Arrangements

A. Contract Requirements.

A licensee that discloses a consumer's nonpublic personal information to a third-party service provider shall enter into a written contract with the third-party service provider that:

(1) Prohibits the third-party service provider from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless processing is necessary to comply with the law or a valid and binding order of a governmental body, in which case the third-party service provider must notify the licensee within 48 hours unless prohibited by law;

(2) Requires the third-party service provider to delete, destroy, de-identify or return all nonpublic personal information to the licensee when requested by the licensee; or to delete nonpublic personal information after it is no longer necessary to fulfill a legal requirement or to meet the record retention requirements of the licensee or third-party service provider, and to notify the licensee of the action taken;

(3) Requires the third-party service provider to notify the licensee if it can no longer comply with its obligations under this contract and provides the licensee with a right to terminate the contract;

(4) Requires that any contract between a third-party service provider and a subcontractor with access to a consumer's nonpublic personal information must contain provisions no less protective of nonpublic personal information than those contained in the third-party service provider's agreement with the licensee;

(5) Requires the third-party service provider to provide assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act;

(6) Requires the third-party service provider to implement and maintain administrative, technical, and physical data security practices to protect the nonpublic personal information from unauthorized access, destruction, use, modification, or disclosure;

(7) Requires the third-party service provider to notify the licensee of a failure to meet the obligations of Subsections (1) to (6) above within 48 hours of discovery by the third-party service provider.

B. A licensee that discloses a consumer's nonpublic personal information to a third-party service provider remains fully responsible for compliance with this Act and the handling of nonpublic personal information.

© 2026 National Association of Insurance Commissioners

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

A. A consumer may file the following requests with a licensee, which shall be processed in accordance with the following standards:

(1) Within 45 days of receiving an authenticated request from a consumer for their nonpublic personal information, a licensee shall disclose:

(a) All nonpublic personal information about the consumer that is maintained by the licensee or any contracted third-party service provider; and

(b) A list of all third-party service providers to whom the licensee disclosed the consumer's nonpublic personal information.

(2) A licensee shall not be required to disclose the following:

(a) A consumer's Social Security Number, driver's license number or other government-issued identification number, financial account number(s), any health insurance or medical identification number, any account password(s), security questions and answers, unique biometric data or other information that could create a high risk of identity theft. The licensee may instead disclose the types of nonpublic personal information maintained by listing each type of nonpublic personal information it has about the consumer;

(b) Duplicative nonpublic personal information, if it is described in a manner reasonably understandable by the consumer and the consumer is offered an opportunity to review the nonpublic personal information for inconsistencies; or

(c) Information that is outside the scope of the request, if the consumer has requested only specified items or categories of information.

(d) Information pertaining to an anticipated, suspected, or active fraud investigation or the detection or prevention of fraud, or information shared in accordance with the reporting of suspected insurance fraud under **state mandatory fraud reporting, related immunity, and confidentiality statute(s).**

Drafting Note: Insert applicable mandatory fraud reporting, related immunity, and confidentiality statute(s).

B. Correction of nonpublic personal information.

(1) A consumer may make an authenticated request for the correction of their nonpublic personal information by filing a request with the licensee that:

(a) Identifies the specific nonpublic personal information the consumer wishes to correct; and

© 2026 National Association of Insurance Commissioners

(b) Provides an explanation of why the nonpublic personal information is incorrect.

(2) Within 45 days of receipt of the request under this subsection, a licensee shall take one of the following actions and notify the consumer:

(a) Correct the nonpublic personal information in dispute as requested by the consumer;

(b) Delete the nonpublic personal information in dispute; or

(c) Deny the request and provide:

(i) The basis for refusal to correct the nonpublic personal information as requested;

(ii) Information about how the consumer may appeal the denial; and

(iii) An explanation of how the appeal will be reviewed and how the consumer will be notified of the decision on appeal.

(3) A licensee may deny a request for correction if:

(a) The nonpublic personal information is accurate and complete and if the licensee provides a process for appeal of the decision; or

(b) The nonpublic personal information that is the subject of the request was not created by the licensee, unless there is a reasonable basis to believe that the originator of the nonpublic personal information is no longer available to act on the requested correction, and the consumer has independently demonstrated the information is incorrect; or

(c) The nonpublic personal information that is the subject of the request pertains to an anticipated, suspected, or active fraud investigation or the detection or prevention of fraud, or information shared in accordance with the reporting of suspected insurance fraud under **state mandatory fraud reporting, related immunity, and confidentiality statute(s).**

Drafting Note: Insert applicable mandatory fraud reporting, related immunity, and confidentiality statute(s).

C. Deletion of nonpublic personal information.

(1) Within 45 days of an authenticated request from a consumer, a licensee shall delete the nonpublic personal information about the consumer that is maintained by the licensee or direct a third-party service provider to delete the nonpublic personal information on the licensee's behalf.

(2) The licensee is not required to delete nonpublic personal information if:

(a) The licensee is required by law or regulation to retain the nonpublic personal information;

© 2026 National Association of Insurance Commissioners

(b) The nonpublic personal information may be necessary to perform the contract or service requested by or benefiting the consumer;

(c) The information is necessary to comply with a legal obligation; or

(d) The information is maintained in reasonable anticipation of a claim or civil or criminal proceeding; or

(e) The information pertains to an anticipated, suspected, or active fraud investigation or the detection or prevention of fraud, or information shared in accordance with the reporting of suspected insurance fraud under **state mandatory fraud reporting, related immunity, and confidentiality statute(s).**

Drafting Note: Insert applicable mandatory fraud reporting, related immunity, and confidentiality statute(s)

(3) A licensee may delay fulfilling a consumer's request, up to 45 days, to delete nonpublic personal information stored on an archived or backup system. A licensee must notify the consumer of such delay.

D. Request and Response Procedures

(1) Except as provided in Subsection D(1)(b), a licensee shall respond to requests submitted under this section within 45 days in the following manner:

(a) A licensee may use its secure communications portal to authenticate requests from consumers holding current accounts with the licensee, unless the licensee has reason to believe the request has been submitted through an account that has been compromised. Otherwise, the licensee may use methods that are commercially reasonable, but not unduly burdensome, to authenticate the identity of the person making the request and to verify that this person is either:

(i) The consumer;

(ii) A person acting with the consumer's written authorization, including but not limited to a valid power of attorney;

(iii) The parent or legal guardian of a consumer who is a minor, except where the information relates to health insurance claims in circumstances where the child has a legal right to obtain the services in question without the parent's or guardian's consent;

(iv) The legal guardian or other person authorized by law to act on behalf of an incapacitated consumer; or

(v) The personal representative or other person authorized by law to act on behalf of a deceased consumer.

(b) A licensee is required to notify the consumer if either of the following prevents the licensee from complying with the request:

© 2026 National Association of Insurance Commissioners

(i) The specific nonpublic personal information at issue is not locatable or retrievable by the licensee; or

Drafting Note: Examiners should review licensees' notifications to consumers regarding nonpublic personal information that is not locatable or retrievable by the licensee and its justifications for irretrievability during Market Conduct and/or IT Exams.

(ii) The licensee is unable to verify the request after requesting that the consumer provide additional information necessary to authenticate the identity of the consumer and authenticate the consumer's request.

(c) If a licensee declines the consumer's request, the licensee shall inform the consumer of the basis for declining the request and provide instructions for how to request review of the decision.

(2) There shall be no cap on the number of requests to correct or delete nonpublic personal information.

(3) If a consumer disagrees with a licensee's refusal to correct or delete nonpublic personal information per the consumer's request, the consumer shall be permitted to file with the licensee:

(a) A concise statement setting forth why the consumer disagrees with the licensee's refusal and what the consumer thinks is the correct, relevant or fair information; and

(b) The licensee shall maintain the statement with the disputed nonpublic personal information and allow anyone reviewing the disputed nonpublic personal information to be made aware of the dispute and have access to the consumer's statement.

© 2026 National Association of Insurance Commissioners

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7. Initial and Subsequent Delivery Notice of Information Practices to Consumers Required

A. Initial Delivery of Notice. A licensee shall provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to all consumers no later than when the licensee obtains access to the consumer's nonpublic personal information, except that a licensee may provide the initial notice within a reasonable time after access to the consumer's nonpublic personal information if:

(1) Obtaining access to the consumer's nonpublic personal information is not at the consumer's election and the licensee follows the Notice of Information Practices previously sent to the consumer; or

(2) Providing notice when the licensee obtains access to the consumer's nonpublic personal information would substantially delay the consumer's transaction and the consumer agrees to receive the notice at a later time.

B. Subsequent Delivery of Notice

When a consumer with an existing relationship with a licensee obtains a new insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, the licensee satisfies the initial notice requirements of Subsection A of this section as follows:

(1) The licensee may provide a revised notice, under Section 13 , that covers the consumer's new insurance product or service; or

(2) If the initial, revised or annual notice that the licensee most recently provided to that consumer was accurate with respect to the new insurance product or service, the licensee does not need to provide a new notice of information practices under Subsection A of this section.

C. For purposes of this section:

(1) "Not at consumer's election" includes the scenario where a licensee acquires or is assigned a consumer's policy from another financial institution or residual market mechanism and the consumer does not have a choice about the licensee's acquisition or assignment.

(2) "Substantially delay the consumer's transaction" includes the scenario where the licensee and the individual agree over the telephone or electronically to enter into a consumer relationship involving prompt delivery of the insurance product or service but does not include the scenario where the relationship is initiated in person at the licensee's office or through other means by which the consumer may view the notice, such as on a website.

Section 8. Annual Notice of Information Practices to Consumers Required

General rule. A licensee shall provide a clear and conspicuous notice to consumers that accurately reflects its privacy policies and practices at least once in any period of twelve (12) consecutive

 © 2026 National Association of Insurance Commissioners

months. A licensee may define the twelve-consecutive-month period, but the licensee shall apply it to the consumer on a consistent basis.

A. Example. A licensee provides a notice annually if it defines the twelve-consecutive-month period as a calendar year and provides the annual notice to the consumer once in each calendar year following the calendar year in which the licensee provided the initial notice. For example, if a consumer opens an account on any day of year 1, the licensee shall provide an annual notice to that consumer by December 31 of year 2.

(1) Exceptions.

(1) A licensee that provides nonpublic personal information to nonaffiliated third parties only in accordance with Sections 22, 23, or 24 and has not changed its policies and practices with regard to disclosing Nonpublic Personal Information from the policies and practices that were disclosed in the most recent disclosure sent to consumers in accordance with this section or Section 7 shall not be required to provide an annual disclosure under this section until such time as the licensee fails to comply with any criteria described in this paragraph.

(2) A licensee is not required to provide notice if the licensee no longer has access to the consumer's nonpublic personal information.

(2) For the purposes of this Act, a licensee no longer has an obligation to continue to notify a consumer if the licensee's records do not contain a valid address. An address is deemed invalid if electronic or regular mail sent to that address by the licensee has been returned as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.

Section 9. Information to be Included in Notices of Information Practices

A. General rule. The initial, annual and revised Notice of Information Practices that a licensee provides under Sections 7,8, and 13 shall include each of the following items of information, in addition to any other information the licensee wishes to provide, that applies to the licensee and to the consumers to whom the licensee sends its Notice of Information Practices:

(1) The categories of nonpublic personal information that the licensee collects, including, but not limited to, whether information is collected from the consumer, through the consumer's transactions with affiliates or nonaffiliated third parties, or consumer reporting agencies;

(2) The categories of nonpublic personal information that the licensee discloses, including at least one example in each category. Categories may include, but are not limited to, application information, transaction information, or consumer reports;

(3) The categories of affiliates and nonaffiliated third parties, and the types of business in which they engage, to whom the licensee discloses nonpublic personal information, other than those parties to whom the licensee discloses information under Sections 22, 23, and 24. The types of businesses may be described in general terms only if the licensee uses illustrative examples of each significant line of business;

© 2026 National Association of Insurance Commissioners

(4) An explanation of the consumer's right under Section 12 to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;

(5) An explanation of the consumer's rights with regard to the sale of nonpublic personal information and disclosure of sensitive personal information pursuant to Sections 20 and 21;

(6) A description of the consumer's options to request access, correction, or deletion of nonpublic personal information about the consumer as established under this Act and the instructions for exercising such options;

(7) Any disclosures that the licensee makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);

(8) The licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; by

(a) Describing in general terms who is authorized to have access to the information; and

(b) Stating whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance with the licensee's policy. The licensee is not required to describe technical information about the safeguards it uses; and

(c) Any disclosure that the licensee makes as authorized under Section 22, 23, or 24, except that the licensee is not required to list those exceptions in the initial or annual Notice of Information Practices required by Sections 7 and 8. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.

B. The licensee's notice may include:

(1) Categories of nonpublic personal information that the licensee reserves the right to disclose in the future, but does not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the right in the future to disclose, but to whom the licensee does not currently disclose, nonpublic personal information.

C. Exceptions:

If a licensee does not disclose, and does not reserve the right to disclose, nonpublic personal information about consumers to affiliates or nonaffiliated third parties except as authorized under Sections22, 23, or 24, the licensee shall state that in its notice, in addition to the information it shall provide under Subsections A(1) and A(8) and Subsection B of this section.

D. Sample Clauses and Federal Model Privacy Form.

© 2026 National Association of Insurance Commissioners

(1) Licensees are not required to use any prescribed clauses or model form.

(2) The commissioner may determine that a Licensee's use of any of the following constitutes compliance with this Act:

(a) Sample clauses illustrating some of the notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner;

(b) Model forms illustrating notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner; or

(c) The Federal Model Privacy Forms are included in Appendix A and Appendix B, of this Act.

Section 10. Short Form Initial Notice of Information Practices

A. A licensee may satisfy the initial notice requirements in Sections 7A and 13A by providing a Short Form Initial Notice of Information Practices at the same time the licensee delivers an opt-out notice as required in Section 12 if:

(1) The licensee provides the consumer a reasonable means to obtain its Notice of Information Practices; and

(2) The licensee provides the Notice of Information Practices upon request.

B. A Short Form Initial Notice of Information Practices shall meet all of the following requirements.

(1) Be clear and conspicuous;

(2) State that the licensee's Notice of Information Practices is available upon request;

(3) Explain the reasonable means to obtain the licensee's Notice of Information Practices;

(4) Contain contact information for the commissioner; and

(5) Describe how the consumer can request access to or correction of their nonpublic personal information.

C. For purposes of this section "reasonable means to obtain the licensee's Notice of Information Practices" includes:

(1) Providing a toll-free telephone number that the consumer may call to request the notice;

(2) Providing a website or other electronic medium that is easily accessible by the consumer; or

(3) Maintaining copies of the notice at the licensee's place of business to be provided upon request.

© 2026 National Association of Insurance Commissioners

Section 11. Form of Opt-In Notice to Consumers and Opt-In Methods

A. If a licensee is required to provide an opt-int notice under Sections 20 or 21, it shall provide a clear and conspicuous notice to each of its consumers that accurately explains the information proposed to be disclosed, the use of that information, and the consumer's option to opt in to that use. The notice shall state:

(1) The licensee discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;

(2) The consumer has the option to opt in to that disclosure; and

(3) A reasonable means by which the consumer may exercise the option to opt in.

B. The licensee shall not disclose that information to a nonaffiliated third party unless the consumer has affirmatively opted in to the use.

C. The opt-in must be an affirmative act by the consumer. The licensee cannot deem a failure to respond as an opt-in or use pre-checked boxes.

D. The opt-in should be obtained separately from any other communication or consent.

E. The opt-in may be revoked at any time by the consumer.

Section 12. Form of Opt-Out Notice to Consumers and Opt-Out Methods

A. (1) If a licensee is required to provide an opt-out notice, it shall provide a clear and conspicuous notice to each consumer that accurately explains the right to opt out under that section. To the extent applicable, the notice shall state:

(a) That the licensee discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;

(b) That the consumer has the right to opt out of that disclosure; and

(c) A reasonable means by which the consumer may exercise the opt-out right.

(2) Requirements

(a) A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if the licensee:

(i) Identifies all of the categories of nonpublic personal information it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to whom the licensee discloses the information, as described in Section 9A(2) and (3), and states the consumer can opt out of the disclosure of that information; and

(ii) Identifies the insurance products or services the consumer obtains from the licensee, either singly or jointly, to which the opt-out would apply.

© 2026 National Association of Insurance Commissioners

(b) A licensee provides a reasonable means to exercise an opt-out right if it:

(i) Designates check-off boxes in a prominent position on the relevant forms with the opt-out notice;

(ii) Includes a reply form together with the opt-out notice;

(iii) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the licensee's website, if the consumer agrees to the electronic delivery of information; or

(iv) Provides a toll-free telephone number that consumers may call to opt out.

(c) A licensee does not provide a reasonable means of opting out if:

(i) The only means of opting out is for the consumer to write a letter to the licensee to exercise their opt-out right; or

(ii) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the licensee provided with the initial notice but did not include with the subsequent notice.

(d) A licensee may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

B. A licensee may provide the opt-out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 7.

C. If a licensee provides the opt-out notice after it provides the initial notice, the licensee shall include a copy of the initial notice with the opt-out notice in writing or, if the consumer agrees, electronically.

D. Joint relationships.

(1) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt-out notice. The licensee's opt-out notice shall explain how the licensee will treat an opt-out direction by a joint consumer (as explained in Paragraph (2) of this subsection).

(2) Any of the joint consumers may exercise the right to opt out. The licensee may either:

(a) Treat an opt-out direction by a joint consumer as applying to all of the associated joint consumers; or

(b) Permit each joint consumer to opt out separately.

(3) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all the joint consumers.

(4) A licensee may not require all joint consumers to opt out before it implements any opt-out direction.

© 2026 National Association of Insurance Commissioners

E. A licensee shall comply with a consumer's opt-out direction as soon as reasonably practicable but no later than 10 days after the licensee receives it.

F. A consumer may exercise the right to opt out at any time. A consumer's direction to opt-out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.

Section 13. Revised Notice of Information Practices

A. Except as otherwise authorized in this Act, a licensee shall not, directly or through an affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that the licensee provided to that consumer under Section 7, unless:

(1) The licensee has provided to the consumer a clear and conspicuous revised notice that accurately describes its policies and practices;

(2) The licensee has provided to the consumer a new opt-out notice;

(3) The licensee has given the consumer a reasonable opportunity, before the licensee discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(4) The consumer does not opt out.

B. Examples.

(1) Except as otherwise permitted by Sections 19, 20 and 21, a licensee shall provide a revised notice before it:

(a) Discloses a new category of nonpublic personal information to any nonaffiliated third party; or

(b) Discloses nonpublic personal information to a new category of nonaffiliated third party.

(2) A revised notice is not required if the licensee discloses nonpublic personal information to a new nonaffiliated third party that the licensee adequately described in its prior notice.

Section 14. Notice of Information Practices to Group Policyholders

Unless a licensee is providing notices of information practices directly to covered individuals described in Section 4G)2)(e)(i), (ii) or (iii), a licensee shall provide initial, annual and revised notices to the plan sponsor, group or blanket insurance policyholder or group annuity contract holder, or workers' compensation policyholder, in the manner described in Sections 7 through 13 of this Act, describing the licensee's privacy practices with respect to nonpublic personal information about individuals covered under the policies, contracts or plans. Compliance with this section satisfies the licensees initial, annual and renewal Notice of Information Practices as required by Sections 7 and 8 and delivery provisions of Section 15.

© 2026 National Association of Insurance Commissioners

Section 15. Delivery

A. A licensee shall provide any notices that this Act requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer interacts with the licensee online or in some other electronic fashion, electronically.

B. (1) A licensee may reasonably expect that a consumer will receive actual notice if the licensee:

(a) Hand-delivers a printed copy of the notice to the consumer;

(b) Mails a printed copy of the notice to the last known address of the consumer separately, or in a policy, billing or other written communication;

(c) For a consumer who conducts transactions electronically, in accordance with UETA (insert state electronic transactions act statute), posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service;

(i) The notice should be posted in a manner that enables a consumer to print or save it using programs or apps that are widely available and free of charge.

(ii) Notice is available electronically as long as it is in force.

(d) For an isolated transaction with a consumer, such as the licensee providing an insurance quote or selling the consumer travel insurance, posts the notice and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular insurance product or service.

(e) Provides the notice by any other means authorized by the commissioner.

(2) Examples of unreasonable expectation of actual notice. A licensee may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:

(a) Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or

(b) Sends the notice via electronic mail to a consumer who does not otherwise communicate with the licensee electronically.

C. A licensee may reasonably expect that a consumer will receive actual notice of the licensee's Notice of Information Practices if:

(1) The consumer uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or

(2) The consumer has requested that the licensee refrain from sending any information regarding the consumer relationship, and the licensee's current privacy notice remains

© 2026 National Association of Insurance Commissioners

available to the consumer upon request.

D. A licensee may not provide any notice required by this Act solely by orally explaining the notice, either in person or over the telephone.

E. A licensee may provide a joint notice from the licensee and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the licensee and the other institutions. A licensee also may provide a notice on behalf of another financial institution.

F. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of Sections 7A, 8A and 13A, respectively, by providing one notice to those consumers jointly.

© 2026 National Association of Insurance Commissioners

ARTICLE V. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 16. General Rules for Use and Disclosure of Nonpublic Personal Information

A. Use and Disclosure

(1) A licensee may use and disclose nonpublic personal information about a consumer for purposes of processing a business transaction requested or authorized by the consumer.

(2) A licensee may disclose nonpublic personal information with affiliates, provided the affiliates' use and disclosure comply with this Act.

(3) A licensee shall not disclose nonpublic personal information to a nonaffiliated third party except as permitted by this Act.

(4) This section applies to nonpublic personal information collected before and after a consumer exercises an opt-out right under Section 19 or an opt-in right under Sections 20 and 21.(5) If a consumer submits an opt-out request during a transaction and the requested information is necessary to complete that transaction, the licensee shall:

(a) Inform the consumer that the transaction cannot be completed without the information; and

(b) Confirm whether the consumer wishes to proceed.

B. Limits on Disclosure**.** Except as provided by Section 16A(1), before disclosing a consumer's nonpublic personal information to a nonaffiliated third party, whether directly or through an affiliate, a licensee shall:

(1) Provide the initial notice required by Section 7;

(2) Provide a clear and conspicuous notice to the consumer that details:

(a) The consumer's right to opt out of disclosure for targeted advertising under Section 19;

(b) The consumer's option to opt in to the sale of nonpublic personal information under Section 20; or

(c) The consumer's option to opt in to the disclosure of sensitive personal information Section 21.

(3) Provide a reasonable opportunity for the consumer to exercise any applicable opt-out right before disclosure; and

(4) Obtain and document the consumer's opt-in or opt-out election, as applicable.

Section 17. Limits on Redisclosure and Reuse of Nonpublic Personal Information

A. If a licensee receives nonpublic personal information from a nonaffiliated third-party service provider under an exception in Article VI of this Act,

© 2026 National Association of Insurance Commissioners

the licensee may use and disclose the information in the ordinary course of business to carry out the activity covered by the exception under which the licensee received the information.

B. (1) If a licensee receives nonpublic personal information from a nonaffiliated third-party service provider other than under an exception in Article VI of this Act, the licensee may disclose the information only to the following, provided the disclosure is consistent with this Act:

(a) Affiliates of the third party-service provider from which the licensee received the information; and

(b) Affiliates of the licensee who may disclose the information only to the extent that the disclosure would be permissible by the licensee pursuant to this Act.

(2) Example. If a licensee obtains a customer list from a nonaffiliated third-party service provider outside of the exceptions in Article VI:

(a) The licensee may use that list for its own purposes consistent with this Act; and

(b) The licensee may disclose that list to another nonaffiliated third-party service provider only as permitted by this Act.

C. If a licensee discloses nonpublic personal information to a nonaffiliated third-party service provider under an exception in S Article VI of this Act, the third party-service provider:

(1) May disclose the information to the licensee's affiliates; and

(2) May disclose and use the information in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

D. If a licensee discloses nonpublic personal information to a nonaffiliated third-party service provider other than under an exception in Article VI of this Act, the third-party service provider may disclose the information only:

(1) To the licensee's affiliates who may disclose the information only to the extent that it would be permissible for the licensee to disclose the information pursuant to this Act: and

(2) To any other person, if the disclosure would be lawful if the licensee made it directly to that person.

Section 18. Limits on Sharing Access Number or Access Code Information for Marketing Purposes

A. A licensee shall not, directly or through an affiliate, disclose, other than to a consumer reporting agency, a policy number or similar form of access number or access code for a consumer's policy or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

B. Exceptions. Subsection A of this section does not apply if a licensee discloses a policy number or similar form of access number or access code:

 © 2026 National Association of Insurance Commissioners

(1) To the licensee's service provider solely in order to perform marketing for the licensee's own products or services, as long as the service provider is not authorized to directly initiate charges to the account;

(2) To a licensee who is a producer solely in order to perform marketing for the licensee's own products or services; or

(3) To a participant in an affinity or similar program where the participants in the program are identified to the consumer when the consumer enters into the program.

(4) Where the policy number, or similar form of access number or access code, is in an encrypted form, as long as the licensee does not provide a means to decode the access number or access code.

Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted ~~Marketing~~ Advertising

A. Except as otherwise authorized in this Act, a licensee may not, directly or through any affiliate, disclose for the purpose of targeted advertising any nonpublic personal information about a consumer to a nonaffiliated third party unless the consumer has been provided clear and conspicuous notice and a reasonable opportunity to opt out of targeted advertising in accordance with the requirements of Section 12 of this Act.

B. A licensee shall act on a consumer's request to opt out within 15 days of receipt.

C. A licensee is under no obligation to obtain additional information to execute the opt-out request.

D. A licensee may not solicit the consumer to change their election to opt out for twelve months.

E. A consumer has the right to opt out at any time.

Section 20. Limits on Sale of Nonpublic Personal Information

Before a licensee may sell nonpublic personal information:

A. The licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

B. The consumer must affirmatively opt in to the sale of their nonpublic personal information.

Section 21. Limits on Disclosure of Sensitive Personal Information

A. Except as provided by Subsection B below, a licensee may disclose a consumer's sensitive personal information only for those purposes and uses identified in Article VI and as expressly permitted or required by Article VI or other provisions of this Act.

B. Before a licensee may disclose a consumer's sensitive personal information for purposes other than those specified in subsection A of this section:

(1) A licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

© 2026 National Association of Insurance Commissioners

(2) The consumer must affirmatively opt in to disclosure of their sensitive personal information.

© 2026 National Association of Insurance Commissioners

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 22. Exception to Opt-Out Requirements for Disclosure of Nonpublic Personal Information for Service Providers and Joint Marketing

A. General rule.

(1) The opt-out requirements in Sections 12 and 19 do not apply when a licensee provides nonpublic personal information to a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf, if the licensee:

(a) Provides the initial notice in accordance with Section7; and

(b) Enters into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in Sections 23 or 24 in the ordinary course of business to carry out those purposes.

(2) Example. If a licensee discloses nonpublic personal information under this section to a financial institution with which the licensee performs joint marketing, the licensee's contractual agreement with that institution meets the requirements of Paragraph (1)(b) of this subsection if it prohibits the institution from disclosing or using the nonpublic personal information except as necessary to carry out the joint marketing or under an exception in Sections 23 or 24 in the ordinary course of business to carry out that joint marketing.

B. Service may include joint marketing. The services a nonaffiliated third party performs for a licensee under Subsection A of this section may include marketing of the licensee's own products or services or marketing of financial products or services offered pursuant to joint agreements between the licensee and one or more financial institutions.

C. Definition of "joint agreement." For purposes of this section, "joint agreement" means a written contract pursuant to which a licensee and one or more financial institutions jointly offer, endorse or sponsor a financial product or service.

Section 23. Exceptions to Notice and Opt-Out Requirements for Disclosure of Nonpublic Personal Information for Processing and Servicing Transactions

A. Exceptions for processing transactions at consumer's request. The requirements for initial notice in Section 7A(2), the opt-out in Sections 12 and 19, and service providers and joint marketing in Section 22 do not apply if the licensee discloses nonpublic personal information as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Servicing or processing an insurance product or service that a consumer requests or authorizes;

© 2026 National Association of Insurance Commissioners

(2) Maintaining or servicing the consumer's account with a licensee, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity;

(3) A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer; or

(4) Reinsurance or stop loss or excess loss insurance.

B. "Necessary to effect, administer or enforce a transaction" means that the disclosure is:

(1) Required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or

(2) Required, or is a usual, appropriate or acceptable method:

(a) To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer's account in the ordinary course of providing the insurance product or service;

(b) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

(c) To provide a confirmation, statement or other record of the transaction, or information on the status or value of the insurance product or service to the consumer or the consumer's agent or broker;

(d) To accrue or recognize incentives or bonuses associated with the transaction that are provided by a licensee or any other party;

(e) To underwrite insurance at the consumer's request or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects or as otherwise required or specifically permitted by federal or state law; or

(f) In connection with:

(i) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited or otherwise paid using a debit, credit or other payment card, check or account number, or by other payment means;

(ii) The transfer of receivables, accounts or interests therein; or

(iii) The audit of debit, credit or other payment information.

© 2026 National Association of Insurance Commissioners

Section 24. Other Exceptions to Notice and Opt-Out Requirements for Disclosure of Nonpublic Personal Information

A. Exceptions to opt out requirements. The requirements for initial notice to consumers in Section 7A(2), the opt-out in Sections 12 and 19, and service providers and joint marketing in Section 22 do not apply when a licensee discloses nonpublic personal information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

(2) (a) To protect the confidentiality or security of a licensee's records pertaining to the consumer, service, product or transaction;

(b) To protect against or prevent actual or potential fraud or unauthorized transactions;

(c) For required institutional risk control or for resolving consumer disputes or inquiries;

(d) To persons holding a legal or beneficial interest relating to the consumer; or

(e) To persons acting in a fiduciary or representative capacity on behalf of the consumer;

(f) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted nonpublic personal information.

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating a licensee, persons that are assessing the licensee's compliance with industry standards, and the licensee's attorneys, accountants and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the federal Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, the Securities and Exchange Commission, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance authority, and the Federal Trade Commission), self-regulatory organizations or for an investigation on a matter related to public safety;

(5) (a) To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or

(b) From a consumer report reported by a consumer reporting agency;

© 2026 National Association of Insurance Commissioners

(6) In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of the business or unit;

(7) (a) To comply with federal, state or local laws, rules and other applicable legal requirements;

(b) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities; or

(c) To respond to judicial process or government regulatory authorities having jurisdiction over a licensee for examination, compliance or other purposes as authorized by law; or

(8) For purposes related to the replacement of a group benefit plan, a group health plan, a group welfare plan or a workers' compensation plan.

B. Example of revocation of consent. A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under Section 12F.

Drafting Note: Because the notice requirements of this Act could be a financial burden on a company in liquidation or receivership and negatively impact the ability of the liquidator or receiver to pay claims, regulators may want to consider adding an additional exception providing that licensees in liquidation or receivership are not subject to the notice provisions of this Act.

© 2026 National Association of Insurance Commissioners

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 25. When Authorization Required for Disclosure of Nonpublic Personal Health Information

A. A licensee shall not disclose nonpublic personal health information about a consumer unless an authorization is obtained from the consumer whose nonpublic personal health information is sought to be disclosed.

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee:

(1) Claims administration any processing;

(2) Claims adjustment and management;

(3) Detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity;

(4) Underwriting;

(5) Policy placement or issuance;

(6) Loss control;

(7) Ratemaking and guaranty fund functions;

(8) Reinsurance and excess loss insurance;

(9) Risk management;

(10) Case management;

(11) Disease management;

(12) Quality assurance;

(13) Quality improvement;

(14) Performance evaluation;

(15) Provider credentialing verification;

(16) Utilization review;

(17) Peer review activities;

(18) Actuarial, scientific, medical or public policy research;

(19) Grievance procedures;

© 2026 National Association of Insurance Commissioners

(20) Internal administration of compliance, managerial, and information systems;

(21) Policyholder service functions;

(22) Auditing;

(23) Reporting;

(24) Database security;

(25) Administration of consumer disputes and inquiries;

(26) External accreditation standards;

(27) The replacement of a group benefit plan or workers' compensation policy or program;

(28) Activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit;

(29) Any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services or other applicable laws;

(30) Disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes including subrogation, and

(31) Any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with the legal process.

C. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable

Section 26. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article VII shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer who is the subject of the nonpublic personal health information;

(2) A general description of the types of nonpublic personal health information to be disclosed;

(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

(4) The signature, including electronic signatures, of the consumer who is the subject of the

 © 2026 National Association of Insurance Commissioners

nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer may revoke the authorization at any time and the procedure for making a revocation.

(6) Any additional information necessary to comply with HIPAA or any other applicable law.

B. An authorization for the purposes of this Article VII shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article VII at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

E. A signed copy of the authorization shall be provided to the consumer.

Section 27. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer as part of an opt-out notice pursuant to Section 12, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section 25A.

Section 28. Relationship to Federal Rules

A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

This Act shall not apply to nonprofits, such as the National Association of Insurance Commissioners or the National Insurance Crime Bureau, when processing or sharing information solely for investigating criminal or fraudulent insurance acts.

Section 29. Relationship to State Laws

Nothing in this Article shall preempt or supersede existing state law related to medical records, consumer data privacy, health or insurance information privacy, or other mandatory reporting, immunity, or confidentiality laws.

© 2026 National Association of Insurance Commissioners

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 30. Protection of Fair Credit Reporting Act

Nothing in this Act shall be construed to modify, limit or supersede the operation of the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and no inference shall be made regarding whether information is transaction or experience information under Section 603 of that Act.

Section 31. Nondiscrimination

A. A licensee shall not unfairly discriminate against any consumer because that consumer has opted out from the disclosure of his or her nonpublic personal information pursuant to the provisions of this Act.

B. A licensee shall not unfairly discriminate against a consumer because that consumer has not granted authorization for the disclosure of his or her nonpublic personal health information pursuant to the provisions of this Act.

Section 32. Violation

Drafting Note: Cite state unfair trade practices act or other applicable state law.

Section 33. Severability

If any section or portion of a section of this Act or its applicability to any person or circumstance is held invalid by a court, the remainder of the Act or the applicability of the provision to other persons or circumstances shall not be affected.

Section 34. Individual Remedies

This Act may not be construed to create or imply a private cause of action for violation of its provisions, nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Section 35. Effective Date

A. Effective date. This Act has been effective since November 13, 2000. The amendments to this Act are effective [Insert Effective Date]. In order to provide sufficient time for licensees to establish policies and systems to comply with the amendments to this Act, the commissioner has extended the time for compliance with the amendments to this Act until [Insert Compliance Date].

B. By [Insert Compliance Date], a licensee shall provide an initial notice, as required by Section 7, to any existing consumer who has not previously received a notice that complies with the amendments to this Act.

C. Two-year grandfathering of service agreements. Until [Insert Compliance Date], a contract that a licensee has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf satisfies the provisions of Section 22A(1)(b) of this Act, even if

© 2026 National Association of Insurance Commissioners

the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the licensee entered into the agreement on or before [Insert Compliance Date].

© 2026 National Association of Insurance Commissioners

APPENDIX A – SAMPLE CLAUSES

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A-1–Categories of information a licensee collects (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(1) to describe the categories of nonpublic personal information the licensee collects.

Sample Clause A-1:

We collect nonpublic personal information about you from the following sources:

Information we receive from you on applications or other forms;
Information about your transactions with us, our affiliates or others; and
Information we receive from a consumer reporting agency.

A-2–Categories of information a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use one of these clauses, as applicable, to meet the requirement of Section 9A(2) to describe the categories of nonpublic personal information the licensee discloses. The licensee may use these clauses if it discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-2, Alternative 1:

We may disclose the following kinds of nonpublic personal information about you:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premiums, and payment history"]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your creditworthiness and credit history"].

Sample Clause A-2, Alternative 2:

We may disclose all of the information that we collect, as described [describe location in the notice, such as "above" or "below"].

A-3–Categories of information a licensee discloses and parties to whom the licensee discloses (institutions that do not disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirements of Sections 9A(2) and (3) to describe the categories of nonpublic personal information the licensee discloses and the categories of affiliates and

© 2026 National Association of Insurance Commissioners

nonaffiliated third parties to whom the licensee discloses. A licensee may use this clause if the licensee does not disclose nonpublic personal information to any party, other than as permitted by the exceptions in Sections 23 and 24.

Sample Clause A-3:

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

A-4–Categories of parties to whom a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(3) to describe the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information. This clause may be used if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-4:

We may disclose nonpublic personal information about you to the following types of third parties:

Financial service providers, such as [provide illustrative examples, such as "life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents"];

Non-financial companies, such as [provide illustrative examples, such as "retailers, direct marketers, airlines, and publishers"]; and

Others, such as [provide illustrative examples, such as "non-profit organizations"].

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

A-5–Service provider/joint marketing exception
A licensee may use one of these clauses, as applicable, to meet the requirements of Section 9A(2) related to the exception for service providers and joint marketers in Section 22. If a licensee discloses nonpublic personal information under this exception, the licensee shall describe the categories of nonpublic personal information the licensee discloses and the categories of third parties with which the licensee has contracted.

Sample Clause A-5, Alternative 1:

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premium, and payment history"]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your creditworthiness and credit history"].

© 2026 National Association of Insurance Commissioners

Sample Clause A-5, Alternative 2:

We may disclose all of the information we collect, as described [describe location in the notice, such as "above" or "below"] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

A-6–Explanation of opt- out right (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(4) to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. The licensee may use this clause if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-6:

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [describe a reasonable means of opting out, such as "call the following toll-free number: (insert number)].

A-7–Confidentiality and security (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(8) to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A-7:

We restrict access to nonpublic personal information about you to [provide an appropriate description, such as "those employees who need to know that information to provide products or services to you"]. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

© 2026 National Association of Insurance Commissioners

APPENDIX B – FEDERAL MODEL PRIVACY FORM

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the Federal Model Privacy Form, if the Form is accurate for each institution that uses the Form. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A. General Instructions

1. How the Model Privacy Form is used.

(a) The Model Form may be used, at the option of a "licensee", including a group of licensees or other financial institutions that use a common privacy notice, to meet the content requirements of the privacy notice and opt-out notice set forth in [insert citation for sections of statute or regulation sections that parallel Sections 9and 11 of the NAIC *Privacy of Consumer InformationAct*]

(b) The Model Form is a standardized form, including page layout, content, format, style, pagination, and shading. Licensees seeking to obtain the safe harbor through use of the Model Form may modify it only as described in these Instructions.

(c) Note that disclosure of certain information, such as assets, income, and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act (FCRA), codified at 15 U.S.C. §§ 1681-1681x, such as a requirement to permit a consumer to opt out of disclosures to affiliates, or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.

(d) The word "consumer" may be replaced by the word "member," whenever it appears in the Model Form, as appropriate.

2. The Contents of the Model Privacy Form

The Model Form consists of two pages, which may be printed on both sides of a single sheet of paper or may appear on two separate pages. Where a licensee provides a long list of licensees or financial institutions at the end of the Model Form in accordance with Instruction B3(a)(i), or provides additional information in accordance with Instruction B3(c) and such list or additional information exceeds the space available on Page Two of the Model Form, such list or additional information may extend to a third page.

(a) Page One. The first page consists of the following components:

(1) Date last revised (upper right-hand corner)
(2) Title
(3) Key frame (Why? What? How?)
(4) Disclosure table ("Reasons we can share your personal information")
(5) "To limit our sharing" box, as needed, for the licensee's opt-out information
(6) "Questions" box, for customer service contact information
(7) Mail-in opt-out form, as needed

(b) Page Two. The second page consists of the following components:

© 2026 National Association of Insurance Commissioners

(1) Heading (Page 2)
(2) Frequently Asked Questions (“Who we are” and “What we do”)
(3) Definitions
(4) “Other important information” box, as needed

3. The format of the Model Privacy Form.

The format of the Model Form may be modified only as described below.

(a) Easily readable type font. Licensees that use the Model Form must use an easily readable type font. While a number of factors together produce easily readable font, licensees are required to use a minimum of 10- point font (unless otherwise expressly permitted in these Instructions) and sufficient spacing between lines.

(b) Logo. A licensee may include a corporate logo on any page of the notice, so long as it does not interfere with the readability of the Model Form or the space constraints of each page.

(c) Page size and orientation. Each page of the Model Form must be printed in portrait orientation, the size of which must be sufficient to meet the layout and minimum font size requirements, with sufficient white space on the top, bottom, and sides of the content.

(d) Color. The Model Form must be printed on white or light color paper (such as cream) with black or other contrasting ink color. Spot color may be used to achieve visual interest, so long as the color contrast is distinctive and the color does not detract from the readability of the Model Form. Logos may also be printed in color.

(e) Languages. The Model Form may be translated into languages other than English.

B. Information Required in the Model Privacy Form

The information in the Model Form may be modified only as described below:

1. Name of licensee or group of affiliated licensees or institutions providing the notice
Insert the name of the licensee providing the notice, or a common identity of the affiliated licensees or financial institutions jointly providing the notice on the form, wherever [name of licensee] appears.

2. Page One

(a) Last revised date. The licensee must insert in the upper right-hand corner the date on which the notice was last revised. The information shall appear in minimum 8-point font as “rev. [month/year]” using either the name or number of the month, such as “rev. July 2016” or “rev. 7/16.”

(b) General instructions for the “What?” box

(i) The bulleted list identifies the types of personal information that the licensee collects and shares. All licensees must use the term “Social Security Number” in the first bullet.

(ii) A licensee must use five (5) of the following terms, to complete the bulleted list: income; account balances; payment history; transaction history; transaction or loss history; credit history; credit scores; assets; investment experience; credit-based insurance scores; insurance claim history; medical information; overdraft history; purchase history; account transactions; risk tolerance; medical-related debts; credit card or other debt;

 © 2026 National Association of Insurance Commissioners

mortgage rates and payments; retirement assets; checking account information; employment information; wire transfer instructions.

(c) General instructions for the disclosure table. The left column lists reasons for sharing or using personal information. Each reason correlates to a specific legal provision described in Paragraph 2(d) of this Instruction. In the middle column, each licensee must provide a "Yes" or "No" response that accurately reflects its information-sharing policies and practices with respect to the reason listed on the left. In the right column, each licensee must provide in each box one of the following three (3) responses, as applicable, that reflects whether a consumer can limit such sharing:

"Yes," if it is required to or voluntarily provides an opt-out; "No," if it does not provide an opt-out; or

"We don't share," if it answers "No" in the middle column.

Only the sixth row ("For our affiliates to market to you") may be omitted at the option of the licensee. See Paragraph 2(d)(6) of this instruction.

(d) Specific disclosures and corresponding legal provisions

(i) For our everyday business purposes. This reason incorporates sharing information under [insert citation for sections of statute or regulation sections that parallel Sections 23 and 24 of NAIC model *Privacy of Consumer InformationAct*] and with service providers pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*] other than the disclosures described in Paragraphs (2)(d)(ii) or (2)(d)(iii) of this instruction.

(ii) For our marketing purposes. This reason incorporates sharing information with service providers by a licensee for its own marketing pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iii) For joint marketing with other financial companies. This reason incorporates sharing information under joint marketing agreements between 2 or more licensees or financial institutions and with any service provider used in conjunction with such agreement pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iv) For our affiliates' everyday business purposes – information about transactions and experiences. This reason incorporates sharing information specified in Sections 603(d)(2)(A)(i) and (ii) of the FCRA. A licensee that shares information for this reason may choose to provide an opt-out.

(v) For our affiliates' everyday business purposes – information about creditworthiness. This reason incorporates sharing information pursuant to Section 603(d)(2)(A)(iii) of the FCRA. A licensee that shares information for this reason must provide an opt-out.

(vi) For our affiliates to market to you. This reason incorporates sharing information specified in Section 624 of the FCRA. This reason may be omitted from the disclosure table when: the licensee does not have affiliates (or does not disclose personal information to its affiliates); the licensee's affiliates do not use personal information in a manner that requires an opt-out; or the licensee provides the affiliate marketing notice separately. Licensees that include this reason must provide an opt-out of indefinite duration. A licensee that is required to provide an affiliate marketing opt-out, but does not include that opt-out in the Model Form under this part, must comply

© 2026 National Association of Insurance Commissioners

with Section 624 of the FCRA and [insert citation for statute or regulation that parallels NAIC *Privacy of Consumer Information Act*], with respect to the initial notice and opt-out and any subsequent renewal notice and opt-out. A licensee not required to provide an opt-out under this subparagraph may elect to include this reason in the Model Form.

(vii) For nonaffiliates to market to you. This reason incorporates sharing described in [insert citation for sections of statute or regulation sections that parallel Sections 11 and 16(B) of NAIC *Privacy of Consumer Information Act*]. A licensee that shares personal information for this reason must provide an opt-out.

(e) To limit our sharing. A licensee must include this section of the Model Form only if it provides an opt-out. The word "choice" may be written in either the singular or plural, as appropriate. Licensees must select one or more of the applicable opt-out methods described: telephone, such as by a toll-free number; a web site; or use of a mail-in opt-out form. Licensees may include the word "toll-free" before telephone, as appropriate. A licensee that allows consumers to opt out online must provide either a specific web address that takes consumers directly to the opt-out page or a general web address that provides a clear and conspicuous direct link to the opt-out page. The opt-out choices made available to the consumer who contacts the licensee through these methods must correspond accurately to the "Yes" responses in the third column of the disclosure table. In the part entitled "Please note," licensees may insert a number that is 30 days or greater in the space marked "[30]." Instructions on voluntary or state privacy law opt-out information are in Paragraph 2(g)(v) of these Instructions.

(f) Questions box. Customer service contact information must be inserted as appropriate where [phone number] or [web site] appear. Licensees may elect to provide either a phone number, such as a toll-free number, or a web address, or both. Licensees may include the words "toll-free" before the telephone number, as appropriate.

(g) Mail-in opt-out form. Licensees must include this mail-in form only if they state in the "To limit our sharing" box that consumers can opt out by mail. The mail-in form must provide opt-out options that correspond accurately to the "Yes" responses in the third column of the disclosure table. Licensees that require consumers to provide only name and address may omit the section identified as "[account #]." Licensees that require additional or different information, such as a random opt-out number or a truncated account number to implement an opt-out election should modify the "[account #]" reference accordingly. This includes licensees that require customers consumers with multiple accounts to identify each account to which the opt-out should apply. A licensee must enter its opt-out mailing address in the far right of this form (see version 3); or below the form (see version 4). The reverse side of the mail-in opt-out form must not include any content of the Model Form.

(i) Joint accountholder. Only licensees that provide their joint accountholders the choice to opt out for only one accountholder, in accordance with Paragraph 3(a)(5) of these Instructions, must include in the far left column of the mail-in form the following statement:

If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.

□ Apply my choice(s) only to me.

The word "choice" may be written in either the singular or plural, as appropriate. Licensees that provide insurance products or services, provide this option, and elect to use the Model Form may substitute the word "policy" for "account" in this statement. Licensees that do not provide this option may eliminate this left column from the mail-in form.

(ii) FCRA Section 603(d)(2)(A)(iii) opt-out. If the licensee shares personal information pursuant to Section 603(d)(2)(A)(iii) of the FCRA, it must include in the mail-in opt-out form the following statement:

© 2026 National Association of Insurance Commissioners

□ Do not share information about my creditworthiness with your affiliates for their everyday business purposes.

(iii) FCRA Section 624 opt-out. If the licensee uses Section 624 of the FCRA, in accord with paragraph 2(d)(6) of these Instructions, it must include in the mail-in opt-out form the following statement:

□ Do not allow your affiliates to use my personal information to market to me.

(iv) Nonaffiliate opt-out. If the licensee shares personal information pursuant to [insert citation for section of statute or regulation that parallels Section 16(B) of NAIC *Privacy of Consumer InformationAct*], it must include in the mail-in opt-out form the following statement:

□ Do not share my personal information with nonaffiliates to market their products and services to me.

(v) Additional opt-outs. Licensees that use the disclosure table to provide opt-out options beyond those required by Federal law must provide those opt-outs in this section of the Model Form. A licensee that chooses to offer an opt-out for its own marketing in the mail-in opt-out form must include one of the two following statements:

□ Do not share my personal information to market to me. or

□ Do not use my personal information to market to me.

A licensee that chooses to offer an opt-out for joint marketing must include the following statement:

□ Do not share my personal information with other financial institutions to jointly market to me.

(h) Barcodes. A licensee may elect to include a barcode and/or "tagline" (an internal identifier) in 6-point type at the bottom of page one, as needed for information internal to the licensee, so long as these do not interfere with the clarity or text of the form.

3. Page Two

(a) General Instructions for the Questions. Certain Questions on the Model Form may be customized as follows:

(i) "Who is providing this notice?" This question may be omitted where only one licensee provides the Model Form and that licensee is clearly identified in the title on Page One. Two or more licensees or financial institutions that jointly provide the Model Form must use this question to identify themselves as required by [insert citation for section of statute or regulation that parallels Section 15(E) of NAIC model *Privacy of Consumer Information Act*]. Where the list of licensees or financial institutions exceeds four (4) lines, the licensee must describe in the response to this question the general types of licensees or financial institutions jointly providing the notice and must separately identify those licensees or financial institutions, in minimum 8-point font, directly following the "Other important information" box, or, if that box is not included in the licensee's form, directly following the "Definitions." The list may appear in a multi- column format.

(ii) "How does [name of licensee] protect my personal information?" The licensee may only provide additional information pertaining to its safeguards practices following the designated response to this question. Such information may include information about the licensee's use of cookies or other measures it uses to safeguard personal information. Licensees are limited to a maximum of 30 additional words.

© 2026 National Association of Insurance Commissioners

(iii) "How does [name of licensee] collect my personal information?" Licensees must use five (5) of the following terms to complete the bulleted list for this question: open an account; deposit money; pay your bills; apply for a loan; use your credit or debit card; seek financial or tax advice; apply for insurance; pay insurance premiums; file an insurance claim; seek advice about your investments; buy securities from us; sell securities to us; direct us to buy securities; direct us to sell your securities; make deposits or withdrawals from your account; enter into an investment advisory contract; give us your income information; provide employment information; give us your employment history; tell us about your investment or retirement portfolio; tell us about your investment or retirement earnings; apply for financing; apply for a lease; provide account information; give us your contact information; pay us by check; give us your wage statements; provide your mortgage information; make a wire transfer; tell us who receives the money; tell us where to send the money; show your government-issued ID; show your driver's license; order a commodity futures or option trade.

Licensees that collect personal information from their affiliates and/or credit bureaus must include the following statement after the bulleted list: "We also collect your personal information from others, such as credit bureaus, affiliates, or other companies." Licensees that do not collect personal information from their affiliates or credit bureaus but do collect information from other companies must include the following statement instead: "We also collect your personal information from other companies." Only licensees that do not collect any personal information from affiliates, credit bureaus, or other companies can omit both statements.

(iv) "Why can't I limit all sharing?" Licensees that describe state privacy law provisions in the "Other important information" box must use the bracketed sentence: "See below for more on your rights under state law." Other licensees must omit this sentence.

(v) "What happens when I limit sharing for an account I hold jointly with someone else?" Only licensees that provide opt-out options must use this question. Other licensees must omit this question. Licensees must choose one of the following two statements to respond to this question: "Your choices will apply to everyone on your account." or "Your choices will apply to everyone on your account—unless you tell us otherwise." Licensees may substitute the word "policy" for "account" in these statements.

(b) General Instructions for the Definitions. The licensee must customize the space below the responses to the three definitions in this section. This specific information must be in italicized lettering to set off the information from the standardized definitions.

(i) Affiliates. As required by [insert citation for section of statute or regulation that parallels Section 9(A)(3) of NAIC *Privacy of Consumer Information Act*], where [affiliate information] appears, the licensee must:

(a) If it has no affiliates, state: "[name of licensee] has no affiliates";

(b) If it has affiliates but does not share personal information with them, state: "[name of licensee] does not share with our affiliates"; or

(c) If it shares with its affiliates, state, as applicable: "Our affiliates include companies with a [common corporate identity of licensee] name; financial companies such as [insert illustrative list of companies]; nonfinancial companies, such as [insert illustrative list of companies]; and others, such as [insert illustrative list]."

(ii) Nonaffiliates. As required by [insert citation for section of statute or regulation that parallels Section 9)(A)(3) of NAIC *Privacy of Consumer InformationAct*], where [nonaffiliate information] appears, the licensee must:

(a) If it does not share with nonaffiliated third parties, state: "[name of licensee] does not share with

 © 2026 National Association of Insurance Commissioners

nonaffiliates so they can market to you"; or

(b) If it shares with nonaffiliated third parties, state, as applicable: "Nonaffiliates we share with can include [list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations]."

(iii) Joint Marketing. As required by [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*], where [joint marketing] appears, the licensee must:

(a) If it does not engage in joint marketing, state: "[name of licensee] doesn't jointly market"; or

(b) If it shares personal information for joint marketing, state, as applicable: "Our joint marketing partners include [list categories of companies such as credit card companies]."

(c) General instructions for the "Other important information" box. This box is optional. The space provided for information in this box is not limited, and an additional page may be used if necessary. Only the following types of information can appear in this box:

(i) State and/or international privacy law information; and/or

(ii) A form by which the consumer may acknowledge receipt of the notice.

Chronological Summary of Actions (all references are to the Proceedings of the NAIC)

2000 Proc. 3rd Quarter 7, 10, 14-36, 904 (adopted).
2002 Proc. 3rd Quarter12, 13, 71, 72-73 (amended).
2017 Spring National Meeting (amended).

© 2026 National Association of Insurance Commissioners

Version 1:
Model Form with No Opt-Out

Rev. [insert date]

FACTS	WHAT DOES [Name of Licensee] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores] When you are *no longer* our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

Questions?	Call [phone number] or go to [web site]

© 2026 National Association of Insurance Commissioners

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Version 2: Model Form with Opt-Out by Telephone and/or Online

Rev. [insert date]

FACTS	WHAT DOES [NAME OF LICENSEE] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

To limit our sharing	■ Call [phone number] —our menu will prompt you through your choice(s) **or** ■ Visit us online: [web site] **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

© 2026 National Association of Insurance Commissioners

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Rev. [insert date

Version 3: Model Form with Mail-in Opt-Out Form

FACTS	WHAT DOES [NAME OF LICENSEE] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— **to offer our products and services to you**		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

© 2026 National Association of Insurance Commissioners

Page 2

To limit our sharing	▪ Call [phone number] —our menu will prompt you through your choice(s) ▪ Visit us online: [web site] or ▪ Mail the form below **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

Mail-in Form

Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless your mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me.	
	Name	
	Address	
	City, State, Zip	
	[Account #]	
Mail To:	[Name of Licensee] [Address] [City], [ST] [ZIP]	

© 2026 National Association of Insurance Commissioners

Page 3

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ▪ [open an account] or [deposit money] ▪ pay your bills] or [apply for a loan] ▪ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ▪ sharing for affiliates' everyday business purposes—information about your creditworthiness ▪ affiliates from using your information to market to you ▪ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ▪ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ▪ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ▪ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Version 4: Optional Mail-in Form

Mail-in Form	
Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me. **Name** **Address** **City, State, Zip** **[Account #]**
Mail To:	[Name of Licensee], [Address 1], [Address 2], [City], [ST] [ZIP]

EVERSHEDS SUTHERLAND

THE Committee OF Annuity Insurers
www.annuity-insurers.org

September 22, 2026

RE: Revised Model Law 672 – Full Exposure Draft

Dear Chair Dwyer and Co-Vice Chairs Houdek and Cornelius:

The Committee of Annuity Insurers (CAI or Committee)[1] appreciates the opportunity to submit the following comments to the NAIC Privacy Protections (H) Working Group (Working Group) on the Full Draft of Revised Model 672 dated July 24, 2026 (the Full Exposure Draft).

OVERVIEW

The CAI recognizes and appreciates the Working Group's tireless efforts to enhance privacy protections for consumers through a revised version of Model 672, an established and time-tested framework. While the Committee supports enhancing consumer privacy in a manner tailored to the insurance sector, the Committee respectfully submits that substantial work is still needed and meaningful revisions and clarifications to the Full Exposure Draft are necessary to ensure that the final model law is clear, workable, protects consumers and at the same time does not place insurers issuing annuity contracts at a competitive disadvantage relative to other financial services providers. Absent such revisions and clarifications, the CAI is concerned that the revised Model could inadvertently harm the very consumers it seeks to protect by limiting their access to annuity products that provide unique retirement savings benefits.

We note that key provisions of the Full Exposure Draft (particularly those discussed further below) unfortunately remain very unclear, making it extremely difficult at this juncture to assess the intended meaning and effect of the proposed revisions. In several instances, it is unclear whether proposed changes are intentional policy choices that raise significant concerns or whether they are merely the result of inadvertent drafting oversights. We respectfully submit that the Full Exposure Draft must be clarified and stakeholders must have additional meaningful opportunity to comment on a clearly articulated proposal before the revised Model is finalized. As this process continues, we strongly encourage the Working Group to provide more information on how it has assessed and responded to comments received, why it has proposed the language it has, and what it hopes to accomplish by doing so. Providing this kind of transparent communication, similar to what would be provided as part of a state or federal administrative rulemaking process, would maximize the utility and efficiency of the process going forward and ensure that the Working Group and stakeholders are talking to each other, not past each other.

We have focused the substance of our current comments on what we believe is the intended meaning of the revisions in the Full Exposure Draft and the most critical issues they raise. As you continue to work through this process, we strongly urge you to provide stakeholders with explanations of the Working Group's thinking on key issues and fair opportunity for all stakeholders to submit comments on further proposed revisions to Model 672 based on that information .

The comments below focus on issues of particular importance that we have identified in the Full Exposure Draft. In addition, we have appended to this letter an annotated and red-lined copy of the Full Exposure Draft, which includes additional issues and clean-up that we believe need to be addressed,

[1] The Committee of Annuity Insurers is a coalition of life insurance companies that issue annuities. It was formed in 1981 to address legislative and regulatory issues relevant to the annuity industry and to participate in the development of public policy with respect to securities, state regulatory and tax issues affecting annuities. The CAI's current 33 member companies represent approximately 80% of the annuity business in the United States. More information is available at https://www.annuity-insurers.org/.

our reasoning, and suggested language. We hope you find these comments and suggestions constructive and helpful at this juncture.

COMMENTS

1. **The final Model framework must not leave insurers at a competitive disadvantage. Limiting the regulatory burden on insurers and preserving the ability to engage in joint marketing and compete in the broader marketplace is crucial.**

   Annuity products compete with traditional investment accounts, like bank savings accounts and mutual funds, among others. Annuity products provide unique benefits to consumers — like guaranteed income and limited downside risk — that cannot be replicated by traditional retirement savings products. Those competing products are regulated under the Gramm-Leach-Bliley Act (GLBA) through the SEC's recently updated Regulation S-P, which continues to take an opt-out approach consistent with current Model 672. Those products are not subject to privacy rules under state insurance laws. Differences in regulatory burden directly influence product development and pricing decisions and influence financial advisors' product recommendations. If revised Model 672 subjects annuity insurers to materially more limiting and burdensome standards than the standards applicable to traditional retirement savings products, it will hamstring insurers from effectively competing in the broader financial services marketplace; financial advisors would be less likely to recommend annuity products and consumers who would benefit from an annuity would be less likely to have access to them.

   While some limited opt-in (consent) requirements may be workable with appropriate exemptions in place, the best way to ensure annuity insurers can remain competitive in marketing their products to consumers who could benefit from them is by maintaining a predominantly opt-out approach consistent with current Model 672 and the GLBA. As discussed further below and in our attached markup, clarifying changes are needed to ensure that annuity insurers are not prevented from competing in the broader financial services marketplace. Above all, the Committee urges the Working Group to carefully consider any changes that may put annuity insurers at a competitive disadvantage compared to competing non-insurance retirement products. In particular, we emphasize that it is imperative that final revisions retain the existing joint marketing exemption in Section 22, which is essential to annuity insurers' ability to educate consumers and compete with non-insurance retirement products. Additionally, it is important that newly defined restrictions on the ability to disclose personal information to nonaffiliated third parties (such as the limits on sales or targeted advertising) do not act to limit the ability of annuity insurers to market their products or compete with non-insurance retirement products.

2. **The contractual requirements of Section 5 should be integrated into Section 22 to clarify how they fit into the existing Model 672 structure and to avoid creating unintended duplication or confusion.**

   As we have previously commented, mandating that all service provider contracts contain certain prescriptive provisions is a problematic approach. To the extent a licensee is unable to extract contractual terms that precisely match the requirements of Section 5, the licensee would be effectively barred from using that service provider, regardless of whether that service provider would be the most beneficial for the licensee and its consumers overall. We suggest that it should be sufficient for licensees to remain responsible for compliance with the law, including when nonpublic personal information (NPI) is processed by service providers on their behalf.

   Additionally, current Section 5 and Section 22A contain two separate and inconsistent provisions establishing contractual requirements for third-party service providers to qualify for the service provider exemption. It is also unclear whether joint marketing agreements required under Section 22 are also subject to the requirements of Section 5. This duplication and ambiguity generates confusion around how the Section 5 requirements apply. At minimum, the requirements of Section 5 should be integrated into the existing third-party service provider contracting provisions of Section 22A. More limited contractual requirements for joint marketing agreements with nonaffiliated third

parties that are not third-party service providers should be separately and clearly established in Section 22B. This would better preserve the existing structure of Model 672, avoid unintended consequences that may arise from structural changes to the existing model, and clarify the distinction between the contractual requirements for third party service providers and the contractual requirements for nonaffiliated third parties that are not third-party service providers.

In addition, we urge the Working Group to provide more flexibility under Section 5 for third-party service providers to (i) respond to lawful requests by law enforcement or a governmental body without requiring a "valid and binding" order; and (ii) notify the licensee of its failure to meet any of the contractual obligations in Section 5 promptly after discovery, rather than specifying a strict and unnecessarily prescriptive 48-hour time period that would need to be uniform across all service provider contracts. Finally, Section 5B should clarify that the licensee's responsibility for "handling" NPI is limited to the NPI the licensee disclosed to the third-party service provider.

3. Licensees should not be required to disclose a list of all third-party service providers to whom the licensee has disclosed a consumer's NPI.

The proposed obligation under Section 6A(1)(b) to provide a list of all third-party service providers to whom a licensee has disclosed a consumer's NPI would be burdensome, complex, and serve little apparent consumer protection purpose.

The CAI believes that consumer disclosure obligations should provide meaningful, actionable information to the consumer rather than overwhelming them with information they cannot use and may not have requested. The list of service providers would have to be provided even if the consumer does not want and does not request the information, such as where the consumer is only interested in what NPI the licensee maintains about the consumer. It is unclear what meaningful benefit this information would provide to a requesting consumer. The average consumer has little use or interest in knowing the reinsurer, third-party administrator, managing general agent, cloud service provider, or other vendor that the licensee engages to carry out the business of insurance. Even if a consumer objected to the use of a particular third-party service provider, there is (appropriately) no right for a consumer to choose which third party service providers a licensee uses. Pursuant to the exemption for service providers under Section 22, a consumer has no right to opt out from having their NPI shared with a particular third-party service provider.

It would also be very challenging and resource intensive for licensees to track exactly which service providers have received NPI about which consumers. Different vendors may be used for different products, those vendors change over time, and some vendors may be relevant in some circumstances but not others. For example, one vendor may be used in connection with processing claims for certain products, at certain times, but not for others. Determining whether a particular consumer's data was sent to that vendor would require the licensee to determine whether that consumer filed a claim on the particular product, during the particular time frame, when it would have gone to that vendor. There are many other additional factors and circumstances that could add substantial complexity and operational difficulty to tracking exactly which service providers have received NPI about a particular consumer. Moreover, this requirement is not subject to any time limitation and could therefore be read to require a licensee to provide lists spanning decades of third-party service providers with whom the licensee no longer has a business relationship.

Accordingly, the CAI recommends limiting this disclosure obligation to *categories* of nonaffiliated third parties to whom the licensee has disclosed the consumer's NPI in the preceding 12 months. This approach would be consistent with the general approach taken under the California Consumer Privacy Act and other state privacy laws and focus on providing actionable information to consumers, while avoiding placing a substantial burden on licensees with little corresponding benefit to consumers.

4. Exemptions from the right to deletion should be expanded to include additional important exemptions that broadly apply.

Subsection 6.C.(2) appropriately provides certain exceptions from a licensee's obligation to delete NPI in response to a consumer request, including where the licensee is required by law or regulation to retain the information. However, there are additional circumstances where it is important for licensees to be able to retain certain NPI that are not clearly covered by the existing exemptions. This provision should be clarified to permit licensees to retain and process information that is reasonably necessary for normal and expected internal operations and public interest purposes, including safety, security, and anti-fraud efforts. For example, we note that, prior to the point when a licensee reasonably anticipates a claim or civil or criminal proceeding, a licensee may need to maintain NPI for security and antifraud purposes. In the absence of such provisions, it is possible a bad actor may exploit the requirement to timely respond to requests under Section 6 to engage in fraudulent activity and seek to destroy the potential evidence thereof before the licensee is able to determine that a claim or civil or criminal proceeding might arise in connection with the NPI subject to the deletion request. Fraudsters are increasingly sophisticated in their efforts to exploit data privacy rights to facilitate their schemes, and robust exemptions for fraud prevention are essential to combat them and protect legitimate consumers. Accordingly, a broader list of exemptions should be added to broadly protect appropriate and necessary uses of NPI under a revised Model 672. This approach would be consistent with the approach and language adopted by most states that have adopted comprehensive privacy laws.

5. Data should not have to be deleted from backup systems until the backup system is restored to an active system or is next accessed in the ordinary course.

Subsection 6.C.(3) allows deletion to be delayed by up to 45 days where the data is stored on archived or backup systems. However, this 45-day limit does not account for the diverse technological and security architectures that licensees employ to protect consumer NPI or the disproportionate burden of responding to deletion requests with respect to backup or archive systems outside of the ordinary course of business. Some backup and archive systems (e.g. tape archives) are rarely accessed, and immutable backups (i.e., WORM compliant systems established to comply with SEC regulations) are by their nature designed so that they cannot be deleted as an important cybersecurity control.

Mandating deletion within a specified time period would require licensees to identify any backup or archive systems that may contain the consumer's NPI and access those systems solely for purposes of carrying out the deletion request. Not only would this add significant operational costs to licensees, but it could also increase the security risks to those backup systems by requiring that they be accessed more frequently and for different purposes than they would be accessed in the ordinary course. An essential feature of backup and archive systems is that they are appropriately segregated from production systems so that they are secure and available when production systems are lost or compromised. Immutable backups are particularly important as a defense against the risk of ransomware and similar destructive attacks, allowing the licensee to restore active systems after an attack. In recent years, insurance companies have increasingly been targeted by such attacks, and ransomware threats to the insurance sector continue to increase in both frequency and sophistication. In the absence of an exemption for these systems, the Act would essentially prohibit immutable backups, which would place both the licensee's business operations and the consumers' NPI at greater risk.

Subsection 6.C.(3) should therefore preserve immutable backups and other appropriately segregated backup systems by allowing licensees to defer deleting data from such a system until it is restored to an active system or next accessed in the ordinary course and deletion is reasonably feasible. Doing so would still protect consumers whose data is not deleted from such systems within 45 days of the authenticated request, since any access to the system would trigger the deletion obligation and would prevent any inadvertent use or disclosure of the NPI. This approach would better balance consumer privacy risk with licensees' cybersecurity risks and operational burdens and would be consistent with the approach taken by other privacy laws, including the California Consumer Privacy Act (CCPA).

6. Licensees should be exempted from honoring requests where doing so would involve disproportionate effort.

Subsection 6.D.(1)(b) includes an exemption that excuses licensees from responding to authorized consumer requests where the request cannot be fulfilled because the specific NPI is not locatable or retrievable by the licensee. The CAI appreciates and supports the recognition within this section that in some cases a licensee may be unable to locate or retrieve certain data after trying to honor the request, and the Working Group's revision removing the previously proposed "impossible" standard to qualify for this exception is a positive development. However, this subsection would still apparently require an affirmative determination that the NPI cannot be located or retrieved before the exemption would apply. We continue to believe there should be an express exception for circumstances where locating or retrieving such information would involve disproportionate effort (e.g., if honoring a consumer's request would require hundreds of hours of manually reviewing hardcopy documents or searching through legacy systems that were not designed with modern data retrieval capabilities). Other modern privacy frameworks, including the CCPA, allow businesses to decline to honor consumer requests where doing so would involve disproportionate effort. Implementing a similar standard here would better balance the interests of consumers in exercising their privacy rights with the potential practical difficulties of honoring those requests, and would ensure that licensees' resources are focused on honoring requests that can be meaningfully fulfilled. The CAI also recommends corresponding changes to the drafting note so that examiners are directed to review the licensee's justifications for denying a consumer request under the disproportionate effort standard, including the facts and circumstances supporting the determination.

In addition, the CAI recommends removing the language indicating that there shall be no cap on the number of requests to correct or delete NPI. Affirmatively specifying that there is no cap could inadvertently encourage repetitive and abusive requests, which would divert resources from responding to legitimate consumer requests. Therefore, if a cap is not adopted, the Model should remain silent on this point. This approach is consistent with state privacy laws, which generally do not affirmatively state that there is no limit on the number of requests.

7. Article IV's expanded notice requirements should be narrowed and clarified to avoid undue operational burdens.

Under the Full Exposure Draft, the distinction between a "consumer" and a "customer" has been eliminated and, as a result, the Model requires annual privacy notices to be provided to all consumers, including former customers and consumers who never become customers. Because the obligation to provide privacy notices is no longer tied to the formation of an ongoing customer relationship, this substantially increases the operational burden and costs on licensees in providing such notices.

Licensees are generally required to retain records of contacts with consumers for several years or may retain information on backup systems for security purposes and would therefore be obligated to provide annual privacy notices during that time even if the licensee does not use or disclose the consumer's NPI for any purpose other than to meet its legal obligations or for another permitted purpose under the Model. However, consumers that do not have an ongoing relationship with a licensee would not expect to continue receiving annual privacy notices and providing such notices may generate confusion or concern. For example, a consumer that applied for, but ultimately did not purchase, an insurance product may question why the licensee is continuing to send annual privacy notices years later. From the consumer's perspective, receiving annual privacy notices from a company with which they have no ongoing relationship may feel intrusive rather than protective and prompt unnecessary consumer inquiries or complaints. Where the consumer's NPI is retained solely to comply with a legal requirement or for a purpose otherwise expressly permitted under the Model (e.g. security or anti-fraud purposes), the licensee would also not be obligated to honor the consumer's request if the consumer submits a request for deletion in response to receiving an annual privacy notice.

Accordingly, the CAI recommends an express exception from the notice requirement be provided for consumers with whom the licensee has no ongoing relationship and where the NPI is retained solely to comply with a legal requirement or for another permitted purpose under the Model. This exception would reduce consumer confusion while appropriately focusing annual notice requirements on consumers who have a meaningful relationship with the licensee.

Additionally, Section 10 currently ties the short-form initial privacy notice to delivery of an opt-out notice. Because privacy notices are now required for all consumers, including those for whom no opt-out right would apply, it is important that Section 10 be revised to permit the use of the short-form notice broadly without necessarily requiring an accompanying opt-out notice. Enabling the use of the short-form notice also helps balance the burden placed on licensees to delivery notices to all consumers, not just those that become customers, with the interest of consumers in having access to information on how their NPI will be processed.

Finally, the elimination of the distinction between a "customer" and a "consumer" and the elimination of existing exemptions from the initial notice requirement for consumers in Section 5B of existing Model 672 has the effect of obligating a licensee to provide initial and annual notices to all consumers whose NPI the licensee received from another financial institution pursuant to a joint marketing agreement (e.g., a list of individuals to be jointly marketed to), even though the licensee's use of such consumers' NPI would be limited to the permitted purpose of conducting the joint marketing.

This result is entirely inconsistent with the nature and purpose of the joint marketing exemption and serves no practical consumer protection purpose. Requiring licensees to deliver initial and annual privacy notices to consumers on a joint marketing list – individuals who may have no awareness of or relationship with the licensee – would generate significant consumer confusion. Such notices would lack the context necessary for a consumer to understand how the licensee's information practices are meaningful to them. In addition to generating consumer confusion, this requirement would impose a substantial burden on licensees and impair insurers' ability to compete in the broader financial marketplace through joint marketing.

Accordingly, the CAI recommends a limited exemption from the requirement to provide initial and annual notices to consumers whose NPI the licensee received from a nonaffiliated third party pursuant to a joint marketing agreement, provided that the licensee provides the applicable notices when the consumer enters into an ongoing relationship (i.e., customer relationship) with the licensee and before the licensee discloses the consumer's NPI to a nonaffiliated third party other than as authorized by Sections 23 and 24. This approach would ensure that every consumer receives the full complement of initial and annual notices at the point when those notices are both relevant and actionable, while avoiding the delivery of notices that would confuse consumers and unduly burden licensees.

8. The prescribed time period for acting on an opt-out request should be extended and applied consistently.

Section 12 would require that licensees act on an opt-out request within 10 days of receipt. This directly conflicts with a parallel requirement in Section 19 which would require licensees to comply with a consumer's opt-out direction no later than 15 days after receipt. These provisions should be aligned with one another for the avoidance of doubt. Moreover, the prescribed time period should be extended to allow 30 days for compliance, which more appropriately reflects the operational realities of implementing opt-out requests across systems and use cases. If an opt-out request is received after a licensee has already begun disclosing a consumer's NPI to nonaffiliated third parties (i.e., after the consumer was given a reasonable opportunity to exercise the opt-out right as required by Section 12), the steps the licensee must take to comply with the opt-out request may require coordination across multiple systems, product lines, and third-party relationships. A 30-day compliance period would ensure that licensees can implement opt-out requests thoroughly and completely while still requiring prompt action for consumers.

9. Article V should be revised to establish a consistent framework for when disclosure of NPI to nonaffiliated third parties is permitted, subject to an opt-out right, requires opt-in consent, or is strictly prohibited.

Section 16A(3) of the Full Exposure Draft currently appears to broadly prohibit any disclosure of NPI not specifically accounted for in the Act. While the disclosure of NPI for purposes of targeted advertising is clearly subject to an out-out right and the sale of NPI or the disclosure of sensitive personal information (SPI) each clearly require opt-in consent, it is unclear what framework applies to other disclosures of NPI not captured in these categories. Importantly, Section 16 also does not account for the Article VI exceptions. The CAI recommends establishing a default framework providing an opt-out right for any disclosure of NPI that is not allowed under the Article VI exceptions and is not otherwise expressly addressed. Doing so would continue to put meaningful control in hands of consumers, while aligning with the tried and tested default applied to financial services broadly under the GLBA. Doing so would maintain parity of insurance within the broader financial services ecosystem, while still providing consumers enhanced protections for the most sensitive types of disclosure (sale and processing SPI).

It is additionally unclear how the opt-out right for targeted advertising under Section 19 is intended to fit within the broader framework of limits on the disclosure of NPI. We suggest that this requirement should be clearly articulated as an exception to the otherwise permitted disclosure of NPI to service providers and joint marketing. We believe this is, in fact, the intent of providing the opt-out requirement specifically for targeted advertising, and doing so would provide a powerful consumer right to limit how their data is used for cross-context behavioral advertising while preserving the broad ability of licensees to engage service providers and engage in joint marketing.

10. Section 17 should be revised to clarify how licensees who receive NPI from nonaffiliated third parties that are not service providers may use or disclose that NPI.

It is currently unclear what the revisions to Section 17 are intended to accomplish. Under existing Model 672, the equivalent section functions to define how a licensee who receives NPI under any exemption in Model 672 is permitted to further use or disclose that NPI. It generally allows them to use the NPI for exempted purposes (i.e. Article VI exempted purposes) or to disclose NPI in ways that the original disclosing financial institution would have been permitted to disclose the NPI directly.

Revised Section 17 does not carry out this same function. Rather, it would appear to only apply to NPI received pursuant to the exemptions defined in Sections 20 and 21 of revised Article V, but not the exemptions provided in Article VI. Additionally, it would appear to apply only to NPI received from nonaffiliated third-party service providers, but not necessarily other financial institutions who are not service providers (e.g. NPI disclosed from a ceding insurer to a reinsurer). As the CAI previously commented, these changes strip away the framework and structure of existing Model 672 without providing a replacement framework. This leaves non-service provider disclosures apparently subject only to the general rules articulated in Section 16, creating uncertainty about how licensees should handle NPI received from other financial institutions in the ordinary course of business and lacking necessary exemptions for the normal conduct of the business of insurance. Section 17 should be revised to apply to nonaffiliated third-party licensees regardless of whether they are service providers.

11. The definition of "third party" should be separated from the definition of "third party service provider."

The definition of "third party" has been bundled into the definition of "third party service provider." This converts references to a third party throughout the Act into references to a third-party service provider, even when the third party is clearly not a service provider. This would create numerous unintended consequences. The CAI recommends leaving "third party" undefined so that the Act can distinguish between nonaffiliated third parties generally and third-party service providers as the context requires.

12. The Article VI exceptions should apply to the proposed new opt-in requirements related to the disclosure of SPI.

As currently drafted, the Article VI exceptions would not apply to the proposed opt-in requirements in Article V. It is important that the exceptions to the opt-out requirements, which are well established and allow licensees to conduct normal operations, are equally applicable to the proposed opt-in requirements. While it appears the Working Group intended for the Article VI exceptions to apply to the limits on the use and disclosure of SPI under Section 21, which expressly cross-references to Article VI, that is not reflected in revised Article VI, which makes no reference to opt-in requirements whatsoever. Without an express reference to opt-in requirements, licensees would be unable to conduct ordinary insurance operations involving SPI without obtaining opt-in consent, such as disclosing SPI to a reinsurer or a third-party service provider. This ambiguity should be resolved by expressly applying the Article VI exceptions equally to both opt-out requirements and the opt-in requirements under Section 21.

* * *

As the Working Group continues work on the revised Model, we urge the Working Group to keep an eye toward ensuring that the revised draft ultimately provides clear and understandable standards that work as a whole and that any changes – particularly to the defined terms or to the structure of the Model – do not inadvertently disrupt other sections of the revised Model. We recognize that this is a complex and painstaking process, but the CAI remains committed to working constructively with the Working Group to develop a final Model that enhances consumer privacy protections while preserving the ability of annuity insurers to compete fairly in the marketplace and serve consumers' retirement needs.

We again want to express our appreciation for the opportunity to comment on the Full Exposure Draft. We hope that you find these comments and the attached annotated markup helpful. Please do not hesitate to contact us if you have any questions.

Respectfully submitted,

Eversheds Sutherland (US) LLP

For The Committee of Annuity Insurers

Eversheds Sutherland (US) LLP

Please direct any questions or requests regarding this letter to any of the following:

Stephen E. Roth
Partner
Eversheds Sutherland (US) LLP
SteveRoth@eversheds-sutherland.us
202.383.0158

Alexander F. L. Sand
Partner
Eversheds Sutherland (US) LLP
AlexanderF.L.Sand@eversheds-sutherland.us
512.721.2721

Mary Jane Wilson-Bilik
Partner
Eversheds Sutherland (US) LLP
MJWilson-Bilik@eversheds-sutherland.us
202.383.0660

PRIVACY OF CONSUMER INFORMATION ACT

Table of Contents

ARTICLE I. GENERAL PROVISIONS

Section 1. Purpose
Section 2. Scope and Compliance
Section 3. Rule of Construction
Section 4. Definitions

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Section 5. Third-Party Service Provider Arrangements

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7. Initial and Subsequent Delivery Notice of Information Practices to Consumers Required
Section 8. Annual Notice of Information Practices to Consumers Required
Section 9. Information to be Included in Notices of Information Practices
Section 10. Short Form Initial Notice of Information Practices
Section 11. Form of Opt-In Notice to Consumers and Opt-In Methods
Section 12. Form of Opt-Out Notice to Consumers and Opt-Out Methods
Section 13. Revised Notice of Information Practices
Section 14. Notice of Information Practices to Group Policyholders
Section 15. Delivery

ARTICLE V. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 16. General Rules for Use and Disclosure of Nonpublic Personal ~~InformationSection~~ Information
Section 17. Limits on Redisclosure and Reuse of Nonpublic Personal Information
Section 18. Limits on Sharing Access Number or Access Code Information for Marketing Purposes
Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted Advertising
Section 20. Limits on Sale of Nonpublic Personal Information
Section 21. Limits on Disclosure of Sensitive Personal Information

© 2026 National Association of Insurance Commissioners

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 22. Exception to Opt Out Requirements for Disclosure of Nonpublic Personal Information for Service Providers and Joint Marketing
Section 23. Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Information for Processing and Servicing Transactions
Section 24. Other Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Information

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 25. When Authorization Required for Disclosure of Nonpublic Personal Health Information
Section 26. Authorizations
Section 27 Authorization Request Delivery
Section 28. Relationship to Federal Rules
Section 29. Relationship to State Laws

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 30. Protection of Fair Credit Reporting Act
Section 31. Nondiscrimination
Section 32. Violation
Section 33. Severability
Section 34. Individual Remedies
Section 35. Effective Date

APPENDICES

Appendix A Sample Clauses
Appendix B Federal Model Privacy Form
Model Law Forms

© 2026 National Association of Insurance Commissioners

ARTICLE I. GENERAL PROVISIONS

Section 1. Purpose

Purpose. This Act governs the treatment of nonpublic personal health information and nonpublic personal information about individuals by all licensees of the state insurance department. This Act:

A. Requires a licensee to provide notice to individuals about its privacy policies and practices;

B. Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal information about individuals to affiliates and nonaffiliated third parties; and

C. Provides methods for individuals to prevent a licensee from disclosing that information.

Drafting Note: Whether this model is adopted as an Act or Regulation will depend upon individual state law. If a state adopts the model as an Act, reference to the model as an Act should be updated throughout the model.

Section 2. Scope and Compliance

A. Scope. This Act applies to:

(1) Nonpublic personal information about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. This Act does not apply to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes; and

(2) All nonpublic personal health information.

B. Compliance. A licensee domiciled in this state that is in compliance with this Act in a state that has not enacted laws or regulations that meet the requirements of Title V of the Gramm-Leach-Bliley Act (PL 102-106) may nonetheless be deemed to be in compliance with Title V of the Gramm-Leach-Bliley Act in the other state.

Drafting Note: Subsection B is intended to give licensees some guidance for complying with Title V of the Gramm-Leach-Bliley Act in those states that do not have laws or regulations that meet GLBA's privacy requirements.

© 2026 National Association of Insurance Commissioners

Section 3. Rule of Construction

The examples in this Act, the sample clauses in Appendix A, and the Federal Model Privacy Form in Appendix B of this Act are not exclusive. Compliance with an example, use of a sample clause, or the Federal Privacy Model Form, to the extent applicable, constitutes compliance with this Act.

Licensees may rely on use of the Federal Privacy Form in Appendix B, consistent with the attached instructions, as a safe harbor of compliance with the Notice of Information Practices content requirements of this Act.

Use of the Federal Model Privacy Form is not required. Licensees may continue to use other types of privacy notices, including notices that contain the examples in this Act and/or the sample clauses in Appendix A, provided that such notices accurately describe the Licensee's privacy practices and otherwise meet the notice content requirements of this Act.

Section 4. Definitions

As used in this Act, unless the context requires otherwise:

A. "Affiliate" means a company that controls, is controlled by or is under common control with another company.

B. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

C. (1) "Clear and conspicuous" means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) Examples.

(a) Reasonably understandable. A licensee makes its notice reasonably understandable if it:

(i) Presents the information in the notice in clear, concise sentences, paragraphs and sections;

(ii) Uses short explanatory sentences or bullet lists whenever possible;

(iii) Uses definite, concrete, everyday words and active voice whenever possible;

(iv) Avoids multiple negatives;

(v) Avoids legal and highly technical business terminology whenever possible; and

(vi) Avoids explanations that are imprecise and readily subject to different interpretations.

© 2026 National Association of Insurance Commissioners

(b) Designed to call attention. A licensee designs its notice to call attention to the nature and significance of the information in it if the licensee:

(i) Uses a plain-language heading to call attention to the notice;

(ii) Uses a typeface and type size that are easy to read;

(iii) Provides wide margins and ample line spacing;

(iv) Uses boldface or italics for key words; and

(v) In a form that combines the licensee's notice with other information, uses distinctive type size, style, and graphic devices, such as shading or sidebars.

(c) Notices on web sites. If a licensee provides a notice on a web page, the licensee designs its notice to call attention to the nature and significance of the information in it if the licensee uses text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks or sound) do not distract attention from the notice, and the licensee either:

(i) Places the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(ii) Places a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

D. "Collect" means to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

E. "Commissioner" means the chief insurance regulatory official of the state.

Drafting Note: Use the title of the chief insurance regulatory official wherever the term "commissioner" appears. If the jurisdiction of certain health licensees, such as health maintenance organizations, lies with some state agency other than the insurance department, or if there is dual regulation, a state should add language referencing that agency to ensure the appropriate coordination of responsibilities.

F. "Company" means a corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.

G. (1) "Consumer" means an individual who seeks to obtain, obtains or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, and about whom the licensee has nonpublic personal information, or that individual's legal representative.

© 2026 National Association of Insurance Commissioners

(2) Examples.

(a) An individual who provides nonpublic personal information to a licensee in connection with obtaining or seeking to obtain financial, investment or economic advisory services relating to an insurance product or service is a consumer regardless of whether the licensee establishes an ongoing advisory relationship.

(b) An applicant for insurance prior to the inception of insurance coverage is a licensee's consumer.

(c) An individual who is a consumer of another financial institution is not a licensee's consumer solely because the licensee is acting as agent for, or provides processing or other services to, that financial institution.

(d) An individual is a licensee's consumer if:

(i) (I) The individual is a beneficiary of a life insurance policy underwritten by the licensee;

(II) The individual is a claimant under an insurance policy issued by the licensee;

(III) The individual is an insured or an annuitant under an insurance policy or an annuity, respectively, issued by the licensee; or

(IV) The individual is a mortgagor of a mortgage covered under a mortgage insurance policy; and

(ii) The licensee discloses nonpublic personal information about the individual to a nonaffiliated third party other than as permitted under Sections 22, 23, and 24 of this Act.

(e) Provided that the licensee provides the initial, annual and revised notices under Sections 7, 8, and 13 of this Act to the plan sponsor, group or blanket insurance policyholder or group annuity contractholder, or workers' compensation policyholder, and further provided that the licensee does not disclose to a nonaffiliated third party nonpublic personal ~~financial~~ information about an individual described in Item (i), (ii) or (iii), other than as permitted under Sections 22, 23, or 24 of this Act, such an individual is not the consumer of the licensee solely because he or she is:

Commented [ES1]: Corrected apparent typo - the term "nonpublic personal financial information" has been replaced with "nonpublic personal information" in all other instances throughout the draft.

(i) A participant or a beneficiary of an employee benefit plan that the licensee administers or sponsors or for which the licensee acts as a trustee, insurer or fiduciary;

(ii) Covered under a group or blanket insurance policy or group annuity contract issued by the licensee; or

(iii) A claimant covered by a workers' compensation plan.

© 2026 National Association of Insurance Commissioners

Drafting Note: In states where the workers' compensation self-insurance or workers' compensation state fund coverage is outside the commissioner's jurisdiction, regulators may wish to urge the applicable agency or agencies to promulgate a regulation similar to this Act in order to ensure parity in treatment of workers' compensation plans and to ensure that all workers covered by such plans have privacy protections.

(f) (i) The individuals described in Subparagraph (e)(i) through (iii) of this paragraph are consumers of a licensee if the licensee does not meet all the conditions of Subparagraph (e).

(ii) In no event shall the individuals, solely by virtue of the status described in Subparagraph (e)(i) through (iii) above, be deemed to be consumers for purposes of this Act.

Commented [ES2]: As revised, these provisions directly conflict with one another. Originally, paragraph (ii) was intended to prevent a consumer covered under paragraph (i) from being considered a customer. This needs to be clarified.

(g) An individual is not a licensee's consumer solely because he or she is a beneficiary of a trust for which the licensee is a trustee.

(h) An individual is not a licensee's consumer solely because he or she has designated the licensee as trustee for a trust.

H. "Consumer reporting agency" has the same meaning as in Section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

I. "Control" means:

(1) Ownership, control or power to vote twenty-five percent (25%) or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

(2) Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or

(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the commissioner determines.

J. "De-identified data" means information that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual.

K. (1) "Financial institution" means any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 1843(k)(4)(B**)** of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial institution does not include:

(a) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 *et seq.*);

(b) The Federal Agricultural Mortgage Corporation or any entity charged and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*); or

© 2026 National Association of Insurance Commissioners

(c) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as the institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

L. (1) "Financial product or service" means a product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 1843(k)(4)(B**)** of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.

~~M~~M. "Genetic information" means any data, regardless of format, that: (1) results from the analysis of an individual's biological material, including analysis of the complete DNA, regions of DNA, chromosomes, genes, or gene products; and (2) concerns an individual's genetic characteristics. "Genetic information" does not include de-identified data.

Commented [ES3]: The term "genetic information" was included in the definition of "sensitive personal information" but was not, itself, defined. In order to clarify the scope of "sensitive personal information," the CAI proposes this definition, which we note is consistent with the definition used in the privacy laws of Indiana, Connecticut, and other states.

N. "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.

~~N~~O. (1) "Licensee" means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Insurance Law of this state, [and health maintenance organizations holding a certificate of authority pursuant to Section [insert section] of this state's Public Health Law].

Drafting Note: Add bracketed language if HMOs are licensed under other than insurance statutes and cite appropriate state law.

(2) A licensee is not subject to the notice, opt in and opt out requirements for nonpublic personal information set forth in Articles I, II, III and IV of this Act if the licensee is an employee, agent or other representative of another licensee ("the principal") and:

Commented [ES4]: It is important that these exemptions extend to opt in requirements, not just notice and opt out requirements. We believe this was an inadvertent omission.

~~(a)~~ ~~The~~(a) To the best of the licensee's knowledge, the principal otherwise complies with, and provides the notices required by, the provisions of this Act; and

Commented [ES5]: We note that a licensee should not be made subject to the notice and opt out requirements by virtue of the principal's failure to comply with and provide notices under the Act if it reasonably believed the principal was in compliance and had provided such notices.

(b) The licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates in a manner permitted by this Act.

(3) (a) Subject to Subparagraph (b), "licensee" shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only in regard to the excess lines placements placed pursuant to Section [insert section] of this state's laws.

(b) An excess lines broker or excess lines insurer shall be deemed to be in compliance with the notice and opt out requirements for nonpublic personal information set forth in Articles I, II, III and IV of this Act provided:

© 2026 National Association of Insurance Commissioners

(i) The broker or insurer does not disclose nonpublic personal information of a consumer to nonaffiliated third parties for any purpose, including joint servicing or marketing under Section 22 of this Act, except as permitted by Section 23 or 24 of this Act; and

(ii) The broker or insurer delivers a notice to the consumer at the time a consumer relationship is established on which the following is printed in 16-point type:

NOTICE OF INFORMATION PRACTICES
"Neither the U.S. brokers that handled this insurance nor the insurers that have underwritten this insurance will disclose nonpublic personal information concerning the buyer to nonaffiliates of the brokers or insurers except as permitted by law."

Drafting Note: References to "excess lines broker" and "excess lines insurer" should be changed as necessary to correspond with the applicable terms used in each state.

~~O~~P. (1) "Nonaffiliated third party" means any person except:

(a) A licensee's affiliate; or

(b) A person employed jointly by a licensee and any company that is not the licensee's affiliate (but nonaffiliated third party includes the other company that jointly employs the person).

(2) Nonaffiliated third party includes any company that is an affiliate solely by virtue of the direct or indirect ownership or control of the company by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

~~P~~Q. "Nonpublic personal health information" means any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of an individual;

(2) The provision of health care to an individual; or

(3) Payment for the provision of health care to an individual.

~~Q~~R. "Nonpublic personal information" means any personally identifiable information that is linked or reasonably linkable to an identified natural person. Nonpublic personal information does not include de-identified data or publicly available information.

© 2026 National Association of Insurance Commissioners

~~R~~S. (1) "Personally identifiable information" means any information:

(a) A consumer provides to a licensee to obtain an insurance product or service from the licensee;

(b) About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

(c) The licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.

(2) Examples.

(a) Information included. Personally identifiable information includes:

(i) Information a consumer provides to a licensee on an application to obtain an insurance product or service;

(ii) Account balance information and payment history;

(iii) The fact that an individual is or has been one of the licensee's consumers or has obtained an insurance product or service from the licensee;

(iv) Any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer;

(v) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;

(vi) Any information the licensee collects through an Internet cookie (an information-collecting device from a web server); and

(vii) Information from a consumer report.

(b) Information not included. Personally identifiable information does not include:

(i) A list of names and addresses of customers of an entity that is not a financial institution; and

(ii) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.

~~S~~T. "Opt in" means an affirmative direction by a consumer that authorizes a licensee to disclose the consumer's information.

~~T~~U. "Opt out" means a direction by a consumer that the licensee may not disclose nonpublic personal information about the consumer to a nonaffiliated third party, except as permitted under Sections 22, 23,

© 2026 National Association of Insurance Commissioners

or 24.

~~U~~V. (1) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

(a) Federal, state or local government records;

(b) Widely distributed media; or

(c) Disclosures to the general public that are required to be made by federal, state or local law.

(2) Reasonable basis. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

(a) That the information is of the type that is available to the general public; and

(b) Whether an individual can direct that the information not be made available to the general public and, if so, that the licensee's consumer has not done so.

(3) Examples.

(a) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(b) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(c) Reasonable basis.

(i) A licensee has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(ii) A licensee has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the licensee has located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

~~V~~W. "Reasonable opportunity" means any of the following:

(1) The licensee mails the notices required to the consumer and allows the consumer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within sixty (60) days from the date the licensee mailed the notices;

© 2026 National Association of Insurance Commissioners

(2) Where a consumer agrees to receive the notices required by this Act electronically in accordance with UETA [insert state electronic transactions act statute], the licensee allows the consumer to opt out by any reasonable means at any time; or

(3) For an isolated transaction, such as providing the consumer with an insurance quote, the licensee provides the notices required by this Act at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction.

X. "Sale" or "selling" means the exchange of nonpublic personal information with a nonaffiliated third party for monetary or other valuable consideration. A licensee does not sell nonpublic personal information when:

(1) The disclosure is to a third party for the purpose of or in support of providing a product or service requested by the consumer.

(2) A licensee provides information to or receives anything of value from an insurance support organization, statistical agent, or reinsurer;

(3) A licensee provides nonpublic personal information to ~~an affiliate or to a financial institution~~nonaffiliated third party with which the licensee performs joint marketing;

(4) The business transfers to a third party the nonpublic personal information as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction in which the party assumes control of all or part of the licensee's assets; or

(5) A consumer uses or directs the business to (i) disclose nonpublic personal information; or (ii) interact with one or more third parties including but not limited to referrals to other licensees.

Y. "Sensitive Personal Information" means ~~personally identifiable~~ "nonpublic personal information" about a consumer that includes:

(1) Racial or ethnic origin, religious beliefs, sexual orientation, or citizenship or citizenship status; or

(2) Genetic information ~~or~~and biometric data that ~~may be~~is processed for the purpose of uniquely identifying an individual.

Z. (1) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on nonpublic personal ~~data~~information obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests.

(2) "Targeted advertising" does not include:

(a) Online advertisements based on activities within a Licensee's own websites or

Commented [ES6]: The definition of "sale" or "selling" should be clarified to exclude affiliates. Without this clarification, affiliates may share information systems or otherwise have access to nonpublic personal information in a way that may be viewed as involving monetary or other valuable consideration.

Commented [ES7]: This language suggests that joint marketing limitations apply to marketing with affiliates, however the joint marketing provision (Section 22) only applies to disclosures of information with nonaffiliated third parties. This should be clarified.

Commented [ES8]: "Personally identifiable" is included in the definition of "nonpublic personal information" and therefore this language is duplicative and should be deleted.

Commented [ES9]: Consistent with the recommendation to define the term "genetic information," we recommend changing "or" to "and."

Commented [ES10]: Updated for consistency with the definition of the term "biometric data," which only includes such data that is "used to identify a specific individual." The term "may" implies a deviation from that definition for purposes of "sensitive personal information" which does not appear to be intentional.

Commented [ES11]: The term "personal data" is not defined, which raises questions regarding the scope of "targeted advertising." In keeping with the scope of the Act as described in Section 2, we recommend using the defined term "nonpublic personal information" here.

© 2026 National Association of Insurance Commissioners

online applications;

(b) Online advertisements based on the context of a consumer's current search query, visit to a website, or online application;

(c) Online advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(d) Processing Nonpublic Personal Information solely for measuring or reporting advertising performance, reach, or frequency.

AA. "Third party service provider" ~~or "third party"~~ means a person or entity not otherwise defined as a licensee or affiliate of a licensee that:

(1) Provides services to the licensee; and

(2) Maintains, processes or otherwise is permitted access to nonpublic personal information through its provisions of services to the licensee.

Commented [ES12]: Providing that the term "third party" has the same meaning as the term "third party service provider" essentially results in all references to third parties throughout the Act referring exclusively to service providers and leaves no means of describing third parties that are not service providers. This creates a range of confusing and, we believe, unintentional outcomes.

© 2026 National Association of Insurance Commissioners

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Section 5. Third-Party Service Provider Arrangements

A. Contract Requirements.

A licensee that discloses a consumer's nonpublic personal information to a third-party service provider shall enter into a written contract with the third-party service provider that:

(1) Prohibits the third-party service provider from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, including use under an exception in Sections 23 or 24 in the ordinary course of business to carry out those purposes, unless processing is necessary to comply with the law or a ~~valid and binding order of~~ lawful request by law enforcement or a governmental body, in which case the third-party service provider must notify the licensee within 48 hours unless prohibited by law;

(2) Requires the third-party service provider to delete, destroy, de-identify or return all nonpublic personal information to the licensee when requested by the licensee; or to delete nonpublic personal information after it is no longer necessary to fulfill a legal requirement or to meet the record retention requirements of the licensee or third-party service provider, and to notify the licensee of the action taken;

(3) Requires the third-party service provider to notify the licensee if it can no longer comply with its obligations under this contract and provides the licensee with a right to terminate the contract;

(4) Requires that any contract between a third-party service provider and a subcontractor with access to a consumer's nonpublic personal information must contain provisions no less protective of nonpublic personal information than those contained in the third-party service provider's agreement with the licensee;

(5) Requires the third-party service provider to provide assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act;

(6) Requires the third-party service provider to implement and maintain administrative, technical, and physical data security practices to protect the nonpublic personal information from unauthorized access, destruction, use, modification, or disclosure;

(7) Requires the third-party service provider to notify the licensee of a failure to meet the obligations of Subsections (1) to (6) above ~~within 48 hours of~~promptly after discovery by the third-party service provider.

B. A licensee that discloses a consumer's nonpublic personal information to a third-party service provider remains fully responsible for compliance with this Act and the handling of such nonpublic personal information.

Commented [ES13]: As discussed in CAI Comment #2, this section is duplicative and confusing in connection with Section 22A. Our changes are intended to align the two sections. See corresponding suggested edits in Section 22.

Commented [ES14]: The Working Group should consider providing more flexibility for third party service providers to respond to lawful requests by law enforcement or a governmental body without necessarily requiring a valid and binding order.

Commented [ES15]: The Working Group should consider adopting a less prescriptive standard for the timing of notification. For example, if a service provider refuses to commit to anything less than 72 hours (a common industry benchmark), that should not lead to a violation of this Section 5.

Commented [ES16]: This change is intended to clarify that the responsibility for handling nonpublic personal information specifically relates to nonpublic personal information disclosed to the third party service provider by the licensee.

© 2026 National Association of Insurance Commissioners

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

A. A consumer may file the following requests with a licensee, which shall be processed in accordance with the following standards:

(1) Within 45 days of receiving an authenticated request from a consumer for their nonpublic personal information, a licensee shall disclose:

(a) All nonpublic personal information about the consumer that is maintained by the licensee or any contracted third-party service provider; and

(b) A list of ~~all~~the categories of nonaffiliated third ~~party service providers~~ parties to whom the licensee disclosed the consumer's nonpublic personal information in the preceding 12 months.

(2) A licensee shall not be required to disclose the following:

(a) A consumer's Social Security Number, driver's license number or other government-issued identification number, financial account number(s), any health insurance or medical identification number, any account password(s), security questions and answers, genetic information, unique biometric data or other information that could create a high risk of identity theft. The licensee may instead disclose the types of nonpublic personal information maintained by listing each type of nonpublic personal information it has about the consumer;

(b) Duplicative nonpublic personal information that has already been disclosed in response to the consumer's request, if it is described in a manner reasonably understandable by the consumer and the ~~consumer is offered an opportunity~~licensee takes reasonable steps to ~~review~~ensure the duplicative nonpublic personal information ~~for inconsistencies~~is consistent with disclosed nonpublic personal information; or

(c) Information that is outside the scope of the request, if the consumer has requested only specified items or categories of information.

B. Correction of nonpublic personal information.

(1) A consumer may make an authenticated request for the correction of their nonpublic personal information by filing a request with the licensee that:

(a) Identifies the specific nonpublic personal information the consumer wishes to correct; and

(b) Provides an explanation of why the nonpublic personal information is incorrect.

(2) Within 45 days of receipt of the request under this subsection, a licensee shall take one of the following actions and notify the consumer:

Commented [ES17]: As discussed in CAI Comment #3, it would be very difficult to track all third party service providers with whom a particular individual's information has been disclosed, and it is unclear what value this information would provides to consumers, considering they cannot opt out of information sharing with third party service providers pursuant so Section 22. It is also important this requirement be bounded to a reasonable time frame, such as in the past 12 months.

Commented [ES18]: Although genetic information would likely fall within the scope of "other information that could create a high risk of identity theft," we recommend expressly including it in the list of types of nonpublic personal information exempted from disclosure, given the high risk of identity theft inherent to genetic information.

Commented [ES19]: Revised to clarify that "duplicative nonpublic personal information" refers to information that may be stored in multiple instances, one instance of which has already been disclosed in response to the consumer's request. In addition, this subsection implies that consumers have a secondary right to further have the duplicative information provided, which appears to negate the purpose of the exception for duplicative nonpublic personal information. Rather than providing secondary disclosure rights to duplicative information, we recommend that the exception require the licensee to take reasonable steps to ensure sets of duplicative nonpublic personal information are consistent with one another.

© 2026 National Association of Insurance Commissioners

(a) Correct the nonpublic personal information in dispute as requested by the consumer;

(b) Delete the nonpublic personal information in dispute; or

(c) Deny the request and provide:

(i) The basis for refusal to correct the nonpublic personal information as requested;

(ii) Information about how the consumer may appeal the denial; and

(iii) An explanation of how the appeal will be reviewed and how the consumer will be notified of the decision on appeal.

(3) A licensee may deny a request for correction if:

(a) ~~The~~The licensee reasonably determines that the nonpublic personal information is accurate and complete and ~~if the licensee~~ provides a process for appeal of the decision; or

(b) The nonpublic personal information that is the subject of the request was not created by the licensee, unless there is a reasonable basis to believe that the originator of the nonpublic personal information is no longer available to act on the requested correction, and the consumer has independently demonstrated the information is incorrect.

C. Deletion of nonpublic personal information.

(1) Within 45 days of an authenticated request from a consumer, a licensee shall delete the nonpublic personal information about the consumer that is maintained by the licensee or direct a third-party service provider to delete the nonpublic personal information on the licensee's behalf.

(2) The licensee is not required to delete nonpublic personal information if:

(a) The licensee is required by law or regulation to retain the nonpublic personal information;

(b) The nonpublic personal information may be necessary to perform the contract or service requested by or benefiting the consumer;

(c) The nonpublic personal information is necessary to comply with a legal obligation; ~~or~~

(d) The nonpublic personal information is maintained in reasonable anticipation of a claim or civil or criminal proceeding~~.~~;

(e) The nonpublic personal information is maintained for purposes reasonably related to the prevention, detection, protection against, or response to security

Commented [ES20]: This provision should allow for a licensee's reasonable determination that the nonpublic personal information is accurate and complete, rather than whether such information is actually accurate.

Commented [ES21]: Replaced "information" with "nonpublic personal information" for consistency.

© 2026 National Association of Insurance Commissioners

incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity; or

(f) The nonpublic personal information is maintained to the extent it may be necessary to preserve the integrity or security of systems or to investigate, report, or prosecute those responsible for breaches of system security.

(3) A licensee may delay fulfilling a consumer's request~~, up to 45 days,~~ to delete nonpublic personal information stored on an archived or backup system~~. A licensee must notify the consumer of such delay.~~ until that system is restored to an active system or is next accessed in the ordinary course and targeted deletion on the backup system is reasonably feasible, whichever occurs first.

D. Request and Response Procedures

(1) Except as provided in Subsection D(1)(b), a licensee shall respond to requests submitted under this section within 45 days in the following manner:

(a) A licensee may use its secure communications portal to authenticate requests from consumers holding current accounts with the licensee, unless the licensee has reason to believe the request has been submitted through an account that has been compromised. Otherwise, the licensee may use methods that are commercially reasonable, but not unduly burdensome, to authenticate the identity of the person making the request and to verify that this person is either:

(i) The consumer;

(ii) A person acting with the consumer's written authorization, including but not limited to a valid power of attorney;

(iii) The parent or legal guardian of a consumer who is a minor, except where the information relates to health insurance claims in circumstances where the child has a legal right to obtain the services in question without the parent's or guardian's consent;

(iv) The legal guardian or other person authorized by law to act on behalf of an incapacitated consumer; or

(v) The personal representative or other person authorized by law to act on behalf of a deceased consumer.

(b) A licensee is required to notify the consumer if either of the following prevents the licensee from complying with the request:

(i) The specific nonpublic personal information at issue is not locatable or retrievable by the licensee or doing so would involve disproportionate effort; or

Drafting Note: Examiners should review licensees' notifications to consumers regarding nonpublic personal information that is not locatable or retrievable by the licensee and its justifications for ~~irretrievability~~denying a

Commented [ES22]: As discussed in CAI Comment #4, additional important exemptions to the right to deletion should apply, particularly to safeguard necessary security and antifraud purposes.

Commented [ES23]: As discussed in CAI Comment #5, it is crucial that there be an allowance for deletion from backup systems that is not time-specific and limited where deletion is not feasible. Immutable backups are designed so that they cannot be deleted as an important cybersecurity control, and other backup or archive systems are so rarely accessed that the burden of doing so solely to delete a consumer's nonpublic personal information would outweigh the benefit of having such data deleted on the backup system while exposing the backup system to elevated cybersecurity risks.

Commented [ES24]: As discussed in CAI Comment #6, although we appreciate the revision removing the "impossible" standard, we note that this provision may still be read as requiring an affirmative determination that the nonpublic personal information at issue cannot be located or retrieved. We continue to believe allowance should be made for circumstances where locating or retrieving such information would involve disproportionate effort (e.g., if honoring a consumer request would require hundreds of hours of manually reviewing hardcopy documents). We have also made a corresponding change to the drafting note encouraging examiners to review the licensee's justifications for denying a request.

© 2026 National Association of Insurance Commissioners

consumer request under this Subsection D(1)(b)(i) during Market Conduct and/or IT Exams.

(ii) The licensee is unable to verify the request after requesting that the consumer provide additional information necessary to authenticate the identity of the consumer and authenticate the consumer's request.

(c) If a licensee declines the consumer's request, the licensee shall inform the consumer of the basis for declining the request and provide instructions for how to request review of the decision.

~~(2) There shall be no cap on the number of requests to correct or delete nonpublic personal information.~~

~~(3~~(2) If a consumer disagrees with a licensee's refusal to correct ~~or delete~~ nonpublic personal information per the consumer's request, the consumer shall be permitted to file with the licensee:

(a) A concise statement setting forth why the consumer disagrees with the licensee's refusal and what the consumer thinks is the correct, relevant or fair information; and

(b) The licensee shall maintain the statement with the disputed nonpublic personal information and allow anyone reviewing the disputed nonpublic personal information to be made aware of the dispute and have access to the consumer's statement.

Commented [ES25]: It does not appear necessary to expressly state that there is no cap on the number of requests that may be made. Moreover, including this provision may inadvertently encourage repetitive and abusive requests.

Commented [ES26]: We note that filing a statement of disagreement is only relevant to correction requests, as the statement of disagreement provides the consumer with the opportunity to assert the information the consumer believes to be correct, relevant or fair. Accordingly, this provision should not be extended to deletion requests.

© 2026 National Association of Insurance Commissioners

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7. Initial and Subsequent Delivery Notice of Information Practices to Consumers Required

A. Initial Delivery of Notice. A licensee shall provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to all consumers no later than when the licensee obtains access to the consumer's nonpublic personal information, except that a licensee may provide the initial notice within a reasonable time after access to the consumer's nonpublic personal information if:

(1) Obtaining access to the consumer's nonpublic personal information is not at the consumer's election and the licensee follows the Notice of Information Practices previously sent to the consumer; or

(2) Providing notice when the licensee obtains access to the consumer's nonpublic personal information would substantially delay the consumer's transaction and the consumer agrees to receive the notice at a later time.

B. Subsequent Delivery of Notice

When a consumer with an existing relationship with a licensee obtains a new insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, the licensee satisfies the initial notice requirements of Subsection A of this section as follows:

(1) The licensee may provide a revised notice, under Section 13, that covers the consumer's new insurance product or service; or

(2) If the initial, revised or annual notice that the licensee most recently provided to that consumer was accurate with respect to the new insurance product or service, the licensee does not need to provide a new notice of information practices under Subsection A of this section.

C. For purposes of this section:

(1) "Not at consumer's election" includes the scenario where a licensee acquires or is assigned a consumer's policy from another financial institution or residual market mechanism and the consumer does not have a choice about the licensee's acquisition or assignment.

(2) "Substantially delay the consumer's transaction" includes the scenario where the licensee and the individual agree over the telephone or electronically to enter into a consumer relationship involving prompt delivery of the insurance product or service but does not include the scenario where the relationship is initiated in person at the licensee's office or through other means by which the consumer may view the notice, such as on a website.

D.

Section 8. Annual Notice of Information Practices to Consumers Required

© 2026 National Association of Insurance Commissioners

A. General rule. A licensee shall provide a clear and conspicuous notice to consumers that accurately reflects its privacy policies and practices at least once in any period of twelve (12) consecutive months. A licensee may define the twelve-consecutive-month period, but the licensee shall apply it to the consumer on a consistent basis.

~~A.~~ Example. A licensee provides a notice annually if it defines the twelve-consecutive-month period as a calendar year and provides the annual notice to the consumer once in each calendar year following the calendar year in which the licensee provided the initial notice. For example, if a consumer opens an account on any day of year 1, the licensee shall provide an annual notice to that consumer by December 31 of year 2.

B. Exceptions.

(1) A licensee that provides nonpublic personal information to nonaffiliated third parties only in accordance with Sections 22, 23, or 24 and has not changed its policies and practices with regard to disclosing ~~Nonpublic Personal Information~~nonpublic personal information from the policies and practices that were disclosed in the most recent disclosure sent to consumers in accordance with this section or ~~Section~~Sections 7 or 13 shall not be required to provide an annual disclosure under this section until such time as the licensee fails to comply with any criteria described in this paragraph.

(2) A licensee is not required to provide notice if the licensee no longer has access to the consumer's nonpublic personal information.

~~(2)~~(3) For the purposes of this Act, a licensee no longer has an obligation to continue to notify a consumer if the licensee's records do not contain a valid address. An address is deemed invalid if electronic or regular mail sent to that address by the licensee has been returned as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.

(4) A licensee is not required to provide notice to consumers with whom the licensee has no ongoing relationship, provided the licensee retains the consumer's nonpublic personal information solely to comply with a legal requirement or for purposes otherwise specifically permitted by this Act, including for security and anti-fraud purposes.

Section 9. Information to be Included in Notices of Information Practices

A. General rule. The initial, annual and revised Notice of Information Practices that a licensee provides under Sections 7, 8, and 13 shall include each of the following items of information, in addition to any other information the licensee wishes to provide, that applies to the licensee and to the consumers to whom the licensee sends its Notice of Information Practices:

(1) The categories of nonpublic personal information that the licensee collects, including, but not limited to, whether information is collected from the consumer, through the consumer's transactions with affiliates or nonaffiliated third parties, or consumer reporting agencies;

Commented [ES27]: Established the general rule as Subsection "A" for consistency with the structure of other sections of the Act.

Commented [ES28]: Converted to lowercase for consistency.

Commented [ES29]: It appears the revised notice of information practices under Section 13 was inadvertently omitted here.

Commented [ES30]: Corrected numbering.

Commented [ES31]: The CAI strongly urges the PPWG to adopt a limited exception to the annual notice requirement. The shift to the term "consumer" has significantly expanded the scope of this requirement without providing exceptions for circumstances where there is little value in providing an annual notice. A licensee should not be required to provide an annual notice to a consumer whose nonpublic personal information is retained only to comply with legal obligation, such as where the consumer made inquiries but never purchased a financial product or service and has no other connection to or engagement with the licensee. Additionally, notice should not be required where data is retained solely for expressly permitted uses, such as security and anti-fraud purposes.

© 2026 National Association of Insurance Commissioners

(2) The categories of nonpublic personal information that the licensee discloses~~,~~ to entities described in Subsection (A)(3), including at least one example in each category. Categories may include, but are not limited to, application information, transaction information, or consumer reports;

(3) The categories of affiliates and nonaffiliated third parties, and the types of business in which they engage, to whom the licensee discloses nonpublic personal information, other than those parties to whom the licensee discloses information under Sections 22, 23, and 24. The types of businesses may be described in general terms only if the licensee uses illustrative examples of each significant line of business;

(4) An explanation of the consumer's right under ~~Section 12~~Sections 16 and 19 to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;

(5) An explanation of the consumer's rights with regard to the sale of nonpublic personal information and disclosure of sensitive personal information pursuant to Sections 20 and 21;

(6) A description of the consumer's options to request access, correction, or deletion of nonpublic personal information about the consumer ~~as established under this Act~~pursuant to Section 6 and the instructions for exercising such options;

(7) Any disclosures that the licensee makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);

(8) The licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; by

(a) Describing in general terms who is authorized to have access to the information; and

(b) Stating whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance with the licensee's policy. The licensee is not required to describe technical information about the safeguards it uses~~; and~~.

(~~c~~9) Any disclosure that the licensee makes as authorized under Section 22, 23, or 24, except that the licensee is not required to list those exceptions in the initial or annual Notice of Information Practices required by Sections 7 and 8. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.

B. The licensee's notice may include:

(1) Categories of nonpublic personal information that the licensee reserves the right to disclose in the future, but does not currently disclose; and

Commented [ES32]: This change is intended to clarify the scope of this subsection.

Commented [ES33]: We note that Section 12 describes the form of opt out notice and methods by which an opt out right may be exercised, but does not itself provide an opt out right. Accordingly, we recommend revising this subsection to refer to opt out rights provided under Section 16 (as set forth in our edits thereto) and 19 (providing for opt out from targeted advertising).

Commented [ES34]: For consistency with the other subsections, we recommend referring to the specific section that provides the consumer rights to request access, correction, or deletion of nonpublic personal information, rather than a general reference to the Act in its entirety.

Commented [ES35]: The indentation of subsection (8)(c) appears to be in error, as it does not relate to the details of the licensee's policies and practices for protecting the confidentiality and security of nonpublic personal information that should be described. This subsection should instead be subsection (9).

© 2026 National Association of Insurance Commissioners

(2) Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the right in the future to disclose, but to whom the licensee does not currently disclose, nonpublic personal information.

C. ~~Exceptions:~~

If a licensee does not disclose, and does not reserve the right to disclose, nonpublic personal information about consumers to affiliates or nonaffiliated third parties except as authorized under ~~Sections22~~Sections 22, 23, or 24, the licensee shall state that in its notice, in addition to the information it shall provide under Subsections A(1) ~~and~~through A(8) and Subsection B of this section.

D. Sample Clauses and Federal Model Privacy Form.

(1) Licensees are not required to use any prescribed clauses or model form.

(2) The commissioner may determine that a Licensee's use of any of the following constitutes compliance with this Act:

(a) Sample clauses illustrating some of the notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner;

(b) Model forms illustrating notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner; or

(c) The Federal Model Privacy Forms ~~are~~ included in Appendix A and Appendix B, of this Act.

Section 10. Short Form Initial Notice of Information Practices

A. A licensee may satisfy the initial notice requirements in Sections 7A and 13A by providing a Short Form Initial Notice of Information Practices ~~at the same time the licensee delivers an opt-out notice as required in Section 12 if~~if:

(1) The licensee provides the consumer a reasonable means to obtain its Notice of Information Practices; and

(2) The licensee provides the Notice of Information Practices upon request.

B. A Short Form Initial Notice of Information Practices shall meet all of the following requirements.

(1) Be clear and conspicuous;

(2) State that the licensee's Notice of Information Practices is available upon request;

(3) Explain the reasonable means to obtain the licensee's Notice of Information Practices;

(4) Contain contact information for the commissioner; and

(5) Describe how the consumer can request access to ~~or~~, correction, or deletion of their

Commented [ES36]: Title is not descriptive of the content of Subsection C, as Subsection C does not provide for an exception to the preceding required contents of a notice of information practices. Accordingly, we recommend removing the title of Subsection C.

Commented [ES37]: Apparent typo; it appears this was intended to refer to Subsections A(1) "through" A(8).

Commented [ES38]: Corrected grammatical error.

Commented [ES39]: We note that this Subsection A assumes that an opt out notice must always be provided. This appears to have been inadvertently carried over from current Model 672, under which a notice of information practices is only required prior to forming a customer relationship where an opt out right would also be required. As revised, the notice of information practices is no longer triggered by the formation of a customer relationship where an opt out would also be required. Our recommended edit clarifies that a short-form privacy notice may satisfy notice requirements under Sections 7A and 13A even where the licensee has no obligation to provide an opt out notice because there is no applicable opt out right under the Act.

© 2026 National Association of Insurance Commissioners

nonpublic personal information.

Commented [ES40]: It appears the right to request deletion of nonpublic personal information was inadvertently omitted. For consistency, we recommend including all of the consumer rights established under Section 6.

C. For purposes of this section "reasonable means to obtain the licensee's Notice of Information Practices" includes:

(1) Providing a toll-free telephone number that the consumer may call to request the notice;

(2) Providing a website or other electronic medium that is easily accessible by the consumer; or

(3) Maintaining copies of the notice at the licensee's place of business to be provided upon request.

Section 11. Form of Opt-In Notice to Consumers and Opt-In Methods

A. If a licensee is required to provide an opt-~~int~~in notice under Sections 20 or 21, it shall provide a clear and conspicuous notice to each of its consumers that accurately explains the information proposed to be disclosed, the use of that information, and the consumer's option to opt in to that use. The notice shall state:

Commented [ES41]: Corrected typo.

(1) The licensee discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;

(2) The consumer has the option to opt in to that disclosure; and

(3) A reasonable means by which the consumer may exercise the option to opt in.

B. The licensee shall not disclose that nonpublic personal information to a nonaffiliated third party unless the consumer has affirmatively opted in to the use.

Commented [ES42]: Revised for consistency.

C. The opt-in must be an affirmative act by the consumer. The licensee cannot deem a failure to respond as an opt-in or use pre-checked boxes.

D. The opt-in should be obtained separately from any other communication or consent.

E. The opt-in may be revoked at any time by the consumer. The licensee shall comply with such revocation as soon as reasonably practicable after the licensee receives it.

Commented [ES43]: This sentence has been added to prevent uncertainty regarding the timing for compliance with the revocation of an opt-in election.

Section 12. Form of Opt-Out Notice to Consumers and Opt-Out Methods

A. (1) If a licensee is required to provide an opt-out notice, it shall provide a clear and conspicuous notice to each consumer that accurately explains the right to opt out under that section. To the extent applicable, the notice shall state:

(a) That the licensee discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;

(b) That the consumer has the right to opt out of that disclosure; and

© 2026 National Association of Insurance Commissioners

(c) A reasonable means by which the consumer may exercise the opt-out right.

(2) Requirements

(a) A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if the licensee:

(i) Identifies all of the categories of nonpublic personal information it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to whom the licensee discloses the information, as described in Section 9A(2) and (3), and states the consumer can opt out of the disclosure of that information; and

(ii) Identifies the insurance products or services the consumer obtains from the licensee, either singly or jointly, to which the opt-out would apply.

(b) A licensee provides a reasonable means to exercise an opt-out right if it:

(i) Designates check-off boxes in a prominent position on the relevant forms with the opt-out notice;

(ii) Includes a reply form together with the opt-out notice;

(iii) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the licensee's website, if the consumer agrees to the electronic delivery of information; or

(iv) Provides a toll-free telephone number that consumers may call to opt out.

(c) A licensee does not provide a reasonable means of opting out if:

(i) The only means of opting out is for the consumer to write a letter to the licensee to exercise their opt-out right; or

(ii) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the licensee provided with the initial notice but did not include with the subsequent notice.

(d) A licensee may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

B. A licensee may provide the opt-out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 7.

C. If a licensee provides the opt-out notice after it provides the initial notice, the licensee shall include a copy of the initial notice with the opt-out notice in writing or, if the consumer agrees, electronically.

D. Joint relationships.

© 2026 National Association of Insurance Commissioners

(1) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt-out notice. The licensee's opt-out notice shall explain how the licensee will treat an opt-out direction by a joint consumer (as explained in Paragraph (2) of this subsection).

(2) Any of the joint consumers may exercise the right to opt out. The licensee may either:

(a) Treat an opt-out direction by a joint consumer as applying to all of the associated joint consumers; or

(b) Permit each joint consumer to opt out separately.

(3) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all the joint consumers.

(4) A licensee may not require all joint consumers to opt out before it implements any opt-out direction.

E. A licensee shall comply with a consumer's opt-out direction as soon as reasonably practicable but no later than ~~10~~30 days after the licensee receives it.

F. A consumer may exercise the right to opt out at any time. A consumer's direction to opt-out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.

Commented [ES44]: We note that this 10-day time period for compliance with an opt out request conflicts with the 15-day time period set forth in Section 19 for compliance with opt out requests for disclosure of nonpublic personal information for purposes of targeted advertising. We recommend extending this time period to 30 days, which more appropriately reflects the operational realities of implementing opt-out requests across systems and use cases. At a minimum, the prescribed time period for compliance with opt out requests should be consistent throughout.

Section 13. Revised Notice of Information Practices

A. Except as otherwise authorized in this Act, a licensee shall not, directly or through an affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that the licensee provided to that consumer under Section 7, unless:

(1) The licensee has provided to the consumer a clear and conspicuous revised notice that accurately describes its policies and practices;

(2) The licensee has provided to the consumer a new opt-out notice;

(3) The licensee has given the consumer a reasonable opportunity, before the licensee discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(4) The consumer does not opt out.

B. Examples.

(1) Except as otherwise permitted by Sections 19, 20 and 21, a licensee shall provide a revised notice before it:

(a) Discloses a new category of nonpublic personal information to any nonaffiliated third party; or

(b) Discloses nonpublic personal information to a new category of nonaffiliated third party.

© 2026 National Association of Insurance Commissioners

(2) A revised notice is not required if the licensee discloses nonpublic personal information to a new nonaffiliated third party that the licensee adequately described in its prior notice.

Section 14. Notice of Information Practices to Group Policyholders

Unless a licensee is providing notices of information practices directly to covered individuals described in Section ~~4G)~~4(G)(2)(e)(i), (ii) or (iii), a licensee shall provide initial, annual and revised notices to the plan sponsor, group or blanket insurance policyholder or group annuity contract holder, or workers' compensation policyholder, in the manner described in Sections 7 through 13 of this Act, describing the licensee's privacy practices with respect to nonpublic personal information about individuals covered under the policies, contracts or plans. Compliance with this section satisfies the licensees initial, annual and renewal Notice of Information Practices as required by Sections 7 and 8 and delivery provisions of Section 15.

Section 15. Delivery

A. A licensee shall provide any notices that this Act requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer interacts with the licensee online or in some other electronic fashion, electronically.

B. (1) A licensee may reasonably expect that a consumer will receive actual notice if the licensee:

(a) Hand-delivers a printed copy of the notice to the consumer;

(b) Mails a printed copy of the notice to the last known address of the consumer separately, or in a policy, billing or other written communication;

(c) For a consumer who conducts transactions electronically, in accordance with UETA (insert state electronic transactions act statute), posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service;

(i) The notice should be posted in a manner that enables a consumer to print or save it using programs or apps that are widely available and free of charge.

(ii) Notice is available electronically as long as it is in force.

(d) For an isolated transaction with a consumer, such as the licensee providing an insurance quote or selling the consumer travel insurance, posts the notice and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular insurance product or service.

(e) Provides the notice by any other means authorized by the commissioner.

(2) Examples of unreasonable expectation of actual notice. A licensee may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and

© 2026 National Association of Insurance Commissioners

practices if it:

(a) Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or

(b) Sends the notice via electronic mail to a consumer who does not otherwise communicate with the licensee electronically.

C. A licensee may reasonably expect that a consumer will receive actual notice of the licensee's Notice of Information Practices if:

(1) The consumer uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or

(2) The consumer has requested that the licensee refrain from sending any information regarding the consumer relationship, and the licensee's current privacy notice remains available to the consumer upon request.

D. A licensee may not provide any notice required by this Act solely by orally explaining the notice, either in person or over the telephone.

E. A licensee may provide a joint notice from the licensee and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the licensee and the other institutions. A licensee also may provide a notice on behalf of another financial institution.

F. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of Sections 7A, 8A and 13A, respectively, by providing one notice to those consumers jointly.

© 2026 National Association of Insurance Commissioners

ARTICLE V. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 16. General Rules for Use and Disclosure of Nonpublic Personal Information

A. Use and Disclosure

(1) A licensee may use and disclose nonpublic personal information, including sensitive personal information, about a consumer for purposes of processing a business transaction requested or authorized by the consumer.

(2) A licensee may disclose nonpublic personal information ~~with~~, including sensitive personal information, to affiliates, provided the affiliates' use and disclosure comply with this Act.

~~(3~~(3) (a) Except as provided by Subsection A(3)(b) below, a licensee may disclose a consumer's nonpublic personal information to a nonaffiliated third party only for those purposes and uses identified in Article VI and as expressly permitted or required by Articles V or VI of this Act.

(b) Before a licensee may disclose a consumer's sensitive personal information for purposes other than those specified in subsection A(3)(a) above, a licensee shall provide a clear and conspicuous notice and a reasonable opportunity to opt out of such disclosure in accordance with the requirements of Section 12.

(4) A licensee shall not disclose nonpublic personal information to a nonaffiliated third party except ~~as permitted by~~in compliance with this Act.

(~~4~~5) This section applies to nonpublic personal information collected before and after a consumer exercises an opt-out right under ~~Section~~ Sections 16A(3) and 19 or an opt-in right under Sections 20 and 21~~.(5~~.

(6) If a consumer submits an opt-out request ~~during~~before a transaction ~~and~~is processed and disclosure of the ~~requested~~nonpublic personal information subject to the opt-out request is necessary to ~~complete~~process that transaction, the licensee shall:

(a) Inform the consumer that the transaction cannot be completed without ~~the~~disclosure of the nonpublic personal information; and

(b) Confirm whether the consumer wishes to proceed with the transaction.

B. Limits on Disclosure**.** Except as provided by Section 16A(1), before disclosing a consumer's nonpublic personal information to a nonaffiliated third party, whether directly or through an affiliate, a licensee shall:

(1) Provide the initial notice required by Section 7;

(2) Provide a clear and conspicuous notice to the consumer that details, as relevant:

(a) The consumer's right to opt out of disclosure of nonpublic personal information under Section 16A(3);

Commented [ES45]: For the avoidance of doubt given the restrictive language in Section 21, added specific references to sensitive personal information.

Commented [ES46]: Corrected apparent typo.

Commented [ES47]: As discussed in CAI Comment #9, Article V expressly provides for an opt-out requirement for the disclosure of nonpublic personal information for purposes of targeted advertising and an opt-in requirement for the sale of nonpublic personal information and the disclosure of sensitive personal information, respectively. However, it does not establish a clear baseline for the treatment of disclosures that do not fall into those categories. The following subsection could be read as a broad prohibition on any disclosure that is not expressly permitted in the Act, thereby restricting any disclosures that are not specifically addressed. It also results in uncertainty as to whether the exceptions provided in Article VI constitute "permitted" disclosure, given that they are not addressed in Section 16. We recommend this addition so that all disclosures of nonpublic personal information to nonaffiliated third parties have been addressed with an established standard of treatment, using the opt-out framework as the baseline for disclosures that are not permitted under the exceptions in Article VI or expressly required to use a specific framework under Article V (e.g., Sections 19 through 21). Corresponding changes to the following subsection clarify that disclosure of nonpublic personal information to a nonaffiliated party other than in compliance with the Act is strictly prohibited.

Commented [ES48]: We note that the only opt-out right expressly provided relates to the disclosure of nonpublic personal information for purposes of targeted advertising. It is unclear in what circumstance the processing of a transaction would require the disclosure of nonpublic personal information for purposes of targeted advertising. We have revised the language consistent with our recommendation in Section 16A(3) above. In addition, we note that it may be administratively impossible to halt a transaction to resolve a conflict with an opt-out request received "during" the transaction. Accordingly, we have revised this subsection to require confirmation to proceed with the transaction if (i) an opt-out request is received before the transaction is processed, and (ii) the transaction would require disclosure of nonpublic personal information subject to the opt out request.

Commented [ES49]: Revised to clarify that only the relevant disclosures must be made. As drafted, Section 16(B)(2) could be read to require that a consumer be notified of all possible opt out or opt in rights, even if the licensee is only providing an opt out or seeking an opt in.

Commented [ES50]: Consistent with our comment above, there should be a baseline opt-out requirement for disclosure of nonpublic personal information that does not fall within an exception in Article VI and for which there is no other express requirement articulated under Article V.

© 2026 National Association of Insurance Commissioners

(b) The consumer's right to opt out of disclosure for targeted advertising under Section 19;

(~~b~~c) The consumer's option to opt in to the sale of nonpublic personal information under Section 20; and/or

(~~c~~d) The consumer's option to opt in to the disclosure of sensitive personal information under Section 21.

(3) Provide a reasonable opportunity, before the licensee discloses the information to the nonaffiliated third party, for the consumer to exercise any applicable opt-out right ~~before disclosure~~; and

(4) Obtain and document the consumer's opt-in or opt-out election, as applicable.

C. A licensee may allow a consumer to select certain nonpublic personal information or certain nonaffiliated third parties with respect to which the consumer wishes to exercise any applicable opt out right or opt in option.

Section 17. Limits on Redisclosure and Reuse of Nonpublic Personal Information

A. If a licensee receives nonpublic personal information from a nonaffiliated third-party ~~service provider~~licensee under an exception in Article VI of this Act, the licensee may use and disclose the information in the ordinary course of business to carry out the activity covered by the exception under which the licensee received the information.

B. (1) If a licensee receives nonpublic personal information from a nonaffiliated third-party ~~service provider~~ licensee other than under an exception in Article VI of this Act, the licensee may disclose the information only to the following, provided the disclosure is consistent with this Act:

(a) Affiliates of the nonaffiliated third party ~~service provider~~licensee from which the licensee received the information; and

(b) Affiliates of the licensee who may disclose the information only to the extent that the disclosure would be permissible by the licensee pursuant to this Act.

(2) Example. If a licensee obtains a customer list from a nonaffiliated third-party ~~service provider~~licensee outside of the exceptions in Article VI:

(a) The licensee may use that list for its own purposes consistent with this Act; and

(b) The licensee may disclose that list to another nonaffiliated third-party ~~service provider~~ only as permitted by this Act.

C. If a licensee discloses nonpublic personal information to a nonaffiliated third-party ~~service provider~~licensee under an exception in ~~S~~Article VI of this Act, the nonaffiliated third party ~~service provider~~licensee:

(1) May disclose the information to the licensee's affiliates; and

Commented [ES51]: Revised to clarify that one or more notices may apply.

Commented [ES52]: Corrected apparent omitted word consistent with the preceding items.

Commented [ES53]: Revised wording to clarify that the word "right" is intended to refer to the consumer's "opt-out right," rather than to impose timing of the reasonable opportunity "right before" disclosure (which would conflict with the definition of "reasonable opportunity").

Commented [ES54]: For the avoidance of doubt, we recommend including language expressly permitting targeted opt in or opt out elections, if the licensee wishes to provide that option to its consumers.

Commented [ES55]: As discussed in CAI Comment #10, this section should not be limited to the rediscloure and reuse of nonpublic personal information as between the licensee and its third party service providers. The governance of a third party service provider's use and disclosure of nonpublic personal information has already been addressed in the contractual requirements of Section 5 and the general rule of Section 16 above. This Section 17 should address limitations on the redisclosure and reuse of nonpublic personal information by nonaffiliated third parties that are themselves licensees but may not be service providers (e.g., as between a ceding insurer and a reinsurer) to align with the apparent intent of this section. Consistent changes have been made throughout Section 17.

Commented [ES56]: Corrected apparent typo.

© 2026 National Association of Insurance Commissioners

(2) May disclose and use the information in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

D. If a licensee discloses nonpublic personal information to a nonaffiliated third-party ~~service provider~~licensee other than under an exception in Article VI of this Act, the nonaffiliated third-party ~~service provider~~licensee may disclose the information only:

(1) To the licensee's affiliates who may disclose the information only to the extent that it would be permissible for the licensee to disclose the information pursuant to this Act: and

(2) To any other person, if the disclosure would be lawful if the licensee made it directly to that person.

Section 18. Limits on Sharing Access Number or Access Code Information for Marketing Purposes

A. A licensee shall not, directly or through an affiliate, disclose, other than to a consumer reporting agency, a policy number or similar form of access number or access code for a consumer's policy or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

B. Exceptions. Subsection A of this section does not apply if a licensee discloses a policy number or similar form of access number or access code:

(1) To the licensee's service provider solely in order to perform marketing for the licensee's own products or services, as long as the service provider is not authorized to directly initiate charges to the account;

(2) To a licensee who is a producer solely in order to perform marketing for the licensee's own products or services; or

(3) To a participant in an affinity or similar program where the participants in the program are identified to the consumer when the consumer enters into the program.

(4) Where the policy number, or similar form of access number or access code, is in an encrypted form, as long as the licensee does not provide a means to decode the access number or access code.

Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted Advertising

~~A. Except as otherwise authorized in this Act~~A. Notwithstanding the provisions of Section 22, a licensee may not, directly or through any affiliate, disclose for the purpose of targeted advertising any nonpublic personal information about a consumer to a nonaffiliated third party unless the consumer has been provided clear and conspicuous notice and a reasonable opportunity to opt out of targeted advertising in accordance with the requirements of Section 12 of this Act.

B. A licensee shall act on a consumer's request to opt out within ~~15~~30 days of receipt.

C. A licensee is under no obligation to obtain additional information to execute the opt-out request.

D. A licensee may not solicit the consumer to change their election to opt out for twelve months.

Commented [ES57]: Consistent with our recommended changes to the structure of Section 16 above, the disclosure of nonpublic personal information for purposes of targeted advertising in Section 19 should be treated as an exception to the service provider and joint marketing exceptions in Section 22. In other words, although service providers and joint marketing are excepted from the opt-out requirements, disclosure for purposes of targeted advertising would still be subject to an out-out right.

Commented [ES58]: We note that this 15-day time period for compliance with an opt out request conflicts with the 10-day time period set forth in Section 12 for compliance with opt out requests. We recommend extending this time period to 30 days, which more appropriately reflects the operational realities of implementing opt-out requests across systems and use cases. At a minimum, the prescribed time period for compliance with opt out requests should be consistent throughout.

© 2026 National Association of Insurance Commissioners

E. A consumer has the right to opt out at any time.

Section 20. Limits on Sale of Nonpublic Personal Information

Before a licensee may sell nonpublic personal information:

A. The licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

B. The consumer must affirmatively opt in to the sale of their nonpublic personal information.

Section 21. Limits on Disclosure of Sensitive Personal Information

A. Except as provided by Subsection B below, a licensee may disclose a consumer's sensitive personal information only for those purposes and uses identified in Article VI and as expressly permitted or required by Article VI or other provisions of this Act.

B. Before a licensee may disclose a consumer's sensitive personal information for purposes other than those specified in ~~subsection~~Subsection A of this section:

(1) A licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

(2) The consumer must affirmatively opt in to disclosure of their sensitive personal information.

Commented [ES59]: Despite the express reference to Article VI in this section, the exceptions under Article VI remain limited to the notice and opt-out requirements — Article VI was not revised to include any exceptions to opt-in requirements as requested by the CAI. Therefore, it appears the exceptions for disclosure of SPI would be limited to those in Section 16: (i) to process a business transaction requested or authorized by the consumer; and (ii) to affiliates if their use and disclosure comply with the Act. This is problematic, as it would require a licensee to obtain a consumer's affirmative opt-in consent before allowing nonaffiliated third party service providers to, for example, access SPI outside of the context of processing a business transaction requested or authorized by the consumer (e.g., to investigate security incidents, in connection with a merger or similar corporate transaction, etc.).

Commented [ES60]: Capitalized for consistency.

© 2026 National Association of Insurance Commissioners

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 22. Exception to Notice, Opt-Out and Opt-In Requirements for Disclosure of Nonpublic Personal Information for Service Providers and Joint Marketing

A. General rule.

(1) The opt-out requirements in Sections ~~12~~16A(3) and ~~19~~the opt-in requirements in Section 21 do not apply when a licensee provides nonpublic personal information to a ~~nonaffiliated~~ third party ~~to perform services for the licensee or functions on the licensee's behalf~~service provider, if the licensee:

(a) Provides the initial notice in accordance with Section7; and

(b) Enters into a contractual agreement with the third party ~~that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in Sections 23 or 24 in the ordinary course of business to carry out those purposes~~service provider in accordance with Section 5.

~~(2) Example. If a licensee discloses nonpublic personal information under this section to a financial institution with which the licensee performs joint marketing, the licensee's contractual agreement with that institution meets the requirements of Paragraph (1)(b) of this subsection if it prohibits the institution from disclosing or using the nonpublic personal information except as necessary to carry out the joint marketing or under an exception in Sections 23 or 24 in the ordinary course of business to carry out that joint marketing.~~

~~B. Service may include joint marketing. The services a nonaffiliated third party performs for a licensee under Subsection A of this section may include~~

B. Joint marketing.

(1) The opt-out requirements in Sections 16A(3) and the opt-in requirements in Section 21 do not apply when a licensee provides nonpublic personal information to a nonaffiliated third party for the marketing of the licensee's own products or services or marketing of financial products or services offered pursuant to joint agreements between the licensee and one or more financial institutions~~.~~, if the licensee:

(a) Provides the initial notice in accordance with Section 7; and

() Enters into a contractual agreement with the nonaffiliated third party that prohibits the nonaffiliated third party from disclosing or using the nonpublic personal information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in Sections 23 or 24 in the ordinary course of business to carry out those purposes.

Commented [ES61]: We note that Section 12 describes the form of opt out notice and methods by which an opt out right may be exercised, but does not itself provide an opt out right. We have replaced this reference with a reference to our proposed additional opt-out requirements in Section 16A(3).

Commented [ES62]: As discussed in CAI Comment #12, the exception for disclosure of nonpublic personal information for service providers should also provide for an exception to the opt-in requirement for disclosure of sensitive personal information in Section 21. Despite the express reference to Article VI in Section 21, the exceptions under Article VI remained limited to the notice and opt-out requirements — not opt-in requirements. This is problematic, as it would require a licensee to obtain a consumer's affirmative opt-in consent before allowing nonaffiliated third party service providers to access sensitive personal information outside of the context of processing a business transaction requested or authorized by the consumer.

Commented [ES63]: Revised to clarify the contractual requirements applicable to joint marketing agreements with nonaffiliated third parties that are not third party service providers and to resolve potential conflicts with new Section 5 for third party service providers.

© 2026 National Association of Insurance Commissioners

(2) The initial notice requirements of Section 7 and annual notice requirements of Section 8 do not apply where a licensee receives nonpublic personal information from a nonaffiliated third party pursuant to a joint agreement, provided the licensee:

(a) shall provide an initial notice to a consumer in accordance with Section 7 and annual notices in accordance with Section 8 where a consumer whose information received pursuant to a joint agreement enters into an ongoing relationship with the licensee; and

(b) shall provide an initial notice to a consumer in accordance with Section 7 before the licensee discloses any nonpublic personal information about the consumer to any nonaffiliated third party, other than as authorized by Sections 23 and 24.

C. Definition of "joint agreement." For purposes of this section, "joint agreement" means a written contract pursuant to which a licensee and one or more financial institutions jointly offer, endorse or sponsor a financial product or service.

Section 23. Exceptions to Notice, Opt-In, and Opt-Out Requirements for Disclosure of Nonpublic Personal Information for Processing and Servicing Transactions

A. Exceptions for processing transactions at consumer's request. The requirements for initial notice in Section 7A~~(2),~~ the opt-out requirements in Sections ~~12~~16A(3) and 19, the opt-in requirements in Section 21, and service providers and joint marketing in Section 22 do not apply if the licensee discloses nonpublic personal information as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Servicing or processing an insurance product or service that a consumer requests or authorizes;

(2) Maintaining or servicing the consumer's account with a licensee, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity;

(3) A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer; or

(4) Reinsurance or stop loss or excess loss insurance.

B. "Necessary to effect, administer or enforce a transaction" means that the disclosure is:

(1) Required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or

(2) Required, or is a usual, appropriate or acceptable method:

(a) To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer's account in the ordinary course of providing the insurance product or service;

(b) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

Commented [ES64]: This addition accounts for the elimination of the distinction between a "customer" and a "consumer" and the elimination of existing exemptions from the initial notice requirement for consumers in Section 5B of existing Model 672.

Without this added limited exception to the notice requirements, a licensee who *receives* NPI from another financial institution pursuant to a joint marketing agreement (such as a list of individuals to be jointly marketed to) would be obligated to provide initial and annual notices to all such consumers, despite being limited in their use of the consumer's NPI to only the limited and permitted purpose of conducting the joint marketing. Such an outcome would be entirely inconsistent with the nature of the joint marketing exemption, would cause significant consumer confusion, and would be burdensome for licensees and impair their ability to compete in the broader financial marketplace.

The suggested limited exemption would avoid the need to provide initial and annual notices solely related to joint marketing, but would be clear that such notices would be required when an ongoing relationship (i.e. customer relationship) is formed or prior to disclosure of NPI to other nonaffiliated third parties except as authorized under Sections 23 and 24.

Commented [ES65]: As noted above, it is important that these exemptions extend to opt-in requirements as well as opt-out to avoid conflicting with the necessary processing or servicing of transactions.

Commented [ES66]: This provision should apply to the entirety of Section 7A, not just Subsection 2 thereof. The reference to Subsection 2 appears to have been carried over from current Model 672, which distinguished between customers and consumers. Since this distinction has been removed, this cross-reference should apply to all of Section 7A.

Commented [ES67]: We note that Section 12 describes the form of opt out notice and methods by which an opt out right may be exercised, but does not itself provide an opt out right. We have replaced this reference with a reference to our proposed additional opt-out requirements in Section 16A(3).

Commented [ES68]: As discussed in CAI Comment #12, the exception for disclosure of nonpublic personal information for processing and servicing transactions should also provide for an exception to the opt-in requirement for disclosure of sensitive personal information in Section 21. Despite the express reference to Article VI in Section 21, the exceptions under Article VI remained limited to the notice and opt-out requirements — not opt-in requirements. This is problematic, as it would require a licensee to obtain a consumer's affirmative opt-in consent before allowing disclosure of sensitive personal information as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer or in connection with the circumstances specified in this Section 23.

© 2026 National Association of Insurance Commissioners

(c) To provide a confirmation, statement or other record of the transaction, or information on the status or value of the insurance product or service to the consumer or the consumer's agent or broker;

(d) To accrue or recognize incentives or bonuses associated with the transaction that are provided by a licensee or any other party;

(e) To underwrite insurance at the consumer's request or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects or as otherwise required or specifically permitted by federal or state law; or

(f) In connection with:

(i) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited or otherwise paid using a debit, credit or other payment card, check or account number, or by other payment means;

(ii) The transfer of receivables, accounts or interests therein; or

(iii) The audit of debit, credit or other payment information.

Section 24. Other Exceptions to Notice, Opt-In, and Opt-Out Requirements for Disclosure of Nonpublic Personal Information

A. Exceptions to opt out requirements. The requirements for initial notice to consumers in Section 7A~~(2),~~ the opt-out requirements in Sections ~~12~~16A(3) and 19, the opt-in requirements in Section 21, and service providers and joint marketing in Section 22 do not apply when a licensee discloses nonpublic personal information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

(2) (a) To protect the confidentiality or security of a licensee's records pertaining to the consumer, service, product or transaction;

(b) To protect against or prevent actual or potential fraud or unauthorized transactions;

(c) For required institutional risk control or for resolving consumer disputes or inquiries;

(d) To persons holding a legal or beneficial interest relating to the consumer; or

(e) To persons acting in a fiduciary or representative capacity on behalf of the

Commented [ES69]: This provision should apply to the entirety of Section 7A, not just Subsection 2 thereof. The reference to Subsection 2 appears to have been carried over from current Model 672, which distinguished between customers and consumers. Since this distinction has been removed, this cross-reference should apply to all of Section 7A.

Commented [ES70]: We note that Section 12 describes the form of opt out notice and methods by which an opt out right may be exercised, but does not itself provide an opt out right. We have replaced this reference with a reference to our proposed additional opt-out requirements in Section 16A(3).

Commented [ES71]: As discussed in CAI Comment #12, the other exceptions for disclosure of nonpublic personal information in this Section 24 should also provide for an exception to the opt-in requirement for disclosure of sensitive personal information in Section 21. Despite the express reference to Article VI in Section 21, the exceptions under Article VI remained limited to the notice and opt-out requirements — not opt-in requirements. This is problematic, as it would require a licensee to obtain a consumer's affirmative opt-in consent before allowing disclosure of sensitive personal information as necessary for the critical operational needs provided in this Section 24, such as to protect against fraud; to prevent, detect, and investigate security incidents; and to comply with legal obligations.

© 2026 National Association of Insurance Commissioners

consumer;

(f) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted nonpublic personal information.

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating a licensee, persons that are assessing the licensee's compliance with industry standards, and the licensee's attorneys, accountants and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the federal Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, the Securities and Exchange Commission, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance authority, and the Federal Trade Commission), self-regulatory organizations or for an investigation on a matter related to public safety;

(5) (a) To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or

(b) From a consumer report reported by a consumer reporting agency;

(6) In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of the business or unit;

(7) (a) To comply with federal, state or local laws, rules and other applicable legal requirements;

(b) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities; or

(c) To respond to judicial process or government regulatory authorities having jurisdiction over a licensee for examination, compliance or other purposes as authorized by law; or

(8) For purposes related to the replacement of a group benefit plan, a group health plan, a group welfare plan or a workers' compensation plan.

B. Example of revocation of consent. A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under Section 12F.

Drafting Note: Because the notice requirements of this Act could be a financial burden on a company in liquidation or receivership and negatively impact the ability of the liquidator or receiver to pay claims, regulators may want

© 2026 National Association of Insurance Commissioners

to consider adding an additional exception providing that licensees in liquidation or receivership are not subject to the notice provisions of this Act.

© 2026 National Association of Insurance Commissioners

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 25. When Authorization Required for Disclosure of Nonpublic Personal Health Information

A. A licensee shall not disclose nonpublic personal health information about a consumer unless an authorization is obtained from the consumer whose nonpublic personal health information is sought to be disclosed.

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee:

(1) Claims administration any processing;

(2) Claims adjustment and management;

(3) Detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity;

(4) Underwriting;

(5) Policy placement or issuance;

(6) Loss control;

(7) Ratemaking and guaranty fund functions;

(8) Reinsurance and excess loss insurance;

(9) Risk management;

(10) Case management;

(11) Disease management;

(12) Quality assurance;

(13) Quality improvement;

(14) Performance evaluation;

(15) Provider credentialing verification;

(16) Utilization review;

(17) Peer review activities;

(18) Actuarial, scientific, medical or public policy research;

(19) Grievance procedures;

© 2026 National Association of Insurance Commissioners

(20) Internal administration of compliance, managerial, and information systems;

(21) Policyholder service functions;

(22) Auditing;

(23) Reporting;

(24) Database security;

(25) Administration of consumer disputes and inquiries;

(26) External accreditation standards;

(27) The replacement of a group benefit plan or workers' compensation policy or program;

(28) Activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit;

(29) Any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services or other applicable laws;

(30) Disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes including subrogation, and

(31) Any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with the legal process.

C. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable

Section 26. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article VII shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer who is the subject of the nonpublic personal health information;

(2) A general description of the types of nonpublic personal health information to be disclosed;

(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

(4) The signature, including electronic signatures, of the consumer who is the subject of the

© 2026 National Association of Insurance Commissioners

nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer may revoke the authorization at any time and the procedure for making a revocation.

(6) Any additional information necessary to comply with HIPAA or any other applicable law.

B. An authorization for the purposes of this Article VII shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article VII at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

E. A signed copy of the authorization shall be provided to the consumer.

Section 27. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer as part of an opt-out notice pursuant to Section 12, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section 25A.

Section 28. Relationship to Federal Rules

A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

This Act shall not apply to nonprofits, such as the National Association of Insurance Commissioners or the National Insurance Crime Bureau, when processing or sharing information solely for investigating criminal or fraudulent insurance acts.

Section 29. Relationship to State Laws

Nothing in this Article shall preempt or supersede existing state law related to medical records, consumer data privacy, health or insurance information privacy.

© 2026 National Association of Insurance Commissioners

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 30. Protection of Fair Credit Reporting Act

Nothing in this Act shall be construed to modify, limit or supersede the operation of the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and no inference shall be made regarding whether information is transaction or experience information under Section 603 of that Act.

Section 31. Nondiscrimination

A. A licensee shall not unfairly discriminate against any consumer because that consumer has opted out from the disclosure of his or her nonpublic personal information pursuant to the provisions of this Act.

B. A licensee shall not unfairly discriminate against a consumer because that consumer has not granted authorization for the disclosure of his or her nonpublic personal health information pursuant to the provisions of this Act.

Section 32. Violation

Drafting Note: Cite state unfair trade practices act or other applicable state law.

Section 33. Severability

If any section or portion of a section of this Act or its applicability to any person or circumstance is held invalid by a court, the remainder of the Act or the applicability of the provision to other persons or circumstances shall not be affected.

Section 34. Individual Remedies

This Act may not be construed to create or imply a private cause of action for violation of its provisions, nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Section 35. Effective Date

A. Effective date. This ~~Acthas~~Act has been effective since November 13, 2000. The amendments to this Act are effective [Insert Effective Date]. In order to provide sufficient time for licensees to establish policies and systems to comply with the amendments to this Act, the commissioner has extended the time for compliance with the amendments to this Act until [Insert Compliance Date].

B. By [Insert Compliance Date], a licensee shall provide an initial notice, as required by Section 7, to any existing consumer who has not previously received a notice that complies with the amendments to this Act.

C. Two-year grandfathering of service agreements. Until [Insert Compliance Date], a contract that a licensee has entered into with a ~~nonaffiliated~~ third party ~~to perform services for the licensee or functions on the licensee's behalf~~service provider satisfies the provisions of Section ~~22A(1)(b)~~5 of this Act, even if the contract does not include ~~a requirement that the third party maintain the confidentiality of nonpublic personal information~~the provisions specified in Section 5, as long as

© 2026 National Association of Insurance Commissioners

the licensee entered into the agreement on or before [Insert Compliance Date].

Commented [ES72]: Revised for consistency with the contractual requirements in Section 5 above for third party service providers.

© 2026 National Association of Insurance Commissioners

APPENDIX A – SAMPLE CLAUSES

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A-1–Categories of information a licensee collects (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(1) to describe the categories of nonpublic personal information the licensee collects.

Sample Clause A-1:

We collect nonpublic personal information about you from the following sources:

Information we receive from you on applications or other forms;
Information about your transactions with us, our affiliates or others; and
Information we receive from a consumer reporting agency.

A-2–Categories of information a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use one of these clauses, as applicable, to meet the requirement of Section 9A(2) to describe the categories of nonpublic personal information the licensee discloses. The licensee may use these clauses if it discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-2, Alternative 1:

We may disclose the following kinds of nonpublic personal information about you:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premiums, and payment history"]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your creditworthiness and credit history"].

Sample Clause A-2, Alternative 2:

We may disclose all of the information that we collect, as described [describe location in the notice, such as "above" or "below"].

A-3–Categories of information a licensee discloses and parties to whom the licensee discloses (institutions that do not disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirements of Sections 9A(2) and (3) to describe the

© 2026 National Association of Insurance Commissioners

categories of nonpublic personal information the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses. A licensee may use this clause if the licensee does not disclose nonpublic personal information to any party, other than as permitted by the exceptions in Sections 23 and 24.

Sample Clause A-3:

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

A-4–Categories of parties to whom a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(3) to describe the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information. This clause may be used if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-4:

We may disclose nonpublic personal information about you to the following types of third parties:

Financial service providers, such as [provide illustrative examples, such as "life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents"];

Non-financial companies, such as [provide illustrative examples, such as "retailers, direct marketers, airlines, and publishers"]; and

Others, such as [provide illustrative examples, such as "non-profit organizations"].

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

A-5–Service provider/joint marketing exception
A licensee may use one of these clauses, as applicable, to meet the requirements of Section 9A(2) related to the exception for service providers and joint marketers in Section 22. If a licensee discloses nonpublic personal information under this exception, the licensee shall describe the categories of nonpublic personal information the licensee discloses and the categories of third parties with which the licensee has contracted.

Sample Clause A-5, Alternative 1:

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premium, and payment history"]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your

© 2026 National Association of Insurance Commissioners

creditworthiness and credit history"].

Sample Clause A-5, Alternative 2:

We may disclose all of the information we collect, as described [describe location in the notice, such as "above" or "below"] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

A-6–Explanation of opt- out right (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(4) to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. The licensee may use this clause if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-6:

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [describe a reasonable means of opting out, such as "call the following toll-free number: (insert number)].

A-7–Confidentiality and security (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(8) to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A-7:

We restrict access to nonpublic personal information about you to [provide an appropriate description, such as "those employees who need to know that information to provide products or services to you"]. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

© 2026 National Association of Insurance Commissioners

APPENDIX B – FEDERAL MODEL PRIVACY FORM

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the Federal Model Privacy Form, if the Form is accurate for each institution that uses the Form. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A. General Instructions

1. How the Model Privacy Form is used.

(a) The Model Form may be used, at the option of a "licensee", including a group of licensees or other financial institutions that use a common privacy notice, to meet the content requirements of the privacy notice and opt-out notice set forth in [insert citation for sections of statute or regulation sections that parallel Sections 9and 11 of the NAIC *Privacy of Consumer ~~InformationAct~~Information Act*]

(b) The Model Form is a standardized form, including page layout, content, format, style, pagination, and shading. Licensees seeking to obtain the safe harbor through use of the Model Form may modify it only as described in these Instructions.

(c) Note that disclosure of certain information, such as assets, income, and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act (FCRA), codified at 15 U.S.C. §§ 1681-1681x, such as a requirement to permit a consumer to opt out of disclosures to affiliates, or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.

(d) The word "consumer" may be replaced by the word "member," whenever it appears in the Model Form, as appropriate.

2. The Contents of the Model Privacy Form

The Model Form consists of two pages, which may be printed on both sides of a single sheet of paper or may appear on two separate pages. Where a licensee provides a long list of licensees or financial institutions at the end of the Model Form in accordance with Instruction B3(a)(i), or provides additional information in accordance with Instruction B3(c) and such list or additional information exceeds the space available on Page Two of the Model Form, such list or additional information may extend to a third page.

(a) Page One. The first page consists of the following components:

(1) Date last revised (upper right-hand corner)
(2) Title
(3) Key frame (Why? What? How?)
(4) Disclosure table ("Reasons we can share your personal information")
(5) "To limit our sharing" box, as needed, for the licensee's opt-out information
(6) "Questions" box, for customer service contact information
(7) Mail-in opt-out form, as needed

(b) Page Two. The second page consists of the following components:

© 2026 National Association of Insurance Commissioners

(1) Heading (Page 2)
(2) Frequently Asked Questions ("Who we are" and "What we do")
(3) Definitions
(4) "Other important information" box, as needed

3. The format of the Model Privacy Form.

The format of the Model Form may be modified only as described below.

(a) Easily readable type font. Licensees that use the Model Form must use an easily readable type font. While a number of factors together produce easily readable font, licensees are required to use a minimum of 10-point font (unless otherwise expressly permitted in these Instructions) and sufficient spacing between lines.

(b) Logo. A licensee may include a corporate logo on any page of the notice, so long as it does not interfere with the readability of the Model Form or the space constraints of each page.

(c) Page size and orientation. Each page of the Model Form must be printed in portrait orientation, the size of which must be sufficient to meet the layout and minimum font size requirements, with sufficient white space on the top, bottom, and sides of the content.

(d) Color. The Model Form must be printed on white or light color paper (such as cream) with black or other contrasting ink color. Spot color may be used to achieve visual interest, so long as the color contrast is distinctive and the color does not detract from the readability of the Model Form. Logos may also be printed in color.

(e) Languages. The Model Form may be translated into languages other than English.

B. Information Required in the Model Privacy Form

The information in the Model Form may be modified only as described below:

1. Name of licensee or group of affiliated licensees or institutions providing the notice
Insert the name of the licensee providing the notice, or a common identity of the affiliated licensees or financial institutions jointly providing the notice on the form, wherever [name of licensee] appears.

2. Page One

(a) Last revised date. The licensee must insert in the upper right-hand corner the date on which the notice was last revised. The information shall appear in minimum 8-point font as "rev. [month/year]" using either the name or number of the month, such as "rev. July 2016" or "rev. 7/16."

(b) General instructions for the "What?" box

(i) The bulleted list identifies the types of personal information that the licensee collects and shares. All licensees must use the term "Social Security Number" in the first bullet.

(ii) A licensee must use five (5) of the following terms, to complete the bulleted list: income; account balances; payment history; transaction history; transaction or loss history; credit history; credit scores; assets; investment experience; credit-based insurance scores; insurance claim history; medical information; overdraft

© 2026 National Association of Insurance Commissioners

history; purchase history; account transactions; risk tolerance; medical-related debts; credit card or other debt; mortgage rates and payments; retirement assets; checking account information; employment information; wire transfer instructions.

(c) General instructions for the disclosure table. The left column lists reasons for sharing or using personal information. Each reason correlates to a specific legal provision described in Paragraph 2(d) of this Instruction. In the middle column, each licensee must provide a "Yes" or "No" response that accurately reflects its information-sharing policies and practices with respect to the reason listed on the left. In the right column, each licensee must provide in each box one of the following three (3) responses, as applicable, that reflects whether a consumer can limit such sharing:

"Yes," if it is required to or voluntarily provides an opt-out; "No," if it does not provide an opt-out; or

"We don't share," if it answers "No" in the middle column.

Only the sixth row ("For our affiliates to market to you") may be omitted at the option of the licensee. See Paragraph 2(d)(6) of this instruction.

(d) Specific disclosures and corresponding legal provisions

(i) For our everyday business purposes. This reason incorporates sharing information under [insert citation for sections of statute or regulation sections that parallel Sections 23 and 24 of NAIC model *Privacy of Consumer ~~InformationAct~~Information Act*] and with service providers pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*] other than the disclosures described in Paragraphs (2)(d)(ii) or (2)(d)(iii) of this instruction.

(ii) For our marketing purposes. This reason incorporates sharing information with service providers by a licensee for its own marketing pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iii) For joint marketing with other financial companies. This reason incorporates sharing information under joint marketing agreements between 2 or more licensees or financial institutions and with any service provider used in conjunction with such agreement pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iv) For our affiliates' everyday business purposes – information about transactions and experiences. This reason incorporates sharing information specified in Sections 603(d)(2)(A)(i) and (ii) of the FCRA. A licensee that shares information for this reason may choose to provide an opt-out.

(v) For our affiliates' everyday business purposes – information about creditworthiness. This reason incorporates sharing information pursuant to Section 603(d)(2)(A)(iii) of the FCRA. A licensee that shares information for this reason must provide an opt-out.

(vi) For our affiliates to market to you. This reason incorporates sharing information specified in Section 624 of the FCRA. This reason may be omitted from the disclosure table when: the licensee does not have affiliates (or does not disclose personal information to its affiliates); the licensee's affiliates do not use personal information in a manner that requires an opt-out; or the licensee provides the affiliate marketing notice separately. Licensees that include this reason must provide an opt-out of indefinite duration. A licensee that is required to provide an

© 2026 National Association of Insurance Commissioners

affiliate marketing opt-out, but does not include that opt-out in the Model Form under this part, must comply with Section 624 of the FCRA and [insert citation for statute or regulation that parallels NAIC *Privacy of Consumer Information Act*], with respect to the initial notice and opt-out and any subsequent renewal notice and opt-out. A licensee not required to provide an opt-out under this subparagraph may elect to include this reason in the Model Form.

(vii) For nonaffiliates to market to you. This reason incorporates sharing described in [insert citation for sections of statute or regulation sections that parallel Sections 11 and 16(B) of NAIC *Privacy of Consumer Information Act*]. A licensee that shares personal information for this reason must provide an opt-out.

(e) To limit our sharing. A licensee must include this section of the Model Form only if it provides an opt-out. The word "choice" may be written in either the singular or plural, as appropriate. Licensees must select one or more of the applicable opt-out methods described: telephone, such as by a toll-free number; a web site; or use of a mail-in opt-out form. Licensees may include the word "toll-free" before telephone, as appropriate. A licensee that allows consumers to opt out online must provide either a specific web address that takes consumers directly to the opt-out page or a general web address that provides a clear and conspicuous direct link to the opt-out page. The opt-out choices made available to the consumer who contacts the licensee through these methods must correspond accurately to the "Yes" responses in the third column of the disclosure table. In the part entitled "Please note," licensees may insert a number that is 30 days or greater in the space marked "[30]." Instructions on voluntary or state privacy law opt-out information are in Paragraph 2(g)(v) of these Instructions.

(f) Questions box. Customer service contact information must be inserted as appropriate where [phone number] or [web site] appear. Licensees may elect to provide either a phone number, such as a toll-free number, or a web address, or both. Licensees may include the words "toll-free" before the telephone number, as appropriate.

(g) Mail-in opt-out form. Licensees must include this mail-in form only if they state in the "To limit our sharing" box that consumers can opt out by mail. The mail-in form must provide opt-out options that correspond accurately to the "Yes" responses in the third column of the disclosure table. Licensees that require consumers to provide only name and address may omit the section identified as "[account #]." Licensees that require additional or different information, such as a random opt-out number or a truncated account number to implement an opt-out election should modify the "[account #]" reference accordingly. This includes licensees that require customers consumers with multiple accounts to identify each account to which the opt-out should apply. A licensee must enter its opt-out mailing address in the far right of this form (see version 3); or below the form (see version 4). The reverse side of the mail-in opt-out form must not include any content of the Model Form.

(i) Joint accountholder. Only licensees that provide their joint accountholders the choice to opt out for only one accountholder, in accordance with Paragraph 3(a)(5) of these Instructions, must include in the far left column of the mail-in form the following statement:

If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.

□ Apply my choice(s) only to me.

The word "choice" may be written in either the singular or plural, as appropriate. Licensees that provide insurance products or services, provide this option, and elect to use the Model Form may substitute the word "policy" for "account" in this statement. Licensees that do not provide this option may eliminate this left column from the mail-in form.

(ii) FCRA Section 603(d)(2)(A)(iii) opt-out. If the licensee shares personal information pursuant to Section

© 2026 National Association of Insurance Commissioners

603(d)(2)(A)(iii) of the FCRA, it must include in the mail-in opt-out form the following statement:

□ Do not share information about my creditworthiness with your affiliates for their everyday business purposes.

(iii) FCRA Section 624 opt-out. If the licensee uses Section 624 of the FCRA, in accord with paragraph 2(d)(6) of these Instructions, it must include in the mail-in opt-out form the following statement:

□ Do not allow your affiliates to use my personal information to market to me.

(iv) Nonaffiliate opt-out. If the licensee shares personal information pursuant to [insert citation for section of statute or regulation that parallels Section 16(B) of NAIC *Privacy of Consumer ~~InformationAct~~Information Act*], it must include in the mail-in opt-out form the following statement:

□ Do not share my personal information with nonaffiliates to market their products and services to me.

(v) Additional opt-outs. Licensees that use the disclosure table to provide opt-out options beyond those required by Federal law must provide those opt-outs in this section of the Model Form. A licensee that chooses to offer an opt-out for its own marketing in the mail-in opt-out form must include one of the two following statements:

□ Do not share my personal information to market to me. or

□ Do not use my personal information to market to me.

A licensee that chooses to offer an opt-out for joint marketing must include the following statement:

□ Do not share my personal information with other financial institutions to jointly market to me.

(h) Barcodes. A licensee may elect to include a barcode and/or "tagline" (an internal identifier) in 6-point type at the bottom of page one, as needed for information internal to the licensee, so long as these do not interfere with the clarity or text of the form.

3. Page Two

(a) General Instructions for the Questions. Certain Questions on the Model Form may be customized as follows:

(i) "Who is providing this notice?" This question may be omitted where only one licensee provides the Model Form and that licensee is clearly identified in the title on Page One. Two or more licensees or financial institutions that jointly provide the Model Form must use this question to identify themselves as required by [insert citation for section of statute or regulation that parallels Section 15(E) of NAIC model *Privacy of Consumer Information Act*]. Where the list of licensees or financial institutions exceeds four (4) lines, the licensee must describe in the response to this question the general types of licensees or financial institutions jointly providing the notice and must separately identify those licensees or financial institutions, in minimum 8-point font, directly following the "Other important information" box, or, if that box is not included in the licensee's form, directly following the "Definitions." The list may appear in a multi- column format.

(ii) "How does [name of licensee] protect my personal information?" The licensee may only provide additional information pertaining to its safeguards practices following the designated response to this question. Such information may include information about the licensee's use of cookies or other measures it uses to

© 2026 National Association of Insurance Commissioners

safeguard personal information. Licensees are limited to a maximum of 30 additional words.

(iii) "How does [name of licensee] collect my personal information?" Licensees must use five (5) of the following terms to complete the bulleted list for this question: open an account; deposit money; pay your bills; apply for a loan; use your credit or debit card; seek financial or tax advice; apply for insurance; pay insurance premiums; file an insurance claim; seek advice about your investments; buy securities from us; sell securities to us; direct us to buy securities; direct us to sell your securities; make deposits or withdrawals from your account; enter into an investment advisory contract; give us your income information; provide employment information; give us your employment history; tell us about your investment or retirement portfolio; tell us about your investment or retirement earnings; apply for financing; apply for a lease; provide account information; give us your contact information; pay us by check; give us your wage statements; provide your mortgage information; make a wire transfer; tell us who receives the money; tell us where to send the money; show your government-issued ID; show your driver's license; order a commodity futures or option trade.

Licensees that collect personal information from their affiliates and/or credit bureaus must include the following statement after the bulleted list: "We also collect your personal information from others, such as credit bureaus, affiliates, or other companies." Licensees that do not collect personal information from their affiliates or credit bureaus but do collect information from other companies must include the following statement instead: "We also collect your personal information from other companies." Only licensees that do not collect any personal information from affiliates, credit bureaus, or other companies can omit both statements.

(iv) "Why can't I limit all sharing?" Licensees that describe state privacy law provisions in the "Other important information" box must use the bracketed sentence: "See below for more on your rights under state law." Other licensees must omit this sentence.

(v) "What happens when I limit sharing for an account I hold jointly with someone else?" Only licensees that provide opt-out options must use this question. Other licensees must omit this question. Licensees must choose one of the following two statements to respond to this question: "Your choices will apply to everyone on your account." or "Your choices will apply to everyone on your account—unless you tell us otherwise." Licensees may substitute the word "policy" for "account" in these statements.

(b) General Instructions for the Definitions. The licensee must customize the space below the responses to the three definitions in this section. This specific information must be in italicized lettering to set off the information from the standardized definitions.

(i) Affiliates. As required by [insert citation for section of statute or regulation that parallels Section 9(A)(3) of NAIC *Privacy of Consumer Information Act*], where [affiliate information] appears, the licensee must:

(a) If it has no affiliates, state: "[name of licensee] has no affiliates";

(b) If it has affiliates but does not share personal information with them, state: "[name of licensee] does not share with our affiliates"; or

(c) If it shares with its affiliates, state, as applicable: "Our affiliates include companies with a [common corporate identity of licensee] name; financial companies such as [insert illustrative list of companies]; nonfinancial companies, such as [insert illustrative list of companies]; and others, such as [insert illustrative list]."

(ii) Nonaffiliates. As required by [insert citation for section of statute or regulation that parallels Section 9~~)~~[(A)(3) of NAIC *Privacy of Consumer ~~InformationAct~~Information Act*], where [nonaffiliate information] appears, the licensee must:

© 2026 National Association of Insurance Commissioners

(a) If it does not share with nonaffiliated third parties, state: "[name of licensee] does not share with nonaffiliates so they can market to you"; or

(b) If it shares with nonaffiliated third parties, state, as applicable: "Nonaffiliates we share with can include [list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations]."

(iii) Joint Marketing. As required by [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*], where [joint marketing] appears, the licensee must:

(a) If it does not engage in joint marketing, state: "[name of licensee] doesn't jointly market"; or

(b) If it shares personal information for joint marketing, state, as applicable: "Our joint marketing partners include [list categories of companies such as credit card companies]."

(c) General instructions for the "Other important information" box. This box is optional. The space provided for information in this box is not limited, and an additional page may be used if necessary. Only the following types of information can appear in this box:

(i) State and/or international privacy law information; and/or

(ii) A form by which the consumer may acknowledge receipt of the notice.

Chronological Summary of Actions (all references are to the Proceedings of the NAIC)

2000 Proc. 3rd Quarter 7, 10, 14-36, 904 (adopted).
2002 Proc. 3rd Quarter12, 13, 71, 72-73 (amended).
2017 Spring National Meeting (amended).

© 2026 National Association of Insurance Commissioners

Version 1:
Model Form with No Opt-Out

Rev. [insert date]

FACTS	WHAT DOES [Name of Licensee] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores] When you are *no longer* our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

Questions?	Call [phone number] or go to [web site]

© 2026 National Association of Insurance Commissioners

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Version 2: Model Form with Opt-Out by Telephone and/or Online

Rev. [insert date]

FACTS	WHAT DOES [NAME OF LICENSEE] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

To limit our sharing	■ Call [phone number] —our menu will prompt you through your choice(s) **or** ■ Visit us online: [web site] **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

© 2026 National Association of Insurance Commissioners

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Rev. [insert date

Version 3: Model Form with Mail-in Opt-Out Form

FACTS	WHAT DOES **[NAME OF LICENSEE]** DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

© 2026 National Association of Insurance Commissioners

Page 2

To limit our sharing	▪ Call [phone number] —our menu will prompt you through your choice(s) ▪ Visit us online: [web site] or ▪ Mail the form below **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

Mail-in Form

Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless your mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me.
	Name
	Address
	City, State, Zip
	[Account #]
Mail To:	[Name of Licensee] [Address] [City], [ST] [ZIP]

© 2026 National Association of Insurance Commissioners

Page 3

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ▪ [open an account] or [deposit money] ▪ pay your bills] or [apply for a loan] ▪ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ▪ sharing for affiliates' everyday business purposes—information about your creditworthiness ▪ affiliates from using your information to market to you ▪ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ▪ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ▪ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ▪ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Version 4: Optional Mail-in Form

Mail-in Form	
Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me. **Name** **Address** **City, State, Zip** **[Account #]**
Mail To:	[Name of Licensee], [Address 1], [Address 2], [City], [ST] [ZIP]

© 2026 National Association of Insurance Commissioners

THE COUNCIL
OF INSURANCE AGENTS & BROKERS

September 22, 2026

Re: CIAB Comments on Revised *Privacy of Consumer Information Act* (#672)

Dear Chair Dwyer and Working Group members,

The Council of Insurance Agents and Brokers (The Council) appreciates the opportunity to review and comment on the proposed revisions to the *Privacy of Consumer Information Act* (#672). The Council is home to 150 of the fastest-growing, most innovative commercial property and casualty and employee benefits brokerages around the world. Council member firms represent 47 of the top 50 largest brokers of U.S. business, annually placing 70 percent of all employee benefits business in the U.S. and 90 percent of all property and casualty premiums.

The Council commends the Privacy Protections (H) Working Group for its efforts to modernize the model law and strengthen consumer privacy protections. At the same time, our members are increasingly challenged by a growing patchwork of state, federal, and industry-specific privacy requirements. As the Working Group considers revisions to Model #672, we encourage you to prioritize uniformity, clarity, and interoperability with existing privacy frameworks, and to avoid creating unique requirements that could further complicate nationwide compliance efforts.

With these goals in mind, The Council respectfully offers the below recommendations to further improve Model #672.

1. **Restore the Customer-Based Trigger for Licensee Obligations.**

The new "consumer"-based approach would trigger significant regulatory obligations for licensees with respect to individuals with whom they never established a business relationship or no longer maintain one. Under the current model, privacy notice and other obligations attach when an individual becomes a customer with an ongoing business relationship with the licensee (i.e., when the licensee actually provides products or services to a consumer). By contrast, a "consumer" includes individuals who *seek to obtain* products or services from a licensee or *have obtained* products or services in the past.

The practical result is that licensees could be obligated to provide initial *and* ongoing privacy notices (so long as the licensee retains mere "access" to a consumer's data) and to effectuate individuals' rights to access, correct, and delete non-public personal information (NPI), even if the consumer never actually obtains products or services from the licensee. Further, because these obligations appear to continue for as long as a licensee has access to a consumer's NPI, a licensee could remain subject to ongoing compliance obligations long after any business relationship has ended.
We appreciate that the model includes certain exceptions intended to address these operational concerns, but those exceptions do not go far enough and generate a lot of compliance uncertainty for licensees. Section 23, for example, appears to provide exemptions from the initial privacy

notice and opt-out requirements when a licensee discloses NPI as necessary to effect, administer, or enforce a transaction requested or authorized by a consumer (i.e., to try to place coverage for a consumer after the consumer files an application). But it would not provide that relief if the licensee gains *access* to a consumer's NPI (the trigger for Section 7 notices) and ultimately does not *disclose* the NPI (the trigger for the Section 23 exception). Section 23 also does not appear to relieve licensees of their obligations to comply with consumer rights requests relating to access, correction, or deletion of NPI, or annual notice requirements under Section 8 for individuals who never become customers.

Likewise, the model exempts licensees from annual notice requirements when they no longer have *access* to NPI, which still could require annual notices in the absence of an ongoing relationship with the consumer. This represents a significant departure from the existing framework. If a consumer changes brokers of record, for example, the prior broker could remain obligated to provide annual privacy notices solely because of continued possession of the consumer's NPI. Removing individual consumers' NPI from all systems (i.e., removing licensee access) in real time is operationally infeasible, but until all access is removed, the Section 8 annual notice obligations would continue to apply.

Finally, while we appreciate that the revised model retains the excess lines exception under the definition of "licensee," the new "consumer" trigger still would require excess lines brokers to send notices of information practices to consumers with whom they never directly interact (that is the role of the retail agent) and for whom excess lines coverage is never actually placed.

Ultimately, the revised approach dramatically expands licensees' obligations, administrative burdens, and costs vis-à-vis the current model. Additionally, it has great potential to confuse consumers who could receive privacy notices from all licensees with whom they've ever sought products or services, as well as those with whom they have established an actual customer relationship.

Accordingly, **The Council recommends reinstating the prior customer-based trigger tied to an ongoing business relationship** as a far less cumbersome, confusing, and costly approach**.** Doing so would ensure that privacy and related compliance obligations apply only where a licensee maintains an actual business relationship with an individual and would avoid the illogical result of imposing ongoing obligations with respect to individuals who either never became customers or are no longer customers.

2. **Clarify Applicability of Subsection 4(G)(2)(e) to Insurance Producers and Delete 4(G)(2)(f).**

The Council supports the intent of Section 4(G)(2)(e) to avoid requiring licensees to provide individual privacy notices to every participant, beneficiary, or covered individual under an employee benefit plan or group policy when notice is appropriately provided to the plan sponsor/group policyholder. The exception in (e)(i) for benefit plans is too narrow to capture producers, however, because producers do not typically administer or sponsor employee benefit

plans *or* act as trustees, insurers or fiduciaries. **We therefore recommend revising (e)(i) to include employee benefit plans that the licensee *places*, administers or sponsors.**

Additionally, subsection 4(G)(2)(f) is difficult to parse and appears to be entirely unnecessary. Subsection (e) already captures licensees' obligations with respect to plan sponsors/group policyholders and clarifies that individuals do not become "consumers" solely because of their status as participants, beneficiaries, or covered individuals under group insurance. **The Council therefore recommends deleting subsection 4(G)(2)(f) entirely** to avoid unnecessary confusion**.**

3. **Rationalize Disclosure Provisions Regarding NPI Shared by Licensees with Third-Party Service Providers.**

Section 6(A)(1) requires licensees to disclose to consumers, upon request, *all* NPI about the consumer that is maintained by a contracted third-party service provider. This is an unreasonable standard. Licensees should not and cannot practically track or disclose NPI held by third parties that does not come from the licensees or that is not maintained by the third party on the licensee's behalf.

In addition, requiring disclosure of all specific third-party service providers that *ever* receive NPI from the licensee is unnecessarily onerous and operationally infeasible. Licensee contracts with particular providers change over time, as do third-party entities themselves (i.e., they cease doing business, they change ownership or merge, etc.). Under the proposal, licensees' notices would have to be constantly updated to keep up with those developments and licensees would have to disclose past sharing of NPI with third parties that may have terminated their contractual relationship with the licensee or even ceased to exist long ago.

The Council therefore **recommends revising Section 6(A)(1) by**:

- Limiting disclosure obligations to NPI **maintained by a contracted third-party service provider *on the licensee's behalf***; and

- Requiring disclosure of ***categories* of third-party services providers**, rather than a list of every provider that has ever received the consumer's NPI from the licensee.

4. **Harmonize Opt-Out Compliance Timelines around a 15-Day Standard.**

The draft revisions contain inconsistent deadlines for implementing a consumer's opt-out request. Specifically, Section 12 provides a 10-day compliance period, whereas Section 19 provides a 15-day compliance period. To avoid confusion and facilitate compliance, The Council recommends adopting a uniform 15-day timeframe throughout the model.

5. **Expand Exceptions to and Compliance Timelines for Consumer Deletion Rights.**

The Council recommends expanding Section 6(C)(2) to include additional scenarios where a licensee has a legitimate business reason to retain a consumer's NPI, despite the consumer's

request to delete; specifically permitting retention of information necessary for (e.g., to defend against, dispute, or prove claims) or in reasonable anticipation of regulatory proceedings.

We also recommend clarifying that a licensee may request an *additional* 45 days to comply with a deletion request when information is maintained on archived or backup systems. Adding the word "additional" would eliminate ambiguity regarding the available extension period:

> *Section 6(c)(3). (3) A licensee may delay fulfilling a consumer's request, up to* ***an additional*** *45 days, to delete nonpublic personal information stored on an archived or backup system. A licensee must notify the consumer of such delay.*

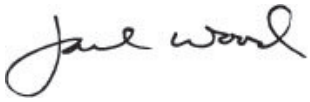
6. Avoid Using Undefined Terms and Clarify the "Sale" Definition.

Several undefined terms are used in the proposed revisions, creating uncertainty regarding content and scope of various compliance obligations (e.g., "servicing," "processing," "authenticated request").

Also, for clarity, we recommend adding an exclusion from the definition of "sale" for remuneration that licensees receive from insurance transactions or through conducting their insurance business (e.g., producer commissions). Establishing such compensation may require exchange of NPI, but it does not constitute the type of consumer data monetization that privacy laws are generally intended to regulate.

The Council appreciates the Working Group's consideration of our comments.

Sincerely,



Joel Wood
President & CEO
The Council of Insurance Agents and Brokers
JWood@ciab.com

Independent Insurance Agents & Brokers of America • 127 South Peyton Street, Alexandria VA 22314

September 22, 2026

Re: Comments Concerning the Proposed Revisions to Model 672 (July 2026 Draft)

Dear Director Dwyer:

On behalf of the Independent Insurance Agents and Brokers of America (IIABA), the largest insurance agent and broker organization in the country, I write to offer our association's comments and perspective regarding the proposed revisions to NAIC Model Law 672 outlined in the July 2026 draft.

Initial Comments

IIABA recognizes and appreciates the desire of the NAIC to review its existing privacy-related proposals for state policymakers and to update and upgrade those model law recommendations. It is appropriate for the NAIC to revisit these issues and consider more robust requirements, especially given the magnitude of privacy activity that has occurred in statehouses over the last several years. Privacy is important to independent insurance agents and the consumers they serve, and our members utilize the nonpublic personal information of customers to address their insurance needs and share it when necessary to provide products and services to those consumers. Consumers understand the reasons why our members need this information, and agents are not misusing or surreptitiously selling off that information in the ways that data brokers in other industries have done.

IIABA does not object to reasonable and thoughtfully crafted enhancements to the data privacy requirements, but we strongly oppose the working group's draft. The proposal is onerous, unrealistic, and notably outside of the regulatory mainstream.

As the NAIC contemplates how to proceed with this project, we encourage you to consider the body of privacy law that has quickly emerged in recent years, the ways in which your proposal deviates from that accepted framework, and the manner in which your proposal is likely to be received by state legislators as a result. A geographically and politically diverse group of 24 states, which represent approximately 60% of the population in our country, have now enacted comprehensive privacy laws[1]. These measures include many of the same core elements, address those issues in a similar way, and have produced a fairly consistent regulatory framework. Although these statutes do not apply to insurance licensees, banks, and other types of financial institutions, these recently enacted laws are very instructive and relevant to the work you are now performing.

These recently enacted privacy laws indicate the current perspectives and views of state legislators, and they suggest that state policymakers would be unlikely to want to establish a completely different and unique set of data privacy requirements just for the insurance industry. Many data privacy observers naturally anticipated that the Privacy Protections Working Group

[1] The following states have enacted comprehensive privacy laws: Alabama, California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Louisiana, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oklahoma, Oregon, Rhode Island, Tennessee, Texas, Utah, Vermont, and Virginia.

would propose requirements for the insurance industry that largely mirror the requirements that these 24 states have applied to many other industries. Unfortunately, the working group's proposal differs in notable and unwarranted ways from the standards and requirements found in these state laws and instead recommends unique mandates and harsher regulatory obligations that would only apply to the insurance industry.

IIABA believes it would be serious mistake – for both public policy and political reasons – to adopt a model law that proposes requirements and obligations that are dramatically different and harsher than the privacy mandates quickly being established for other industries. A proposal that contains such mandates and standards is unlikely to be considered seriously by state policymakers and will not produce the interstate uniformity that is ultimately the goal of your efforts. We recognize that the working group is being encouraged by some well-intentioned and very passionate voices to adopt a model that is a departure from the regulatory mainstream, but we encourage you to reject such calls, be mindful of the flurry of public policymaking activity and the resulting body of privacy law that has emerged, and to move forward in a thoughtful and reasonable way.

In the pages that follow, we highlight some of our most notable concerns with the draft proposal. While we focus in this letter on several key items, we also strongly share many of the same concerns addressed by other industry associations in their submissions to the working group (including the problems and challenges created by the elimination of the "customer" definition and the broad definition and use of the term "consumer").

Section 5 / Third-Party Service Provider Arrangements

Inherent and Threshold Problems with Section 5

Section 5 is a proposed new addition to Model 672 and the source of our strongest objections. Subsection (A) would require any insurance licensee who discloses nonpublic personal information to a third-party service provider to enter into a very detailed and prescriptive contract with that entity. Subsection (B) is equally troubling and totally unprecedented, and this subsection would make a licensee fully responsible for the handling of nonpublic personal information by service providers. The requirements of this section would apply to all insurance licensees, including all insurance agents, regardless of size and sophistication. IIABA strongly opposes both subsections and urges significant revisions to Section 5 if it is ultimately retained in the draft.

Section 5 is impractical and unrealistic because it would attempt to regulate third-party service providers through insurance licensees, and it would unreasonably force small and medium-sized businesses to police and assume absolute legal responsibility for the actions of vendors. The reality is that agents and brokers lack the ability to dictate business practices and contractual terms to service providers (and especially to technology vendors like Microsoft and AWS)), which are typically much larger, more sophisticated, and geographically remote. Our members have even less ability to affect the actions and conduct of a provider's subcontractors. Main street insurance agents rely heavily on the services provided by vendors, yet service providers typically present contracts to licensees on a take-it-or-leave-it basis and without meaningful opportunity for negotiation. The power and bargaining imbalance and the lack of leverage that agents and brokers possess is obvious, and the establishment of the requirements contemplated by Section 5 would only place agents and brokers in an untenable position and in legal jeopardy.

Given the marketplace and structural realities that exist and the problems that the Section 5 requirements would create, it is no surprise that no state has applied mandates of this nature to small and medium-sized businesses. Section 5 and its proposed application of these obligations to *all* licensees is significantly different and far more expansive and onerous than the privacy frameworks that have been put in place in many states. If the NAIC were to move forward with this section in its current form, it effectively would be recommending the establishment of unrealistic mandates for insurance agents and brokers that no other category of small business in the United States is subject to. The creation of such anomalous and unprecedented requirements for insurance agents (and insurance agencies alone) is unwarranted.

Alternatives

IIABA strongly opposes any model law or legislative proposal that contains the types of requirements currently found in Section 5, and we respectfully urge the working group to revisit and dramatically revise this section. The working group can address the problems in Section 5 in one of three ways: (1) by limiting application of the section to large and sophisticated entities, (2) by regulating the conduct of third-party service providers directly, or (3) by deleting the section in its entirety. The working group might also consider a combination of these options and could, for example, delete Subsection (B) while limiting the application of Subsection (A) to larger licensees.

While the option to delete the section altogether likely requires little additional elaboration, we address the other two alternative approaches in more detail below.

Option 1 – Tailoring Application of Section 5

As noted above, the proposed application of Section 5 to all insurance licensees is inconsistent with the many state comprehensive privacy laws enacted in recent years. Those acts do not apply any third-party service provider-related mandates to small- and medium-sized businesses. The comprehensive state privacy laws generally apply their requirements to businesses who maintained the nonpublic personal information of a specified number of state consumers in the previous year, and the lowest of these consumer applicability thresholds is 35,000 residents. Two other states (Nebraska and Texas) only apply requirements to businesses who do not qualify as small businesses under regulations promulgated by the federal Small Business Administration. As a result, any NAIC model law that proposes service provider obligations for all insurance licensees (including all insurance agencies) is significantly different and far more expansive and onerous than the privacy regimes already being put in place by state policymakers.

One option for the working group is to limit the applicability of Section 5 or to include a limited exemption that more closely and appropriately mirrors the comprehensive state privacy laws. There are numerous ways in which such a provision could be crafted, but one possibility would be to add the following as a new subsection:

> *__. The requirements of this section shall not apply to a licensee that:*
>
> *(a) Controlled or processed the nonpublic personal information of fewer than 35,000 resident consumers during the preceding calendar year; or*
>
> *(b) Is a small business as defined by the federal Small Business Administration.*

This recommendation follows the example that has been provided by the comprehensive state privacy laws, and the consumer threshold outlined above is the lowest such threshold found in any of those statutes. IIABA would also be amenable to other alternative thresholds so long as they avoid the problems that the current draft creates. Adding a limited exemption of this nature will help harmonize the model law with state privacy statutes, avoid an outcome in which the insurance industry is uniquely subjected to harsher privacy requirements, prevent small and medium-sized insurance agencies from being placed in untenable positions, and increase the likelihood that this model will be considered and enacted by state legislators.

We should note that we envision this as a *limited exemption* (from Section 5 and any other provisions specified in the proposed draft) and *not a complete exemption* from all of the model's requirements.

Option 2 – Imposing Obligations Directly on Service Providers

Section 5 appears intended to ensure that third-party service providers will act (or not act) in particular ways and engage (or not engage) in certain conduct. Rather than instituting such requirements directly, however, the proposal places the burden of policing service providers on licensees and requires licensees to dictate very specific contractual terms to providers and assume full legal responsibility for vendor behavior. This is challenging and unrealistic for the reasons discussed above. This scenario is additionally troubling because the failure or inability of an insurance agency to convince a service provider to enter into such a contract could prevent that business from securing services that are crucial to meeting client needs or result in statutory violations, enforcement actions, and fines. It should also be noted that even if a licensee is able to secure the contractual terms required by the proposal, there is no guarantee that a service provider will actually honor the agreement or any assurance that the anticipated public policy outcomes will be achieved.

An alternative and far more efficient, effective, and practical way to address these subjects would be to impose requirements on third-party service providers directly. The working group could propose the establishment of whatever statutory requirements it chooses for service providers, and state insurance regulators or some other state agency or official (e.g., a state attorney general) could be charged with enforcement of those obligations. This commonsense approach has successful precedents in both federal and state law, and the direct application of such requirements on service providers would be more likely to produce the desired public policy outcomes you seek. There is no downside to addressing third-party service provider conduct directly, and we urge you to do so.

Section 6 / Access, Correction, and Deletion of Nonpublic Personal Information

Section 6 is a proposed new addition to Model 672 that would enable consumers to request access to and the correction or deletion of certain nonpublic personal information.

Authentication of Requests

Section 6 and paragraph (D)(1) in particular appear to contemplate that all licensees will be required to authenticate any consumer request that are submitted pursuant to this section, but it is unclear exactly what would be expected of licensees. Section 6(D)(1)(a) states that a licensee "may use its secure communications portal to authenticate requests," but this is an option very few agents will be able to offer or be able to cost-effectively implement. The subparagraph also says a "licensee may use methods that are commercially reasonable, but not

unduly burdensome, to authenticate the identity of the person making the request." While this statement is welcome, it would be helpful if the working group can provide greater specificity about its expectations and perhaps provide additional examples of how authentication could occur.

Data Access Requests

IIABA agrees strongly with our fellow commenters who have expressed concern and opposition to Section 6(A)(1)(a), the provision that would require disclosure of every third-party service provider in response to every consumer data access request. Among other issues, a mandate of this nature would be challenging for licensees to satisfy and offer little meaningful benefit to consumers. We urge you to delete this subparagraph.

Data Correction Requests

Section 6(B) addresses the ability of consumers to request corrections of their nonpublic personal information. Paragraph (3) specifies the instances in which a request may be denied, and IIABA recommends revising the provision to make clear that a correction is not required when the information was accurate and complete at the time it was provided. Specifically, the working group might consider revising Section 6(B)(3)(a) so that a correction is not required if "[t]he nonpublic personal information is accurate and complete or was accurate and complete when it was provided and if the licensee provides a process for appeal of the decision."

Data Deletion Requests

Section 6(C) addresses the ability of consumers to request deletion of nonpublic personal information, and paragraph (2) provides a series of exemptions from this proposed obligation. While the exemptions are helpful, they are too narrow in scope, and IIABA joins other industry colleagues in recommending that the working group expand this list to account for other instances in which licensees may require the need to possess certain information. At a minimum, IIABA encourages the working group to add a new exemption to Section 6(C)(2) if the information in question is used to "protect against or prevent actual or potential fraud, identity theft, unauthorized transactions, claims, or other liability."

To the extent that there is any concern with expanding the list of exemptions, the working group could also consider a limitation on the use of information that is retained due to an exemption and only allow a licensee to prospectively use such information for a purpose described in list of exemptions found in Section 6(C)(2).

Other Observations Concerning Consumer Privacy Requests

Laws that enable consumers to request access and correction or deletion of their nonpublic information are not new. Insurance licensees in some states have been required to respond to requests of this nature since the early 1980s, and the nearly 25 state comprehensive privacy laws include provisions along these lines (although they do not apply to the insurance industry and only apply to a large businesses).

As the working group and NAIC consider how to craft the requirements of this section, we note that very few consumers ever make requests to access, correct, or delete their nonpublic person even when a legislature has empowered them to do so. This is especially true in the insurance world, where the information used to help place insurance typically comes from the

applicant/insured directly or from a consumer reporting agency that is subject to its own data privacy regime. We do not make this observation about the lack of such requests in order to argue against the establishment of request rights, but it is especially important (given this reality) that any related obligations imposed on licensees be appropriately crafted and contemplate the costs and benefits of the specific requirements. It does not make sense to impose significant compliance and infrastructure expenses on licensees in order to satisfy requirements that are highly unlikely to be triggered.

Also, unlike the many comprehensive state policy laws that have recently been adopted, the data request rights in this section would apply new requirements to licensees of all sizes, including all insurance agents and brokers, and not merely to large businesses. If these requirements are ultimately established for agents and brokers of all sizes, it will be critically important that the new obligations can easily, efficiently, and cost-effectively be complied with.

Sections 7, 9, 13, and 23 / Notices of Information Practices

As a threshold matter, IIABA shares the concerns expressed by others about the elimination of the "customer" definition and the broad expansion of the notice of information practices provisions. These changes would require the delivery of many new notices (including to individuals who are not even customers of a licensee), confuse the recipients of these notices in many instances, increase compliance burdens for licensees, and provide questionable public policy benefit. We respectfully urge the working group to consider the significant effects these revisions would have and to more appropriately tailor the nature of the privacy notice obligations.

In addition, Section 7(A) requires the delivery of the initial privacy notice to a consumer "no later than when the licensee obtains access to the consumer's nonpublic personal information" unless one of two narrow exceptions are satisfied. The draft suggests that the notice requirement is triggered when a "licensee obtains access to the consumer's nonpublic personal information," but the actual effect of this subsection appears nuanced given the definitions and other provisions found in the draft. IIABA worries that the proposed text in this subsection will confuse laypeople trying to understand their obligations, and IIABA urges the working group to revise the provision (perhaps in a manner consistent with the proposed revision submitted by the American Council of Life Insurers).

Section 9(A) identifies a series of eight items that must be addressed in every notice of information practices, but there are likely to be instances when some of these mandated disclosures are not applicable or relevant. For example, Section 9(A)(4) would require an explanation of how a consumer can opt out of the disclosure of nonpublic personal information, but such a disclosure is likely to be confusing if the licensee informs the consumer pursuant to Section 9(A)(3) that there is no covered information being shared in this way. Similarly, Section 9(A)(5) would require an explanation of a consumer's rights with regard to sale of nonpublic personal information, but this does not make sense if the licensee is not selling information and in light of the fact that any such sale also would require an individual's permission. Accordingly, IIABA urges the working group to amend these and perhaps other paragraphs in Section 9(A) so that the obligation is only triggered "when applicable."

Section 13(B)(1) includes several references to other sections of the proposal, but the references do not appear to be correct. The text currently mentions Sections 19, 20, and 21, and our understanding is that it is intended to reference Sections 22, 23, and 24.

Section 23(A) also includes a reference to Section 7 that should be revised. Specifically, Section 23(A) currently includes a reference to "the requirements for initial notice in Section 7(A)(2)." Given the revisions that have been made to Section 7, this reference should be made to requirements for initial notice in *Section 7.* Other references in this subsection and elsewhere in the proposal may need to be reviewed and corrected as well.

Section 16 / Use and Disclosure of Nonpublic Personal Information

Section 16 is a revision to Section 12 of existing Model 672, and Subsection (B) addresses and updates the existing restrictions that apply to a licensee's disclosure of nonpublic personal information to nonaffiliated third parties. Subsection (A) is an entirely new set of provisions, and several of the items in this subsection are peculiar and potentially troubling. Two of the provisions are particular sources of concern:

- Section 16(A)(1) appears to be a superfluous provision, serves no purpose, and should be deleted. Retaining this paragraph will only create confusion and add to the complexity already associated with the lengthy and complex proposal.

- Section 16(A)(2) is also confusing and unnecessary. Affiliates that receive nonpublic personal information are of course obligated to satisfy any obligations applied to them by this proposal, and the inclusion of this paragraph only muddies the waters.

Intersection with the FCRA

The working group proposal retains a section of the existing model (now found in Section 30) that addresses the Fair Credit Reporting Act (FCRA) and the manner in which 15 U.S.C. 1681t(b)(1) preempts certain areas and types of state law that are governed solely by federal law. There has been very little focus on the intersection of the FCRA and the revisions that the working group has made to Model 672, and this may be a subject that the working group wishes to explore before taking any final action. We imagine, for example, that the working group would want to avoid a scenario in which an unlevel playing field is established among licensees because the requirements proposed in the draft might apply to some competitors and not to others as a result of the FCRA's broad preemptive scope.

Conclusion

IIABA thanks you and the working group for your consideration of our views and looks forward to working with you as your efforts continue. If we can provide any additional information or assistance, please feel free to contact me by phone at 202-302-1607 or via email at wes.bissett@iiaba.net.

Very truly yours,



Wesley Bissett
Senior Counsel, Government Affairs

INSURED RETIREMENT INSTITUTE

September 22, 2026

TO: The NAIC Privacy Protections (H) Working Group (the "Working Group")

Re: Full Exposure Draft of Revisions to the Privacy of Consumer Financial and Health Information Regulation (#672)

Dear Members of the Working Group:

On behalf of our members, the Insured Retirement Institute (IRI)[1] writes to share comments on the full exposure draft of revisions to the Privacy of Consumer Financial and Health Information Regulation (the "Revised Chair's Draft"), released by the Working Group on July 24, 2026. We are appreciative of the Working Group's continued efforts on this important issue, and we welcome the opportunity to comment on the revised Model as an integrated whole for the first time.

Overall, our members appreciate that the Working Group is working to modernize the model privacy framework. We are also pleased to see that a number of our prior recommendations have been reflected in this draft, including, as a structural matter, the separation of "sale" and "targeted advertising" into distinct sections with defined terms and carve-outs. Significant concerns remain in several other areas, however, including the third-party service provider requirements in Article II and the electronic delivery provisions in Section 15.

While the Revised Chair's Draft makes meaningful progress in several areas, there are still some provisions that we believe should be revised. Our members have reviewed the redline submitted by the American Council of Life Insurers (ACLI) to the Working Group on September 22, 2026, and we broadly support the recommended edits reflected in that redline. In particular, we support restoring the "customer" definition and the corresponding distinction between customers and consumers throughout the Model, which several of the recommendations below assume. In addition, we would like to highlight one threshold issue and a select number of provisions of particular importance to our members.

An Opt-Out Default Should Apply Throughout the Model to Preserve GLBA Harmonization

[1] The Insured Retirement Institute (IRI) is the leading association for the entire supply chain of insured retirement strategies, including life insurers, asset managers, and distributors such as broker-dealers, banks and marketing organizations. IRI members account for more than 95 percent of annuity assets in the U.S., include the top 10 distributors of annuities ranked by assets under management, and are represented by financial professionals serving millions of Americans. IRI champions retirement security for all through leadership in advocacy, awareness, research, and the advancement of digital solutions within a collaborative industry community.

As a threshold matter, however, we continue to believe an opt-out approach is the right default. It makes sense to establish an opt-out framework for marketing and targeted advertising, and we appreciate that the Revised Chair's Draft moves in that direction in Section 19. We remain concerned, however, about the opt-in requirements retained in Section 21 for sensitive personal information.

The Exposure Draft would layer three separate consent regimes on top of one another: a general opt-out, a targeted advertising opt-out, and an opt-in for sale and sensitive personal information. Our members are concerned that this creates a fragmented framework that may be difficult for consumers to understand and navigate, and that it would require significant system modifications, new consent-tracking capabilities, and revised notices and workflows. It also departs from the longstanding GLBA standard and places insurers in a different position than other regulated financial institutions such as banks. We continue to urge the Working Group to preserve harmonization with GLBA and to keep an opt-out approach as the default throughout the Model.

Consumer Rights Requests Under Section 6

Article III establishes a new individual-rights regime that will require most carriers to build request-fulfillment capabilities they do not have today. We support giving consumers meaningful access, correction, and deletion rights, but three aspects of Section 6 should be adjusted so that those rights can be administered as intended.

- Section 6.D(2) removes a cap on the number of correction and deletion requests a customer or former customer may submit. Without a reasonable limit, a licensee must authenticate, investigate, and substantively respond to an unlimited volume of duplicative requests, each carrying a 45-day deadline and an appeal right, with little corresponding benefit to a customer or former customer who has already received a response and exhausted the appeal process. We recommend limiting a customer or former customer to two requests per calendar year.

- Section 6.C(3) permits only a 45-day delay for information stored on archived or backup systems. Requiring companies to search inactive archives is overly burdensome and, for many legacy systems, not technically feasible. We suggest allowing compliance to be deferred until the archived or backup system is restored or is next accessed or used.

- Section 6.A(1)(b) requires disclosure of a list of all third-party service providers who received the consumer's information. This should be changed to "categories," which is consistent with comparable state privacy laws. A consumer-specific enumeration is burdensome to produce and does not improve the consumer's understanding of how their information is used.

Notice Obligations Under Sections 7 and 8

Section 7.A would require the notice of information practices to be delivered no later than when the licensee obtains access to a consumer's nonpublic personal information. A notice at collection is extremely difficult to provide when the company does not collect the information directly from the individual and may have no direct relationship with, or reliable contact information for, that individual. We support the approach ACLI has proposed in its redline to address this issue.

Section 8 would extend the annual notice to every consumer, including an applicant whose application was never completed and an individual who simply expressed interest in a product. That is not practical, and as drafted the obligation has no terminating event. The draft language would seemingly require notices to go to these individuals in perpetuity. The existing model appropriately limited the annual notice to customers with an ongoing relationship and only for the duration of that relationship, and we recommend restoring that scope.

We are particularly concerned about beneficiaries. Requiring a notice to be sent to a beneficiary would effectively disclose that the individual has been designated. Designations can change at any time, so the notice may communicate information that is no longer accurate, and there may be legitimate reasons why a policyowner would not want a beneficiary to know of the designation. A notice obligation that discloses a designation the policyowner has chosen not to share does not advance consumer privacy. We recommend that beneficiaries be expressly excluded from the notice obligations, at least prior to the time a claim is made.

Opt-Out Mechanics Under Sections 12 and 19

Section 12.A(2)(a)(ii) would require an opt-out notice to identify the specific insurance products or services the consumer obtains from the licensee. Requiring notices to be individualized in this way could create a significant operational burden because licensees would need to generate and maintain consumer-specific notice content at scale. We support striking this requirement, as reflected in the ACLI redline.

Section 19.A should also be revised to make clear that the targeted advertising opt-out is completed through the company's website rather than by mail. A website-based opt-out is consistent with the CCPA, is what consumers expect, and can be honored far more quickly and reliably than a mailed request — which matters in particular given the 15-day response deadline in Section 19.B.

Finally, while we support the ACLI redline, we understand that other groups are developing and submitting redlines of their own, and we want to be clear that we are fully open to alternative approaches and suggestions that address the concerns we have raised. Additional time and work are needed to work through these issues, and we encourage the Working Group to continue

working with stakeholders as this project moves forward and to provide additional comment periods on any updates that are made to the Model. Given the scope of the revisions reflected in this Exposure Draft, and the fact that several provisions have been substantively changed between exposures, it is important that interested parties have a meaningful opportunity to review and provide feedback on revised language before the Model is finalized.

We appreciate the Working Group's consideration of these comments. Please don't hesitate to contact me with any questions or concerns.

Sincerely,

Sarah E. Wood

Sarah Wood
Director, State Policy & Regulatory Affairs
Insured Retirement Institute
swood@irionline.org



I

September 22, 2026

Re: Comments of the Insurtech Coalition on the revised Privacy of Consumer Financial and Health Information Regulation (Model #672), full exposure draft dated July 24, 2026

Dear Chair and Members of the Working Group:

The Insurtech Coalition supports modernizing Model #672 rather than building a new model from scratch, and we support giving consumers real access, correction and deletion rights in insurance. We are not asking the Working Group to slow down. We are asking you to fix seven provisions in the July 24 draft that either do not work in a digital insurance transaction or work against other things the NAIC is trying to accomplish.

The Coalition's members are technology-enabled insurers, managing general agents and insurance technology companies. Our members compete against carriers many times their size, which shapes how we read this draft. Privacy compliance in insurance is close to a fixed cost, so every obligation that has to be built once and maintained forever is paid disproportionately by newer and smaller carriers and is passed through to their policyholders. Several provisions below cost an incumbent a project and cost a new entrant a market.

1. Keep the definition of nonpublic personal information anchored to the insurance transaction.

Section 4 defines nonpublic personal information as personally identifiable information that is "linked or reasonably linkable to an identified natural person." Section 4R(1) then defines personally identifiable information by reference to the insurance transaction: information a consumer provides to a licensee to obtain an insurance product or service, information about a consumer resulting from an insurance transaction, and information the licensee otherwise obtains about a consumer in connection with one. Read together, those definitions keep nonpublic personal information where Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 et seq., puts it. The linkability standard changes how a licensee decides whether information identifies a person. It does not change what information is in scope. The Coalition reads the draft that way, and we ask the Working Group to say so expressly.

That reading matters most for the data a digital carrier holds before, or without, any insurance transaction. Cookies, device identifiers, IP addresses and the clickstream from an abandoned quote session are not information a consumer provides to obtain insurance, do not result from an insurance transaction and are not obtained in connection with one. They should not carry Article III access, correction and deletion rights or Article IV notice obligations. Information a consumer actually submits in a quote is different, and we do not ask the Working Group to exclude it. Without the clarification, a state could read the linkability standard to reach data GLBA does not. Because state comprehensive privacy statutes exempt data subject to GLBA Title V, the result would be a category of insurance data governed by two regimes with different definitions, different clocks and different exceptions. Add a drafting note confirming that

the linkability standard does not expand the scope set by Section 4R(1), and state expressly that information governed by GLBA, the Fair Credit Reporting Act and HIPAA continues to be governed by those laws.

2. Third-party claimants should not hold access, correction and deletion rights in an open claim file.

Section 4G(2)(d)(i)(II) defines consumer to include claimants. Article III then gives every consumer the right to see all nonpublic personal information a licensee and its service providers hold about them, to demand correction and to demand deletion within 45 days. In automobile insurance the claimant is frequently adverse to the carrier and to the insured. The deletion exceptions cover information retained under a legal requirement or maintained in anticipation of a claim or proceeding, but they are not written to cover the investigation itself: adjuster notes, recorded statements, special investigative unit referrals and the analytics that flag suspected fraud, all of which insurers are required to maintain under state anti-fraud plans and the Insurance Fraud Prevention Model Act (#680).

Read as written, the draft hands a person with a suspicious claim a statutory tool to learn what the carrier knows and then demand that it be deleted. Exclude third-party claimants from Article III while a claim or related proceeding is open, and add express exceptions for claim investigation materials, anti-fraud and SIU records, privileged material and attorney work product.

3. Access should produce categories of third parties, not a vendor list, and should not reach proprietary models.

Section 6(A) requires a licensee to disclose a list of all third-party service providers that received the consumer's information. This scheme would make the insurance industry an outlier, without a clear purpose in doing so. State comprehensive privacy laws require categories of recipients, which is also what Section 9 of this same draft requires in the privacy notice. That notice standard is the right one.

The proposed list requirement carries two costs that categories do not. A per-consumer map of a carrier's data supply chain gives bad actors what they need to create a social engineering attack. That makes the access right a security liability. And for a technology-driven carrier the vendor stack is the architecture, which makes the access right a free competitive intelligence request available to anyone willing to file one. We also ask for an express exception for trade secrets, proprietary models, scores and algorithm inputs, so that an access request is not a discovery mechanism for underwriting IP.

4. Correction should not displace the FCRA dispute process or force rating outside filed rules.

Section 6(B) permits a licensee to deny a correction request for information it did not create, unless the originator is unavailable and the consumer has independently demonstrated the information is incorrect. For consumer report information, Congress already built that process. 15 U.S.C. 1681i places the dispute with the consumer reporting agency and the furnisher, with defined timelines and reinvestigation duties. Layering a second and different process onto the insurer produces two answers to the same question and no way to reconcile them, and it puts carriers in the position of adjudicating the accuracy of data they do not control.

The draft is also silent on what a correction means downstream. Rating variables and underwriting rules are on file with the department, and a carrier cannot re-rate a policy outside its filed rates and rules. Route

disputes about consumer report information to the FCRA process, and state that correction does not require retroactive re-rating or any deviation from filed rates and rules.

5. Deletion should not override retention obligations, and repetitive requests need a valve.

Section 6(C) permits denial where retention is required by law. That is narrower than it sounds. Market conduct examination, statistical reporting, actuarial rate development, reserving and audit obligations are not always framed as a duty to retain a particular record about a particular consumer. A carrier that has deleted the data cannot answer the examiner, cannot support the indication behind a rate filing and cannot reproduce the experience underlying a rate already on file. The Working Group should not adopt a regulation that a licensee can be compelled to use to destroy what a department will ask for on examination.

The draft also states affirmatively that there is no cap on the number of correction or deletion requests. Every state comprehensive privacy law allows a controller to decline or charge for requests that are manifestly unfounded, excessive or repetitive. Model #672 should have the same valve, along with express retention exceptions for examination, statistical reporting, actuarial and rate development, reserving and audit.

6. Article II vendor terms should apply prospectively and drop the 48-hour clock.

Section 5 requires written contracts obligating third-party service providers to notify the licensee within 48 hours in two separate circumstances, to delete or return information on request, to flow terms down to subcontractors on no less protective terms and to assist with Article III requests. We do not object to the substance. We object to the clock and to the timing.

We question why 48 hours was chosen in this case. The failures identified in Section 5A(1)-(6) about which insurers would have to be notified under the draft are significant to be sure, but none create an immediate risk of irreparable harm to consumers. We suggest that a “promptly” or “without unreasonable delay” standard is more appropriate and workable. Moreover, the retroactivity of Section 5 is highly problematic. The providers underneath a modern insurance stack, meaning cloud, payments, identity and AI infrastructure vendors, do not negotiate bespoke terms with a carrier of any size. If Section 5 reaches contracts already in force, the practical result is that smaller carriers lose access to infrastructure that incumbents keep under legacy terms. Apply Section 5 only to contracts entered into or renewed after the effective date, set the notice period at “without unreasonable delay,” and allow a standard data protection addendum to satisfy the requirement.

7. Keep the private cause of action disclaimer as drafted.

Article VIII provides that the regulation may not be construed to create or imply a private cause of action for violation of its provisions, and may not be construed to curtail a private cause of action that would otherwise exist. That language should survive to adoption unchanged. Enforcement belongs with the commissioner under the state unfair trade practices act the draft references. A regulation of this scope carrying a private right of action would not be adopted uniformly, and non-uniform adoption is the outcome that costs consumers the most.

8. Give the market one effective date and one standard.

The draft still carries the 2000 effective date and provides no implementation timeline for the new obligations. Article III consumer request infrastructure, Article IV notice redesign and Article II vendor repapering are each multi-quarter builds, and they are sequential rather than parallel. Provide a uniform implementation period of 24 months from state adoption, a drafting note urging states to adopt without state-specific variation, and a safe harbor providing that a licensee in compliance with this regulation is deemed compliant with any state comprehensive privacy statute as applied to insurance data. The purpose of a model is a single national standard. Without a uniformity provision, this draft produces fifty versions of a right consumers cannot use consistently and carriers cannot build once.

Proposed amendments

The table below states each issue and the change we ask the Working Group to make. We are glad to provide full redline language on any line.

Section	Issue	Proposed amendment
Sec. 4, "nonpublic personal information"	The "linked or reasonably linkable" standard could be read to expand the scope Section 4R(1) sets and reach cookies, device identifiers and abandoned quote clickstream.	Add a drafting note confirming that the linkability standard does not expand the scope of Section 4R(1), and state that information governed by GLBA, FCRA and HIPAA remains governed by those laws.
Sec. 4, "consumer"; Art. III	Third-party claimants hold access, correction and deletion rights in a claim file the licensee is using to evaluate a claim against them.	Exclude third-party claimants from Article III rights while the claim or a related proceeding is open.
Sec. 6(C)	Deletion exceptions do not clearly cover investigation and anti-fraud material insurers are required to keep.	Add express exceptions for claim investigation materials, SIU and anti-fraud records, privileged material and attorney work product.
Sec. 6(A)	A per-consumer list of every service provider is a security exposure and a competitive disclosure, and is inconsistent with the categories standard in Section 9.	Replace the list of all third-party service providers with categories of third parties, consistent with Section 9.
Sec. 6(A)	No exception for proprietary information, so an access request can be used to extract underwriting IP.	Add an exception for trade secrets, proprietary models, scores and algorithm inputs.
Sec. 6(B)	The correction duty displaces the FCRA dispute process and is silent on what a correction means for filed rates and rules.	Route disputes about consumer report information to 15 U.S.C. 1681i, and state that correction does not require retroactive re-rating or deviation from filed rates and rules.
Sec. 6(C), 6(D)	Retention obligations tied to examination and ratemaking are unaddressed, and the draft states there is no cap on requests.	Add retention exceptions for market conduct examination, statistical reporting, actuarial and rate development, reserving and audit, and permit denial of manifestly unfounded, excessive or repetitive requests.

Section	Issue	Proposed amendment
Sec. 5	A 48-hour notice clock and application to vendor contracts already in force. Large infrastructure providers will not repaper.	Use “promptly” or "without unreasonable delay," apply the section only to contracts entered into or renewed after the effective date, and allow a standard data protection addendum to satisfy it.
Art. VIII, nondiscrimination	Does not address the consumer whose deletion or opt-out removes information the licensee needs to underwrite or rate.	Clarify that declining to write, nonrenewing or rating consistent with filed rules is not unfair discrimination where the exercise of a right removes required information.
Art. VIII, individual remedies	None. The provision is correct as drafted.	No change. Retain the disclaimer of a private cause of action through adoption.
Art. VIII, effective date	No implementation runway for Article II, III and IV builds, which are sequential.	Provide 24 months from state adoption, a drafting note urging adoption without state-specific variation, and a safe harbor for licensees in compliance with this regulation.

We appreciate the Working Group's work on this draft and the transparency of the article-by-article process. The Coalition would welcome the chance to walk through these issues with the Working Group before the Fall National Meeting, and we are available to provide drafting support on any item above.

Respectfully submitted,

Jen Crutchfield and Scott Fischer on behalf of the Insurtech Coalition

September 16, 2026

IUA response to the revised exposure draft of the Privacy of Consumer Information Act (Model #672) Issued July 24, 2026

Dear Director Dwyer,

About the IUA

The IUA represents more than 80 international and wholesale insurance and reinsurance companies operating in or through London, many of whom are approved as surplus lines insurers appearing on the NAIC's Quarterly Listing of Alien Insurers. For further information about our organisation and membership, please visit our website.

The IUA exists to promote and enhance the business environment for its members. The IUA's London Company Market Statistics Report shows that overall premium income for the company market in 2025 was £49.206bn. Gross premium written in London totalled £43.658bn while a further £5.548bn was identified as written in other locations but overseen by London operations (of this £49.206bn, £11.656bn represents North American risks, broken down into £9.018bn direct insurance and facultative reinsurance premium and £2.638bn treaty reinsurance premium).

IUA Feedback on the Revised Exposure Draft

The IUA welcomes the opportunity to provide feedback on the proposed changes outlined in the Privacy of Consumer Information Act (Model #672) on behalf of its members ("we"). These are below:

We appreciate the substantial effort undertaken by the Working Group to modernize the Privacy of Consumer Information Act (Act) and to develop a privacy framework that reflects evolving consumer expectations. We also welcome a number of changes made since earlier drafts, such as Article VIII Section 34 which removed the "private cause of action" provision previously raised in our 2023 response.

The IUA supports robust and effective privacy protections for consumers. Our members already operate under comprehensive international data protection frameworks, including the UK and EU GDPR and have extensive experience implementing consumer privacy rights in multiple jurisdictions. Our comments are therefore focused on ensuring that the Act can be implemented effectively within the unique distribution chains of the non-US excess and surplus lines insurers operating in or through the London Market.

Definition of "licensee"

As stated in our previous submission, the IUA recognizes and appreciates the Working Group's efforts to accommodate the surplus lines market. However, we remain concerned that unauthorized insurers continue to be included within the definition of "licensee." Defining unauthorized insurers as “licensees” is inconsistent with other existing state insurance laws where the term “licensee” generally refers only to insurance producers or admitted insurers holding a license or certificate issued by the state insurance department, and not to non-admitted/surplus lines insurers.

In surplus lines transactions, non-US excess and surplus lines insurers operate exclusively through the regulated and licensed surplus lines broker. Therefore, consumer information is typically collected first by retail brokers representing the insured, then shared with surplus lines brokers and finally transmitted through London intermediaries before reaching the unauthorized insurer. Consumers do not interact directly with the unauthorized insurer and will likely be unaware of the identity of all participating insurers, notably in the context of London Market subscription placements. The London Market surplus lines structure differs fundamentally from admitted market transactions, where many of the Act’s notice, opt-out and opt-in provisions may function more effectively in practice.

Accordingly, the IUA continues to support redrafting to reflect that surplus lines brokers remain responsible for the delivery of consumer notices and the administration of consumer privacy rights. We strongly encourage the Working Group to consider removing unauthorized insurers from the definition of "licensee" or otherwise clarifying that insurers receiving information through licensed surplus lines brokers may satisfy their compliance obligations through those brokers or other authorized representatives. This approach would appropriately reflect the movement of information from surplus lines brokers and the London Market, while continuing to safeguard consumer protections.

Consumer Access, Correction and Deletion Rights

The IUA supports the objective of providing consumers with greater transparency and control over their nonpublic personal information. The introduction of Article III Section 6 reflects broader international trends in privacy regulation and is consistent with concepts already applied by IUA members.

However, Article III raises significant practical concerns for the London Market that require further consideration on implementation. Consumer information relating to a single placement may be held by multiple market participants e.g. surplus lines brokers, London brokers, managing general agents, syndicates, coverholders, claims administrators/loss adjusters and reinsurers. Each individual participant will maintain a relevant and limited subset of the overall nonpersonal information relating to a

transaction, determined by their processing activity and legal classification. Without additional clarification or operational hierarchy, consumers are likely to submit multiple requests to numerous market participants and receive inconsistent or incomplete responses. This would result in consumer confusion and unnecessary duplication and administrative burden for non-US excess and surplus lines insurers.

The IUA therefore recommends that the Act expressly permits authorized intermediaries to triage consumer requests and coordinate responses on behalf of participating unauthorized insurers. Such an approach would remove regulatory uncertainty and promote a consistent approach to consumer privacy rights across surplus lines placements.

Consideration should also be given to the practical limitations associated with diverging international data retention obligations with regard to claims files, fraud investigations, sanctions screening and information maintained for reinsurance purposes, where it may not always be legally possible to provide consumer access or deletion rights.

Third-Party Service Provider Requirements

The IUA recognizes the importance of appropriate contractual protections between insurers and third-party service providers. Nevertheless, the requirements in Article II are highly prescriptive and may prove difficult to implement consistently across all types of insurance arrangements, particularly where services are provided through complex international market structures or governed by standardized market agreements.

Many IUA members already operate within robust contractual and regulatory frameworks, including oversight requirements arising under UK GDPR, EU GDPR and applicable operational resilience requirements. The IUA therefore encourages the Working Group to expressly recognize where equivalent contractual protections exist under applicable foreign laws. Such flexibility would achieve the consumer protection objectives of the Act while avoiding unnecessary disruption.

Conclusion

The IUA supports the Working Group's objective of establishing a modern and effective privacy framework for the insurance sector.

At the same time, we would like to stress that many London Market participants remain subject to overlapping and robust privacy obligations in multiple jurisdictions, and do not deal directly with consumers in the United States. We therefore encourage the Working Group to continue seeking alignment, where appropriate, with established international privacy authorities to avoid creating conflicting compliance obligations and duplicative

work that does not take into account the surplus lines broking chain and does not materially enhance consumer protection.

The IUA appreciates the opportunity to comment and would welcome continued engagement with the Working Group as the Act develops.

Yours sincerely,



Christopher Jones

Chief Executive





















September 22, 2026

RE: Joint Trades Concerns with Revised Model 672 to the Privacy Protections (H) Working Group

Dear Chair Dwyer and Vice Chairs Houdek and Cornelius:

The undersigned trade associations appreciate the Working Group's continued efforts to modernize Model 672 and the opportunity to engage throughout this process. Industry has been actively involved since the beginning of these discussions, dedicating significant time and expertise to help identify workable approaches that strengthen consumer privacy protections while preserving consumers' access to affordable, accessible, and innovative insurance products and services. While we appreciate the progress made to date, significant concerns remain across a number of core provisions in the current draft. These concerns are shared broadly across the industry and raise questions about operational feasibility, alignment with existing legal and regulatory frameworks, consumer impacts, and the model's ability to achieve widespread adoption. Our individual comment letters will provide additional detail and, where appropriate, specific drafting suggestions, but we believe it is important to highlight our

collective view that substantial work remains before the draft is ready to move forward. We remain committed to working with the Working Group and stand ready to continue providing feedback to help achieve a workable outcome.

The concerns outlined below represent several of the most significant issues that have consistently surfaced across industry stakeholders during this process. While additional concerns remain and will be addressed in greater detail by individual trades, these issues reflect areas where there is broad industry agreement that further work is needed to improve the draft's workability, implementation, and alignment with existing frameworks before it is ready to advance.

1. **Consumer Definition Expansion:** The current "consumer" definition (and deletion of "customer definition") substantially expand obligations throughout the Model which are inconsistent with current regulation and do not provide meaningful consumer benefits that outweigh the substantial licensee obligation and burden. This includes a specific drafting defect in the Section 4 "Consumer" definition, where the group-participant carve-out disclosure cross-reference was not updated to include new Sections 19–21, and Section 4.G(2)(f)(ii) now directly contradicts Section 4.G(2)(f)(i), together risking inadvertent extension of individual notice and consumer rights to group plan participants, beneficiaries, and other indirect data subjects who have no direct relationship with the licensee.
2. **Access, Correction, Deletion Scope**: Access, correction, and deletion obligations outlined in the draft contain infeasible limits on time for licensees to complete these requests, do not contain any meaningful thresholds on limitations or reasonable time periods, expands obligations beyond what is within licensee control, and pose requirements that would place licensees and insurers overall at risk. While access, correction, and deletion are important to include and there are workable provisions in Section 6, changes to this section are crucial.
3. **Third-Party Service Provider Requirements:** Article II, *Third-Party Service Provider Arrangements* currently requires substantial contract terms that would be infeasible in negotiations with third parties, go beyond the scope of the regulated entity under Model 672, would create substantial operational burdens that do not provide meaningful consumer benefits, and would further stratify the privacy patchwork across states. Without meaningful changes to this section, including deletion of several provisions, this draft would require licensees to become an outlier in the financial services industry and pose great risk to consumers as well. Article II requires meaningful redlines to address the liability standards, contracting burdens, implementation deadlines, and lack of reasonable oversight control.

4. **Sale, Targeted Advertising, and SPI:** In addressing sale, targeted advertising, and sensitive personal information, the draft contains inconsistencies, restrictions beyond GLBA for opt-in that would significantly hinder customer and consumer access to affordable and readily available and accessible products and services, and provides uncertainty for licensees for many operational aspects of business. Without meaningful and considered revisions to Article V, the Model draft will contain likely unintended consequences and harm. Notably, the deviation from an opt-out framework is the basis for a great number of these issues.
5. **Lack of Harmonization and Basis in Existing Frameworks:** Overall, there are opportunities for the draft to modernize while harmonizing with existing, workable provisions demonstrated in GLBA, CCPA, NYDFS regulations, and other modernized data privacy laws. At present, attempts at modernization are not grounded in these existing principles which does not alleviate the patchwork, provides further confusion for consumers, and, in certain sections, requires an infeasible path forward. Revisions are necessary so as not to create a 51st state requirement or an unworkable draft that does not pose a meaningful path toward widespread adoption.
6. **NPI and NPHI Definitions:** The current definitions of nonpublic personal information and nonpublic health information create many implementation issues and should be reevaluated in light of existing frameworks and workability elsewhere in the draft.

As active stakeholders in this process, we appreciate the opportunity to provide these comments and are available to engage in further dialogue regarding these issues.

Sincerely,

American Council of Life Insurers (ACLI)
American Property Casualty Insurance Association (APCIA)
Independent Insurance Agents and Brokers of America (IIABA)
The Committee of Annuity Insurers (CAI)
Consumer Credit Industry Association (CCIA)
The Council of Insurance Agents and Brokers (CIAB)
Insured Retirement Institute (IRI)
National Association of Insurance and Financial Advisors (NAIFA)
National Association of Mutual Insurance Companies (NAMIC)
Wholesale & Specialty Insurance Association (WSIA)

LLOYD'S

August 19, 2026

Re: Revised Exposure Draft of the Privacy of Consumer Information Act (Model #672) Issued July 24, 2026

Dear Director Dwyer:

This comment letter is submitted on behalf of Underwriters at Lloyd's, London ("Lloyd's") in response to the revised exposure draft of the Privacy of Consumer Information Act (Model #672) issued on July 24, 2026. Lloyd's is the largest writer of surplus lines insurance in the United States, writing business in all 50 states through the syndicates appearing on the Quarterly Listing of Alien Insurers maintained by the International Insurers Department of the NAIC. Lloyd's appreciates the considerable time and effort devoted by the Privacy Protections (H) Working Group to modernizing Model #672 and developing a privacy framework that reflects evolving consumer expectations and technological developments.

As we have noted in our prior comment letters, Lloyd's supports strong privacy protections for consumers. The Lloyd's market has long operated under comprehensive privacy requirements in the United Kingdom, including the General Data Protection Regulation (GDPR). Accordingly, Lloyd's does not object to the development of robust privacy standards for the insurance sector. Rather, our comments are focused on ensuring that the model can be implemented effectively across all segments of the insurance marketplace, including the surplus lines market.

We appreciate that the latest exposure draft includes significant revisions intended to address the treatment of excess lines insurers and brokers. In particular, Section 4(N)(3)(b) creates a compliance pathway for excess lines brokers and insurers that satisfy certain conditions. While this addition represents a constructive effort to recognize the unique nature of surplus lines transactions, Lloyd's remains concerned that the continued inclusion of unauthorized insurers within the definition of "licensee" creates structural inconsistencies throughout the model and unnecessary regulatory complexity for surplus lines transactions.

I. Article I, Section 4 - Licensee Definition and Treatment of the Surplus Lines Market

Section 4(N)(3) continues to deem an unauthorized insurer accepting business through a licensed excess lines broker to be a "licensee" for purposes of the Act. Lloyd's respectfully continues to believe that this approach is fundamentally inconsistent with the manner in which surplus lines business is regulated in the United States.

In a surplus lines transaction, the regulated and licensed participant is the surplus lines broker. Consumers do not interact directly with the unauthorized insurer. Rather, the surplus lines broker collects information from the consumer, evaluates placement options, and

communicates with the insurer. This regulatory structure has existed for decades and is reflected throughout state surplus lines laws. Historically, unauthorized insurers have not been treated as licensees under NAIC models because they do not hold certificates of authority or insurance producer licenses issued by the state.

Lloyd's appreciates the Working Group's efforts to address surplus lines concerns through Section 4(N)(3)(b), which establishes a compliance framework for excess lines brokers and insurers that satisfy specified conditions. However, the need for this separate framework underscores the underlying issue created by including unauthorized insurers within the definition of "licensee." The model's notice, opt-out, and opt-in requirements were principally designed for admitted insurance markets in which consumers interact directly with licensed insurers. As a result, Section 4(N)(3)(b) addresses some of the practical consequences of treating unauthorized insurers as licensees but does not resolve the underlying structural inconsistency.

Accordingly, Lloyd's continues to strongly recommend removing unauthorized insurers from the definition of "licensee." A surplus lines insurer that receives nonpublic personal information from a surplus lines broker should instead be treated as a third-party service provider under the Act. This approach would more accurately reflect the actual flow of information in surplus lines transactions, align the Act with the broader framework of insurance regulation, and eliminate the need for specialized exceptions and alternative compliance mechanisms that are necessary only because unauthorized insurers have first been brought within the definition of licensee.

Suggested Edits to Article I, Section 4(N):

N. (1) "Licensee" means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Insurance Law of this state, [and health maintenance organizations holding a certificate of authority pursuant to Section [insert section] of this state's Public Health Law].

(2) A licensee is not subject to the notice and opt out requirements for nonpublic personal information set forth in Articles I, II, III and IV of this Act if the licensee is an employee, agent or other representative of another licensee ("the principal") and:

(a) The principal otherwise complies with, and provides the notices required by, the provisions of this Act; and

(b) The licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates in a manner permitted by this Act.

~~(3) (a) Subject to Subparagraph (b), "licensee" shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but~~

~~only in regard to the excess lines placements placed pursuant to Section [insert section] of this state's laws.~~

~~(b)~~ An excess lines broker ~~or excess lines insurer~~ shall be deemed to be in compliance with the notice and opt out requirements for nonpublic personal information set forth in Articles I, II, III and IV of this Act provided:

(a) ~~(i)~~ The excess lines broker ~~or insurer~~ does not disclose nonpublic personal information of a consumer to nonaffiliated third parties for any purpose, including joint servicing or marketing under Section 22 of this Act, except as permitted by Section 23 or 24 of this Act; and

(b) ~~(ii)~~ The excess lines broker ~~or insurer~~ delivers a notice to the consumer at the time a consumer relationship is established on which the following is printed in 16-point type:

NOTICE OF INFORMATION PRACTICES

"Neither the U.S. brokers that handled this insurance nor the insurers that have underwritten this insurance will disclose nonpublic personal information concerning the buyer to nonaffiliates of the brokers or insurers except as permitted by law."

Drafting Note: References to "excess lines broker" and "excess lines insurer" should be changed as necessary to correspond with the applicable terms used in each state.

II. Article II - Third-Party Service Provider Contract Requirements

The newly proposed third-party service provider provisions in Section 5 impose detailed contractual obligations regarding data processing, deletion, subcontracting, consumer requests, security safeguards, and notice requirements.

Lloyd's agrees that contractual protections are an important component of effective privacy governance. However, the Working Group should recognize that certain insurance relationships, particularly in global insurance and reinsurance markets, involve standardized market arrangements and internationally negotiated agreements that may not always align precisely with the specific contractual provisions contemplated by the model.

Lloyd's encourages the Working Group to confirm that substantial compliance with equivalent contractual requirements, including obligations imposed under applicable foreign privacy laws or regulatory frameworks, may satisfy these requirements. Such flexibility would promote consistency while avoiding unnecessary disruption of longstanding commercial arrangements that already incorporate substantial privacy and security protections.

Suggested Edits to Article II

(C) A Licensee who enters into a contract with a Third-Party Service Provider which contains substantially similar terms shall be deemed to be in compliance with Subsection(A).

III. Article III - Consumer Access, Correction and Deletion Rights

Lloyd's supports the objective of providing consumers with greater transparency and control over their personal information. However, as currently drafted, Article III does not adequately account for the manner in which information is collected, maintained, and shared in the surplus lines market.

In a surplus lines transaction, consumer information is typically collected by a surplus lines broker and then shared with one or more participating insurers. Additionally, due to the nature of wholesale insurance transactions, placements frequently involve multiple brokers. Individual insurers may hold only a portion of the information relating to a placement and receive that information indirectly through intermediaries. As a result, consumers often will not know which entity maintains particular information, which entity is responsible for responding to a request, or whether multiple entities possess the same information.

Without additional clarification, these provisions are likely to create significant consumer confusion, duplication of efforts, and administrative inefficiencies. Consumers may submit identical requests to multiple surplus lines market participants in an effort to identify the appropriate respondent. At the same time, brokers and insurers may independently respond to the same request based on different records, resulting in duplicative requests, inconsistent responses, and uncertainty as to whether a consumer's rights have been fully satisfied. In some circumstances, a consumer could receive conflicting information regarding what data is maintained, corrected, or deleted.

For these reasons, Lloyd's believes Article III will require further drafting to address the realities of surplus lines insurance placements if the proposed edits, outlined above, are not incorporated into the Model Act. If they are not, then at a minimum, the Act should expressly permit licensed surplus lines brokers to coordinate and respond to consumer requests on behalf of participating insurers, or otherwise permit insurers to satisfy their obligations through authorized representatives that maintain the relevant consumer relationship. Such an approach would preserve the substantive consumer rights established by Article III while reducing the likelihood of consumer confusion, duplicative processes, and inconsistent outcomes.

IV. Conclusion

Lloyd’s appreciates the significant efforts undertaken by the Working Group to modernize Model #672 and develop a comprehensive privacy framework for the insurance sector. While the revised exposure draft makes meaningful progress in addressing surplus lines issues, Lloyd's continues to believe that the most effective solution is to remove unauthorized insurers from the definition of “licensee” and instead recognize their role as recipients of information through licensed surplus lines brokers.

Such a change would more accurately reflect the structure of the surplus lines market, reduce regulatory complexity, and allow the Act to achieve its consumer protection objectives without disrupting an important source of insurance capacity.

Lloyd's appreciates the opportunity to provide these comments and would be pleased to discuss them further with the Working Group.

Very truly yours,



Kristi M. Garrett
Associate General Counsel
Lloyd's America, Inc.

cc: Sabrina Miesowitz, General Counsel, Lloyd's America, Inc.

National Association of Mutual Insurance Companies (NAMIC):

PRIVACY OF CONSUMER ~~FINANCIAL AND HEALTH~~ INFORMATION ~~REGULATION~~ACT

Table of Contents

ARTICLE I. GENERAL PROVISIONS

Section 1. ~~Authority~~ Purpose
Section 2. ~~Purpose and~~ Scope and Compliance
Section 3. Rule of Construction
Section 4. Definitions

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS~~PRIVACY AND OPT OUT NOTICES FOR FINANCIAL INFORMATION~~

Section 5. Third-Party Service Provider Arrangements~~Initial Privacy Notice to Consumers Required~~

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7~~6~~. ~~Annual Privacy~~ Initial and Subsequent Delivery Notice of Information Practices to ~~Customers~~ Consumers Required
Section 8~~7~~. ~~Information to be Included in Privacy Notices~~Annual Notice of Information Practices to ~~Customers~~Consumers Required
Section 9~~8~~. ~~Form of Opt Out Notice to Consumers and Opt Out Methods~~Information to be Included in Notices of Information Practices
Section 10~~9~~. ~~Revised Privacy Notices~~Short Form Initial Notice of Information Practices
Section 11~~0~~. Form of Opt-In Notice to Consumers and Opt-In Methods~~Privacy Notices to Group Policyholders~~
Section 12~~1~~. ~~Delivery~~Form of Opt-Out Notice to Consumers and Opt-Out Methods
Section 13. Revised Notice of Information Practices
Section 14. Notice of Information Practices to Group Policyholders
Section 15. Delivery

ARTICLE ~~VIII~~. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL ~~FINANCIAL~~ INFORMATION

Section 16~~2~~. General Rules for Use and Disclosure of Nonpublic Personal Information~~Limitation on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties~~
Section 17~~3~~. Limits on Redisclosure and Reuse of Nonpublic Personal ~~Financial~~ Information
Section 18~~4~~. Limits on Sharing Access ~~Account~~ Number or Access Code Information for Marketing Purposes
Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted Advertising
Section 20. Limits on Sale of Nonpublic Personal Information
Section 21. Limits on Disclosure of Sensitive Personal Information

ARTICLE V[I]. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL ~~FINANCIAL~~ INFORMATION

Section 22~~15~~. Exception to Opt Out Requirements for Disclosure of Nonpublic Personal ~~Financial~~ Information for Service Providers and Joint Marketing
Section 23~~16~~. Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal ~~Financial~~ Information for Processing and Servicing Transactions
Section 24~~17~~. Other Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Information

ARTICLE V[II]. RULES FOR HEALTH INFORMATION

Section 25~~18~~. When Authorization Required for Disclosure of Nonpublic Personal Health Information
Section 26~~19~~. Authorizations
Section 27~~0~~. Authorization Request Delivery
Section 28~~1~~. Relationship to Federal Rules
Section 29~~2~~. Relationship to State Laws

ARTICLE V[III]. ADDITIONAL PROVISIONS

Section 30~~23~~. Protection of Fair Credit Reporting Act
Section 31~~24~~. Nondiscrimination
Section 32~~25~~. Violation
Section 33~~26~~. Severability
Section 34. Individual Remedies
Section 35~~27~~. Effective Date
~~Appendix A Sample Clauses~~
~~Appendix B Federal Model Privacy Form~~

APPENDICES

Appendix A Sample Clauses
Appendix B Federal Model Privacy Form
Model Law Forms

© 202617 National Association of Insurance Commissioners

ARTICLE I. GENERAL PROVISIONS

~~**Section 1. Authority**~~

~~This regulation is promulgated pursuant to the authority granted by Sections [insert applicable sections] of the Insurance Law.~~

Section ~~2~~1. Purpose ~~and Scope~~

~~A.~~ Purpose. This Act~~regulation~~ governs the treatment of nonpublic personal health information and nonpublic personal ~~financial~~ information about individuals by all licensees of the state insurance department. This Act~~regulation~~:

A.~~(1)~~ Requires a licensee to provide notice to individuals about its privacy policies and practices;

B.~~(2)~~ Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal ~~financial~~ information about individuals to affiliates and nonaffiliated third parties; and

C.~~(3)~~ Provides methods for individuals to prevent a licensee from disclosing that information.

Drafting Note: Whether this model is adopted as an Act or Regulation will depend upon individual state law. If a state adopts the model as an Act, reference to the model as an Act should be updated throughout the model.

Section 2. Scope and Compliance

A.~~B.~~ Scope. This Act~~regulation~~ applies to:

(1) Nonpublic personal ~~financial~~ information about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. This ~~regulation~~ Act does not apply to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes; and

(2) All nonpublic personal health information.

B.~~C.~~ Compliance. A licensee domiciled in this state that is in compliance with this Act ~~regulation~~ in a state that has not enacted laws or regulations that meet the requirements of Title V of the Gramm-Leach-Bliley Act (PL 102-106) may nonetheless be deemed to be in compliance with Title V of the Gramm-Leach-Bliley Act in the other state.

Drafting Note: Subsection B~~C~~ is intended to give licensees some guidance for complying with Title V of the Gramm-Leach-Bliley Act in those states that do not have laws or regulations that meet GLBA's privacy requirements.

© 2026~~17~~ National Association of Insurance Commissioners

Section 3. Rule of Construction

The examples in this Act~~regulation~~, the sample clauses in Appendix A, and the Federal Model Privacy Form in Appendix B of this Act~~regulation~~ are not exclusive. Compliance with an example, use of a sample clause, or the Federal Privacy Model Form, to the extent applicable, constitutes compliance with this Act~~regulation~~.

Licensees may rely on use of the Federal Privacy Form in Appendix B, consistent with the attached instructions, as a safe harbor of compliance with the Notice of Information Practices~~privacy notice~~ content requirements of this ~~regulation~~Act.

Use of the Federal Model Privacy Form is not required. Licensees may continue to use other types of privacy notices, including notices that contain the examples in this ~~regulation~~ Act and/or the sample clauses in Appendix A, provided that such notices accurately describe the Licensee's privacy practices and otherwise meet the notice content requirements of this ~~regulation~~Act. ~~However, while Licensees may continue to use privacy notices that contain the examples in this regulation and/or the sample clauses in Appendix A, Licensees may not rely on use of privacy notices with the sample clauses in Appendix A as a safe harbor of compliance with the notice content requirements of this regulation after July 1, 2019.~~

~~**Drafting Note:** Safe harbor of compliance with this regulation Act for use of sample clauses in Appendix A sunsets on July 1, 2019.~~

Section 4. Definitions

As used in this Act~~regulation~~, unless the context requires otherwise:

A. "Affiliate" means a company that controls, is controlled by or is under common control with another company.

B. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

C~~B~~. (1) "Clear and conspicuous" means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) Examples.

(a) Reasonably understandable. A licensee makes its notice reasonably understandable if it:

(i) Presents the information in the notice in clear, concise sentences, paragraphs and sections;

(ii) Uses short explanatory sentences or bullet lists whenever possible;

(iii) Uses definite, concrete, everyday words and active voice whenever possible;

Commented [LS1]: NAMIC recommends that the definition of "biometric data" be consistent with other state privacy law definitions.

For comparison, the VCDPA (§ 59.1-575) defines biometric data as automatically measured biological-characteristic information used for identification, and it excludes physical/digital photographs, audio/video recordings, and data derived from them, with an additional HIPAA carve-out. Draft MDL 672 is broadly similar, but it would likely include photo/video/audio-derived data when generated to identify a specific individual, and it does not reflect the HIPAA carve-out.

© 2026~~17~~ National Association of Insurance Commissioners

(iv) Avoids multiple negatives;

(v) Avoids legal and highly technical business terminology whenever possible; and

(vi) Avoids explanations that are imprecise and readily subject to different interpretations.

(b) Designed to call attention. A licensee designs its notice to call attention to the nature and significance of the information in it if the licensee:

(i) Uses a plain-language heading to call attention to the notice;

(ii) Uses a typeface and type size that are easy to read;

(iii) Provides wide margins and ample line spacing;

(iv) Uses boldface or italics for key words; and

(v) In a form that combines the licensee's notice with other information, uses distinctive type size, style, and graphic devices, such as shading or sidebars.

(c) Notices on web sites. If a licensee provides a notice on a web page, the licensee designs its notice to call attention to the nature and significance of the information in it if the licensee uses text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks or sound) do not distract attention from the notice, and the licensee either:

(i) Places the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(ii) Places a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

D~~C~~. "Collect" means to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

E~~D~~. "Commissioner" means the chief insurance regulatory official ~~commissioner~~ of the state.

Drafting Note: Use the title of the chief insurance regulatory official wherever the term "commissioner" appears. If the jurisdiction of certain health licensees, such as health maintenance organizations, lies with some state agency other than the insurance department, or if there is dual regulation, a state should add language referencing that agency to ensure the appropriate coordination of responsibilities.

F~~E~~. "Company" means a corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.

G~~F~~. (1) "Consumer" means an individual who seeks to obtain, obtains or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, and about whom the licensee has nonpublic personal information, or that individual's legal representative.

(2) Examples.

(a) An individual who provides nonpublic personal information to a licensee in connection with obtaining or seeking to obtain financial, investment or economic advisory services relating to an insurance product or service is a consumer regardless of whether the licensee establishes an ongoing advisory relationship.

(b) An applicant for insurance prior to the inception of insurance coverage is a licensee's consumer.

(c) An individual who is a consumer of another financial institution is not a licensee's consumer solely because the licensee is acting as agent for, or provides processing or other services to, that financial institution.

(d) An individual is a licensee's consumer if:

(i) (I) The individual is a beneficiary of a life insurance policy underwritten by the licensee;

(II) The individual is a claimant under an insurance policy issued by the licensee;

(III) The individual is an insured or an annuitant under an insurance policy or an annuity, respectively, issued by the licensee; or

(IV) The individual is a mortgagor of a mortgage covered under a mortgage insurance policy; and

(ii) The licensee discloses nonpublic personal ~~financial~~ information about the individual to a nonaffiliated third party other than as permitted under Sections ~~15, 16 and 17~~22, 23, and 24 of this ~~regulation~~Act.

(e) Provided that the licensee provides the initial, annual and revised notices under Sections ~~10~~ 7, 8, and 13 of this ~~regulation~~ Act to the plan sponsor, group or blanket insurance policyholder or group annuity contractholder, or workers' compensation policyholder, and further provided that the licensee does not disclose to a nonaffiliated third party nonpublic personal financial information about an individual described in Item (i), (ii) or (iii), other than as permitted under Sections ~~15, 16 and 17~~22, 23, or 24 of this ~~regulation~~Act, such an individual is not the consumer of the licensee solely because he or she is:

(i) A participant or a beneficiary of an employee benefit plan that the licensee administers or sponsors or for which the licensee acts as a trustee, insurer or fiduciary;

(ii) Covered under a group or blanket insurance policy or group annuity contract issued by the licensee; or

(iii) A claimant covered by a workers' compensation plan.

Drafting Note: In states where the workers' compensation self-insurance or workers' compensation state fund coverage is outside the commissioner's jurisdiction, regulators may wish to urge the applicable agency or agencies to promulgate a regulation similar to this ~~regulation~~ Act in order to ensure parity in treatment of workers' compensation plans and to ensure that all workers covered by such plans have privacy protections.

(f) (i) The individuals described in Subparagraph (e)(i) through (iii) of this paragraph are consumers of a licensee if the licensee does not meet all the conditions of Subparagraph (e).

(ii) In no event shall the individuals, solely by virtue of the status described in Subparagraph (e)(i) through (iii) above, be deemed to be ~~customers~~ consumers for purposes of this ~~regulation~~Act.

(g) An individual is not a licensee's consumer solely because he or she is a beneficiary of a trust for which the licensee is a trustee.

(h) An individual is not a licensee's consumer solely because he or she has designated the licensee as trustee for a trust.

H~~G~~. "Consumer reporting agency" has the same meaning as in Section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

I~~H~~. "Control" means:

(1) Ownership, control or power to vote twenty-five percent (25%) or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

(2) Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or

(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the commissioner determines.

~~I. "Customer" means a consumer who has a customer relationship with a licensee.~~

~~J. (1) "Customer relationship" means a continuing relationship between a consumer and a licensee under which the licensee provides one or more insurance products or services to the consumer that are to be used primarily for personal, family or household purposes.~~

~~(2) Examples.~~

Commented [LS2]: NAMIC recommends that the Model align with traditional GLBA designations of consumers and customers, rather than having the focus be on "consumers" as defined. As such, we suggest that "customer" be a defined term and the customer/consumer distinction be utilized throughout the Model as it is in the Model's current form.

~~(a) A consumer has a continuing relationship with a licensee if:~~

~~(i) The consumer is a current policyholder of an insurance product issued by or through the licensee; or~~

~~(ii) The consumer obtains financial, investment or economic advisory services relating to an insurance product or service from the licensee for a fee.~~

~~(b) A consumer does not have a continuing relationship with a licensee if:~~

~~(i) The consumer applies for insurance but does not purchase the insurance;~~

~~(ii) The licensee sells the consumer airline travel insurance in an isolated transaction;~~

~~(iii) The individual is no longer a current policyholder of an insurance product or no longer obtains insurance services with or through the licensee;~~

~~(iv) The consumer is a beneficiary or claimant under a policy and has submitted a claim under a policy choosing a settlement option involving an ongoing relationship with the licensee;~~

~~(v) The consumer is a beneficiary or a claimant under a policy and has submitted a claim under that policy choosing a lump sum settlement option;~~

~~(vi) The customer's policy is lapsed, expired or otherwise inactive or dormant under the licensee's business practices, and the licensee has not communicated with the customer about the relationship for a period of twelve (12) consecutive months, other than annual privacy notices, material required by law or regulation, communication at the direction of a state or federal authority, or promotional materials;~~

~~(vii) The individual is an insured or an annuitant under an insurance policy or annuity, respectively, but is not the policyholder or owner of the insurance policy or annuity; or~~

~~(viii) For the purposes of this regulation, the individual's last known address according to the licensee's records is deemed invalid. An address of record is deemed invalid if mail sent to that address by the licensee has been returned by the postal authorities as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.~~

J. "De-identified data" means information that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual.

Commented [LS3]: NAMIC recommends that the definition for "De-identified data" be edited for consistency with other state privacy laws.

For comparison, under the VCDPA, de-identified data generally depends on whether it can be reasonably linked to an identified or identifiable person (or device). Here, under MDL 672, de-identification additionally turns on whether the data can reasonably be used to infer information about the person and/or otherwise be linked, which could be a stricter and potentially more subjective standard.

K. (1) "Financial institution" means any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 1843(k)(4)(B) ~~4(k)~~ of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial institution does not include:

(a) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 *et seq.*);

(b) The Federal Agricultural Mortgage Corporation or any entity charged and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*); or

(c) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as the institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

L. (1) "Financial product or service" means a product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 1843(k)(4)(B) ~~4(k)~~ of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.

~~M. "Health care" means:~~

~~(1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, services, procedures, tests or counseling that:~~

~~(a) Relates to the physical, mental or behavioral condition of an individual; or~~

~~(b) Affects the structure or function of the human body or any part of the human body, including the banking of blood, sperm, organs or any other tissue; or~~

~~(2) Prescribing, dispensing or furnishing to an individual drugs or biologicals, or medical devices or health care equipment and supplies.~~

~~N. "Health care provider" means a physician or other health care practitioner licensed, accredited or certified to perform specified health services consistent with state law, or a health care facility.~~

M~~P~~. ~~(1)~~ "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.

Commented [LS4]: NAMIC requests clarification on whether the removal of the "health care" definition was intended to narrow or to broaden the applicable scope.

~~(2) Insurance service includes a licensee's evaluation, brokerage or distribution of information that the licensee collects in connection with a request or an application from a consumer for a insurance product or service.~~

~~Q~~N. (1) "Licensee" means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Insurance Law of this state, [and health maintenance organizations holding a certificate of authority pursuant to Section [insert section] of this state's Public Health Law].

Drafting Note: Add bracketed language if HMOs are licensed under other than insurance statutes and cite appropriate state law.

(2) A licensee is not subject to the notice and opt out requirements for nonpublic personal ~~financial~~ information set forth in Articles I, II, III and IV of this ~~regulation~~ Act if the licensee is an employee, agent or other representative of another licensee ("the principal") and:

(a) The principal otherwise complies with, and provides the notices required by, the provisions of this ~~regulation~~Act; and

(b) The licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates in a manner permitted by this ~~regulation~~Act.

(3) (a) Subject to Subparagraph (b), "licensee" shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only in regard to the excess lines placements placed pursuant to Section [insert section] of this state's laws.

(b) An excess lines broker or excess lines insurer shall be deemed to be in compliance with the notice and opt out requirements for nonpublic personal ~~financial~~ information set forth in Articles I, II, III and IV of this ~~regulation~~ Act provided:

(i) The broker or insurer does not disclose nonpublic personal information of a consumer ~~or a customer~~ to nonaffiliated third parties for any purpose, including joint servicing or marketing under Section 22~~15~~ of this ~~regulation~~Act, except as permitted by Section 23~~16~~ or 24~~17~~ of this ~~regulation~~Act; and

(ii) The broker or insurer delivers a notice to the consumer at the time a ~~customer~~ consumer relationship is established on which the following is printed in 16-point type:

NOTICE OF INFORMATION PRACTICES~~PRIVACY NOTICE~~

"Neither the U.S. brokers that handled this insurance nor the insurers that have underwritten this insurance will disclose nonpublic personal information concerning the buyer to nonaffiliates of the brokers or insurers except as permitted by law."

Commented [LS5]: Because the definition and examples of what constitutes "insurance service" were removed, NAMIC requests clarification on the intended scope and how ambiguity is expected to be handled in practice.

Drafting Note: References to "excess lines broker" and "excess lines insurer" should be changed as necessary to correspond with the applicable terms used in each state.

~~R~~O. (1) "Nonaffiliated third party" means any person except:

(a) A licensee's affiliate; or

(b) A person employed jointly by a licensee and any company that is not the licensee's affiliate (but nonaffiliated third party includes the other company that jointly employs the person).

(2) Nonaffiliated third party includes any company that is an affiliate solely by virtue of the direct or indirect ownership or control of the company by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

P. "Nonpublic personal h~~H~~ealth information" means any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of an individual;

(2) The provision of health care to an individual; or

(3) Payment for the provision of health care to an individual.

Q~~S~~. "Nonpublic personal information" means ~~nonpublic personal financial information and nonpublic personal health information.~~any personally identifiable information that is linked or reasonably linkable to an identified natural person. Nonpublic personal information does not include de-identified data or publicly available information.

~~T. (1) "Nonpublic personal financial information" means:~~

~~(a) Personally identifiable financial information; and~~

~~(b) Any list, description or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.~~

~~(2) Nonpublic personal financial information does not include:~~

~~(a) Health information;~~

~~(b) Publicly available information, except as included on a list described in Subsection T(1)(b) of this section; or~~

~~(c) Any list, description or other grouping of consumers (and publicly available~~

~~information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.~~

~~(3) Examples of lists.~~

~~(a) Nonpublic personal financial information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information that is not publicly available, such as account numbers.~~

~~(b) Nonpublic personal financial information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived in whole or in part using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.~~

~~U. "Nonpublic personal health information" means health information:~~

~~(1) That identifies an individual who is the subject of the information; or~~

~~(2) With respect to which there is a reasonable basis to believe that the information could be used to identify an individual.~~

RV. (1) "Personally identifiable ~~financial~~ information" means any information:

(a) A consumer provides to a licensee to obtain an insurance product or service from the licensee;

(b) About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

(c) The licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.

(2) Examples.

(a) Information included. Personally identifiable ~~financial~~ information includes:

(i) Information a consumer provides to a licensee on an application to obtain an insurance product or service;

(ii) Account balance information and payment history;

(iii) The fact that an individual is or has been one of the licensee's consumers~~ustomers~~ or has obtained an insurance product or service from the licensee;

(iv) Any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer;

(v) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;

(vi) Any information the licensee collects through an Internet cookie (an information-collecting device from a web server); and

(vii) Information from a consumer report.

(b) Information not included. Personally identifiable ~~financial~~ information does not include:

~~(i) Health information;~~

(i~~i~~) A list of names and addresses of customers of an entity that is not a financial institution; and

(ii~~i~~) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.

S~~X~~. "Opt in" means an affirmative direction by a consumer that authorizes a licensee to disclose the consumer's information.

T~~X~~. "Opt out" means a direction by a consumer that the licensee may not disclose nonpublic personal information about the consumer to a nonaffiliated third party, except as permitted under Sections 22,23, or 24 ~~15, 16, 17, and 18~~.

U~~W~~. (1) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

(a) Federal, state or local government records;

(b) Widely distributed media; or

(c) Disclosures to the general public that are required to be made by federal, state or local law.

(2) Reasonable basis. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

(a) That the information is of the type that is available to the general public; and

(b) Whether an individual can direct that the information not be made available to the general public and, if so, that the licensee's consumer has not done so.

(3) Examples.

(a) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(b) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(c) Reasonable basis.

(i) A licensee has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(ii) A licensee has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the licensee has located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

V. "Reasonable opportunity" means any of the following:

(1) ~~(a)~~ The licensee mails the notices required to the consumer and allows the consumer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within sixty (60) days from the date the licensee mailed the notices;

(2) ~~(b)~~ Where a consumer agrees to receive the notices required by this Act electronically in accordance with UETA [insert state electronic transactions act statute], the licensee allows the consumer to opt out by any reasonable means at any time;

(3) The licensee makes the privacy policy available on the licensee's website and allows the consumer to opt out by any reasonable means at any time; or

Commented [LS6]: NAMIC recommends allowing for the posting of and access by a consumer to the privacy policy on the licensee's website as a "reasonable opportunity."

(4) ~~(c)~~ For an isolated transaction, such as providing the consumer with an insurance quote, the licensee provides the notices required by this Act at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction.

X. ~~-~~"Sale" or "selling" means the exchange of nonpublic personal information for monetary ~~or other valuable~~ consideration. A licensee does not sell nonpublic personal information when:

Commented [LS7]: Exchanging data for any valuable consideration can be challenging to analyze in practice; as such, NAMIC recommends that the definition of sale be focused on exchange of data for monetary consideration.

(1) The disclosure is to a third party for the purpose of or in support of providing a product

or service for ~~requested by~~ the consumer.

~~(1)~~(2) A licensee provides information to or receives anything of value from an insurance support organization, statistical agent, or reinsurer;

~~(2)~~(3) A licensee provides nonpublic personal information to an affiliate or to a financial institution with which the licensee performs joint marketing;

~~(3)~~(4) The business transfers to a third party the nonpublic personal information as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction in which the party assumes control of all or part of the licensee's assets; ~~or~~

(5) A consumer uses or directs the business to (i) disclose nonpublic personal information; or (ii) interact with one or more third parties including but not limited to referrals to other licensees;

(6) A licensee discloses or makes available nonpublic personal information as reasonably necessary to detect, prevent, investigate, or respond to fraud, misrepresentation, unauthorized activity, security incidents, identity theft, abuse, or other unlawful conduct, including through insurance support organizations, anti-fraud databases, vendors, investigators, reinsurers, statistical agents, or other persons as permitted by law.~~.~~

Drafting Note: States have their own definitions of fraud, and should therefore include and point to that statutory reference in the fraud related provisions within this Draft so as to avoid inadvertent conflicts or discrepancies.

Y. "Sensitive Personal Information" means personally identifiable "nonpublic personal information" about a consumer that includes:

(1) Racial or ethnic origin, religious beliefs, sexual orientation, or citizenship or citizenship status; or

(2) Genetic information or biometric data that may be processed for the purpose of uniquely identifying an individual.

Z. (1) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests.

(2) "Targeted advertising" does not include:

(a) Online advertisements based on activities within a Licensee's own websites or online applications;

(b) Online advertisements based on the context of a consumer's current search query, visit to a website, or online application;

(c) Online advertisements directed to a consumer in response to the consumer's request for information or feedback; or

Commented [LS8]: NAMIC suggests revising this aspect of the "sale" definition to "for the consumer." There may be situations where disclosures occur based on a contract, direct mailing, or otherwise, but the customer/consumer did not actually request or trigger the disclosure.

Commented [LS9]: NAMIC suggests this inclusion because anti-fraud programs often involve vendors, insurance support organizations, databases, investigators, analytics providers, and consortium arrangements where fees or other value may be exchanged, but the purpose is fraud control and consumer/business protection, not monetization of consumer information.

Commented [LS10]: To ensure alignment with state laws and fraud definitions therein, NAMIC suggests this drafting note to allow states to specifically reference and incorporate their fraud statutory references.

(d) Processing Nonpublic Personal Information solely for measuring or reporting advertising performance, reach, or frequency.

AA. "Third party service provider" or "third party" means a person or entity not otherwise defined as a licensee or affiliate of a licensee that:

(1) Provides services to the licensee; and

(2) Maintains, processes or otherwise is permitted access to nonpublic personal information through its provisions of services to the licensee.

(3) For purposes of this definition, a person or entity does not become a third-party service provider solely because the licensee discloses nonpublic personal information to that person or entity at the direction of, with the authorization of, or to facilitate a transaction, claim, repair, replacement, payment, benefit, service, or other activity requested by or benefitting the consumer, where the person or entity is providing goods or services to the consumer and not to or on behalf of the licensee.

Commented [LS11]: NAMIC recommends this clarification, as there is ambiguity when reading the current TPSP definition in the context of Article II, especially when licensees are dealing with consumer selected repair facilities, medical providers, contracts, rental companies, or otherwise.

© 2026~~17~~ National Association of Insurance Commissioners

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS
~~**PRIVACY AND OPT_OUT NOTICES FOR FINANCIAL INFORMATION**~~

Section 5. Third-Party Service Provider Arrangements

A. Contract Requirements.

A licensee that discloses a consumer's nonpublic personal information to a third-party service provider shall enter into a written contract with the third-party service provider that:

(1) Prohibits the third-party service provider from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless processing is necessary to comply with the law or a valid and binding order of a governmental body, in which case the third-party service provider must notify the licensee within 48 hours unless prohibited by law;

(2) Requires the third-party service provider to delete, destroy, de-identify or return all nonpublic personal information to the licensee when requested by the licensee; or to delete nonpublic personal information after it is no longer necessary to fulfill a legal requirement or to meet the record retention requirements of the licensee or third-party service provider, and to notify the licensee of the action taken;

(3) Requires the third-party service provider to notify the licensee if it can no longer comply with its obligations under this contract and provides the licensee with a right to terminate the contract;

(4) Requires that any contract between a third-party service provider and a subcontractor with access to a consumer's nonpublic personal information must contain provisions no less protective of nonpublic personal information than those contained in the third-party service provider's agreement with the licensee;

(5) Requires the third-party service provider to provide assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act;

(6) Requires the third-party service provider to implement and maintain administrative, technical, and physical data security practices to protect the nonpublic personal information from unauthorized access, destruction, use, modification, or disclosure;

(7) Requires the third-party service provider to notify the licensee of a failure to meet the obligations of Subsections (1) to (6) above within 48 hours of discovery by the third-party service provider.

B. A licensee that discloses a consumer's nonpublic personal information to a third-party service provider remains fully responsible for compliance with this Act and the handling of nonpublic personal information.

Drafting Note: The written contract requirement applies to persons or entities that provide services to or on behalf of the licensee and have access to nonpublic personal information through those services. It is not intended to require a written third-party service provider contract solely because a licensee discloses nonpublic personal information to a person or entity selected, directed, authorized, or otherwise engaged by the consumer to

Commented [LS12]: NAMIC asks the Working Group to consider "promptly and without unreasonable delay."

Commented [LS13]: NAMIC requests clarification on the difference between sub (3) noncompliance with the full contract and sub (7) noncompliance with portions of the contract. What is the practical and legal distinction?

Commented [LS14]: NAMIC suggests that sub (7) may also be duplicative of sub (3), which already covers security incidents or breaches in contracts where data is actually exposed.

Commented [LS15]: NAMIC encourages the Working Group to consider edits to, and reevaluate, this provision. Insurers generally allocate TPSP financial responsibility for breaches in standard contract language. If insurance regulators do not have regulatory authority directly over TPSPs, it is unclear whether it would be appropriate or enforceable to add liability provisions in the Model directly applicable to TPSPs.

Also, while the insurer contract language may cover these requirements in substance, the Model's format may create ambiguity. For instance, a regulator may not be able to enforce noncompliance if substance is covered but the specific form is not prescribed.

facilitate a claim, payment, repair, replacement, benefit, or other transaction, unless that person or entity is also providing services to or on behalf of the licensee.

Commented [LS16]: NAMIC recommends inclusion of this drafting note for clarity.

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

A. A consumer may file the following requests with a licensee, which shall be processed in accordance with the following standards:

(1) Within 45 days of receiving an authenticated request from a consumer for their nonpublic personal information, a licensee shall disclose:

(a) All nonpublic personal information about the consumer that is maintained by the licensee or any contracted third-party service provider; and

(b) ~~A list~~Categories of all third-party service providers to whom the licensee disclosed the consumer's nonpublic personal information.

(2) A consumer may request nonpublic personal information, except the following: ~~licensee shall not be required to disclose the following:~~

(a) A consumer's Social Security Number, driver's license number or other government-issued identification number, financial account number(s), any health insurance or medical identification number, any account password(s), security questions and answers, unique biometric data or other information that could create a high risk of identity theft. The licensee may instead disclose the types of nonpublic personal information maintained by listing each type of nonpublic personal information it has about the consumer;

(b) Duplicative nonpublic personal information, if it is described in a manner reasonably understandable by the consumer and the consumer is offered an opportunity to review the nonpublic personal information for inconsistencies; or

(c) Information that is outside the scope of the request, if the consumer has requested only specified items or categories of information.

B. Correction of nonpublic personal information.

(1) A consumer may make an authenticated request for the correction of their nonpublic personal information by filing a request with the licensee that:

(a) Identifies the specific nonpublic personal information the consumer wishes to correct; and

(b) Provides an explanation of why the nonpublic personal information is incorrect.

(2) Within 45 days of receipt of the request under this subsection, a licensee shall take one of the following actions and notify the consumer:

Commented [LS17]: NAMIC recommends changing s. 6(A)(1)(b) to requiring categories rather than a list enumerating all of the TPSPs, as this change better benefits the industry and consumers.

First, a list of all TPSPs could be extensive and not meaningful to a consumer, but instead may invite confusion about a complex industry.

Second, categories are the norm for those jurisdictions that have this requirement today like the CCPA or GDPR; NAMIC recommends not going beyond what CCPA or GDPR require.

Third, requiring categories in place of an enumerated list better protects licensees against cyber threats or competition impacts. Having a list of vendors from one or many licensees may present an opportunity for a bad actor to use for developing insights into a licensee's operations or systems, or for scanning multiple licensees' approaches to create a cyber roadmap for exploiting a vulnerability by targeting critical service providers. Separately, through accessing an extensive list of vendors, competitors may be able to see what specific tasks are handled in-house vs. those that are outsourced, and piece together aspects of other's strategic approaches and partnerships, which does not benefit the marketplace.

Commented [LS18]: NAMIC suggests this verbiage change to avoid confusion due to Sec. 6(A)(1), which directs consumers to make requests, but later sections narrow what can be requested. Such framework could place insurers and consumers in an adversarial position and likely increase consumer complaints needlessly.

(a) Correct the nonpublic personal information in dispute as requested by the consumer;

(b) Delete the nonpublic personal information in dispute; or

(~~b~~c) Deny the request and provide:

(i) The basis for refusal to correct the nonpublic personal information as requested;

(ii) Information about how the consumer may appeal the denial; and

(iii) An explanation of how the appeal will be reviewed and how the consumer will be notified of the decision on appeal.

(3) A licensee may deny a request for correction if:

(a) The nonpublic personal information is accurate and complete and if the licensee provides a process for appeal of the decision; or

(b) The nonpublic personal information that is the subject of the request was not created by the licensee, unless there is a reasonable basis to believe that the originator of the nonpublic personal information is no longer available to act on the requested correction, and the consumer has independently demonstrated the information is incorrect.

(4) A licensee may delay fulfilling a consumer's request, up to 45 days, to correct nonpublic personal information, depending on the complication of the consumer request. A licensee must notify the consumer of such delay.

C. Deletion of nonpublic personal information.

(1) Within 45 days of an authenticated request from a consumer, a licensee shall delete the nonpublic personal information about the consumer that is maintained by the licensee or direct a third-party service provider to delete the nonpublic personal information on the licensee's behalf, unless notifying those third parties proves impossible or involves disproportionate effort.

(2) The licensee is not required to delete nonpublic personal information if:

(a) The licensee is required by law or regulation to retain the nonpublic personal information;

(b) The nonpublic personal information may be necessary to perform the contract or service requested by or benefiting the consumer;

(c) The information is necessary to comply with a legal obligation; ~~or~~

(d) The information is maintained in reasonable anticipation of a claim or civil or criminal proceeding;~~.~~

Commented [LS19]: There is a 45-day extension for deletion, but not currently for correction or access. Depending on how complicated the request, there could be a need to extend correction or access.

Other privacy laws allow for such extension, so NAMIC recommends this addition for consistency purposes. For instance, in VCDPA, the response period may be extended once by 45 additional days when reasonably necessary (considering complexity and number of consumer requests), if the controller informs the consumer within the initial 45-day period and provides reasons for the extension.

Commented [LS20]: NAMIC recommends this inclusion to more closely match the exception allowed for in CCPA.

Commented [LS21]: NAMIC suggests that the limits on the consumer's right to delete should align with other laws like the CCPA, and suggests these additions to be both operationally feasible and to balance the licensee's needs with consumer rights.

(e) The information is publicly available;

(f) The information is needed for business security purposes;

(g) The information is kept for internal uses that are compatible with reasonable consumer expectations or the context in which the information was provided;

(h) The information is necessary to detect, prevent, investigate, or respond to fraud, misrepresentation, unauthorized activity, security incidents, or other unlawful conduct; or

Drafting Note: States have their own definitions of fraud, and should therefore include and point to that statutory reference in the fraud related provisions within this Draft so as to avoid inadvertent conflicts or discrepancies.

Commented [LS22]: To ensure alignment with state laws and fraud definitions therein, NAMIC suggests this drafting note to allow states to specifically reference and incorporate their fraud statutory references.

(i) The information is housed on backup media, and thus the obligation to delete will either be observed when the backup is restored for a business reason, or the backup media are wiped clean in the ordinary course.

(3) A licensee may delay fulfilling a consumer's request, ~~up to 45 days~~until the archived or backup system is restored to an active system or is next accessed or used for a sale, disclosure, or other business or operational purpose, to delete nonpublic personal information stored on an archived or backup system. A licensee must notify the consumer of such delay.

Commented [LS23]: Deletion within 45 days from an archived or backup system may be impractical and appears to go further than even the approach taken under CCPA/CPRA; as such NAMIC suggests this change.

D. Request and Response Procedures

(1) Except as provided in Subsection D(1)(b), a licensee shall respond to requests submitted under this section within 45 days in the following manner:

Commented [LS24]: NAMIC notes that this timeframe should allow for a 45 calendar day extension when necessary, with the licensee providing explanation for the extension.

(a) A licensee may use its secure communications portal to authenticate requests from consumers holding current accounts with the licensee, unless the licensee has reason to believe the request has been submitted through an account that has been compromised. Otherwise, the licensee may use methods that are commercially reasonable, but not unduly burdensome, to authenticate the identity of the person making the request and to verify that this person is either:

(i) The consumer;

(ii) A person acting with the consumer's written authorization, including but not limited to a valid power of attorney;

Commented [LS25]: NAMIC requests that the Working Group provide clarification and definition for what constitutes "written authorization."

(iii) The parent or legal guardian of a consumer who is a minor, except where the information relates to health insurance claims in circumstances where the child has a legal right to obtain the services in question without the parent's or guardian's consent;

(iv) The legal guardian or other person authorized by law to act on behalf of an incapacitated consumer; or

(v) The personal representative or other person authorized by law to act on behalf of a deceased consumer.

(b) A licensee is required to notify the consumer if either of the following prevents the licensee from complying with the request:

(i) The specific nonpublic personal information at issue is not locatable or retrievable by the licensee; or

Drafting Note: Examiners should review licensees' notifications to consumers regarding nonpublic personal information that is not locatable or retrievable by the licensee and its justifications for irretrievability during Market Conduct and/or IT Exams.

(ii) The licensee is unable to verify the request after requesting that the consumer provide additional information necessary to authenticate the identity of the consumer and authenticate the consumer's request.

(c) If a licensee declines the consumer's request, the licensee shall inform the consumer of the basis for declining the request and provide instructions for how to request review of the decision.

(2) There shall be ~~no~~a cap on the number of requests to correct or delete nonpublic personal information~~.~~. A licensee may deny a repetitive or duplicative request for correction or deletion if the licensee has previously responded to a substantially similar request from the same consumer within the preceding twelve months and the consumer does not identify new or materially different nonpublic personal information, a material change in circumstances, or other facts showing that the request should be reconsidered. The licensee shall provide the consumer with a written explanation of the basis for the denial and information about any available appeal process

(3) If a licensee denies a consumer's request to correct nonpublic personal information, the licensee shall maintain a record of the consumer's correction request and the licensee's basis for denial. The licensee shall associate the consumer's dispute with the disputed nonpublic personal information in a manner reasonably designed to alert future users of the information that the consumer disputes its accuracy, but shall not be required to annotate every duplicate instance of the information maintained across separate systems, records, or archives if a reasonably accessible dispute record or system-level indicator is maintained.

~~If a consumer disagrees with a licensee's refusal to correct or delete nonpublic personal information per the consumer's request, the consumer shall be permitted to file with the licensee:~~

~~(a) A concise statement setting forth why the consumer disagrees with the licensee's refusal and what the consumer thinks is the correct, relevant or fair information; and~~

(a~~b~~) The licensee shall maintain the statement with the disputed nonpublic personal information for a period of 5 years and allow anyone reviewing the disputed nonpublic personal information to be made aware of the dispute and have access to the consumer's statement.

Commented [LS26]: While NAMIC appreciates the intent to not limit the number of requests, such unlimited ability may also be ripe for abuse. As such, we recommend this wording which protects consumers but also addresses repetitive, excessive, or abusive requests.

Commented [LS27]: NAMIC suggests this clarification. As currently drafted, the language could be read to require a licensee to annotate every system, policy record, claim file, complaint file, DSAR record, and duplicate instance where the disputed information appears. For insurers, disputed information may exist across multiple policy, billing, underwriting, claims, complaint, litigation, fraud, archival, vendor, and privacy request systems. A more practical approach would require the licensee to maintain a reasonably accessible record of the consumer's dispute and associate or link that dispute to the disputed information in a manner reasonably designed to alert future users that the consumer disputes its accuracy.

Commented [LS28]: NAMIC requests narrowing Section 6(D)(3) so that the dispute statement is maintained and accessible only to persons/entities that:

- receive or use the disputed nonpublic personal information for a purpose that would be affected by accuracy; and
- have a legitimate need to know for compliance/processing.

This avoids turning licensees into general dispute arbitrators or distribution hubs.

Commented [LS29]: NAMIC suggests that a clear period be included for how long licensees are to keep this information. Not having such limitation implies licensees will need to keep tit indefinitely; the record could contain NPI and would go against the spirit of the law if licensees must retain it indefinitely.

ARTICLE IV.——— NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7~~8~~5. Initial and Subsequent Delivery Notice of Information Practices~~Privacy Notice~~ to Consumers Required

A. Initial Delivery of Notice~~notice requirement~~. A licensee shall provide a clear and conspicuous notice that accurately reflects its privacy policies and practices to~~:~~ all consumers no later than when the licensee obtains access to the consumer's nonpublic personal information, except that a licensee may provide the initial notice within a reasonable time after access to the consumer's nonpublic personal information if:

(1) Obtaining access to the consumer's nonpublic personal information is not at the consumer's election and the licensee follows the Notice of Information Practices previously sent to the consumer; or

(2) Providing notice when the licensee obtains access to the consumer's nonpublic personal i~~n~~formation would substantially delay the consumer's transaction and the consumer agrees to receive the notice at a later time.

B. Subsequent Delivery of Notice

When a consumer with an existing relationship with a licensee obtains a new insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, the licensee satisfies the initial notice requirements of Subsection A of this section as follows:

(1) The licensee may provide a revised notice, under Section 13 , that covers the consumer's new insurance product or service; or

(2) If the initial, revised or annual notice that the licensee most recently provided to that consumer was accurate with respect to the new insurance product or service, the licensee does not need to provide a new notice of information practices under Subsection A of this section.

C. For purposes of this section:

(1) "Not at consumer's election" includes the scenario where a licensee acquires or is assigned a consumer's policy from another financial institution or residual market mechanism and the consumer does not have a choice about the licensee's acquisition or assignment.

(2) "Substantially delay the consumer's transaction" includes the scenario where the licensee and the individual agree over the telephone or electronically to enter into a consumer relationship involving prompt delivery of the insurance product or service but does not include the scenario where the relationship is initiated in person at the licensee's office or through other means by which the consumer may view the notice, such as on a website.

~~(1) Customer. An individual who becomes the licensee's customer, not later than when the licensee establishes a customer relationship, except as provided in Subsection E of this section; and~~

Commented [LS30]: NAMIC suggests that this aspect is problematic. Insurers must know the moment they "obtain access" to a consumer's nonpublic personal information and ensure notice is delivered before or at that time. In practice, data is often acquired gradually (application systems, underwriting feeds, verification vendors), making "access" triggers ambiguous.

(2) Consumer. A consumer, before the licensee discloses any nonpublic personal financial information about the consumer to any nonaffiliated third party, if the licensee makes a disclosure other than as authorized by Sections 16 and 17.

B. When initial notice to a consumer is not required. A licensee is not required to provide an initial notice to a consumer under Subsection A(2) of this section if:

(1) The licensee does not disclose any nonpublic personal financial information about the consumer to any nonaffiliated third party, other than as authorized by Sections 16 and 17, and the licensee does not have a customer relationship with the consumer; or

(2) A notice has been provided by an affiliated licensee, as long as the notice clearly identifies all licensees to whom the notice applies and is accurate with respect to the licensee and the other institutions.

C. When the licensee establishes a customer relationship.

(1) General rule. A licensee establishes a customer relationship at the time the licensee and the consumer enter into a continuing relationship.

(2) Examples of establishing customer relationship. A licensee establishes a customer relationship when the consumer:

(a) Becomes a policyholder of a licensee that is an insurer when the insurer delivers an insurance policy or contract to the consumer, or in the case of a licensee that is an insurance producer or insurance broker, obtains insurance through that licensee; or

(b) Agrees to obtain financial, economic or investment advisory services relating to insurance products or services for a fee from the licensee.

D. Existing customers. When an existing customer obtains a new insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, the licensee satisfies the initial notice requirements of Subsection A of this section as follows:

(1) The licensee may provide a revised policy notice, under Section 9, that covers the customer's new insurance product or service; or

(2) If the initial, revised or annual notice that the licensee most recently provided to that customer was accurate with respect to the new insurance product or service, the licensee does not need to provide a new privacy notice under Subsection A of this section.

E. Exceptions to allow subsequent delivery of notice.

(1) A licensee may provide the initial notice required by Subsection A(1) of this section within a reasonable time after the licensee establishes a customer relationship if:

(a) Establishing the customer relationship is not at the customer's election; or
(b) Providing notice not later than when the licensee establishes a customer

~~relationship would substantially delay the customer's transaction and the customer agrees to receive the notice at a later time.~~

~~(2) Examples of exceptions.~~

~~(a) Not at customer's election. Establishing a customer relationship is not at the customer's election if a licensee acquires or is assigned a customer's policy from another financial institution or residual market mechanism and the customer does not have a choice about the licensee's acquisition or assignment.~~

~~(b) Substantial delay of customer's transaction. Providing notice not later than when a licensee establishes a customer relationship would substantially delay the customer's transaction when the licensee and the individual agree over the telephone to enter into a customer relationship involving prompt delivery of the insurance product or service.~~

~~(c) No substantial delay of customer's transaction. Providing notice not later than when a licensee establishes a customer relationship would not substantially delay the customer's transaction when the relationship is initiated in person at the licensee's office or through other means by which the customer may view the notice, such as on a web site.~~

~~F. Delivery. When a licensee is required to deliver an initial privacy notice by this section, the licensee shall deliver it according to Section 11. If the licensee uses a short-form initial notice for non-customers according to Section 7D, the licensee may deliver its privacy notice according to Section 7D(3).~~

Section ~~6~~8. Annual ~~Privacy~~ Notice of Information Practices to ~~Customers~~ Consumers Required

~~A. (1)~~ General rule. A licensee shall provide a clear and conspicuous notice to consumers~~tomers~~ that accurately reflects its privacy policies and practices ~~not less than annually during the continuation of the customer relationship. Annually means~~ at least once in any period of twelve (12) consecutive months~~ during which that relationship exists.~~ A licensee may define the twelve-consecutive-month period, but the licensee shall apply it to the consumer~~ustomer~~ on a consistent basis.

A.~~(2)~~ Example. A licensee provides a notice annually if it defines the twelve-consecutive-month period as a calendar year and provides the annual notice to the consumer~~ustomer~~ once in each calendar year following the calendar year in which the licensee provided the initial notice. For example, if a consumer~~ustomer~~ opens an account on any day of year 1, the licensee shall provide an annual notice to that consumer~~ustomer~~ by December 31 of year 2.

(1) Exceptions~~ to general rule.~~

(1) A licensee that provides nonpublic personal information to nonaffiliated third parties only in accordance with Sections ~~15, 16, or 17~~22, 23, or 24 and has not changed its policies and practices with regard to disclosing ~~n~~Nonpublic P~~p~~ersonal ~~i~~information from the policies and practices that were disclosed in the most recent disclosure sent to consumers in accordance with this section or Section 7~~5~~ shall not be required to provide an annual disclosure under this section until such time as the licensee fails to comply with any

Commented [LS31]: As stated earlier, NAMIC strongly recommends that the revised Model follow the established approach of GLBA, which distinguishes requirements between consumers and customers.

Historically, GLBA has been concerned with delivery of notices to persons who buy products and services for personal or household purposes, and endures as long as the relationship lasts. This draft model will upset that paradigm and cause significant expense and operational complexity as a result.

For instance, the Model is no longer limited to current customers, so it extends the notice obligation to former customers for however many years a licensee may have data for a legitimate purpose. Also, it applies to insureds and claimants (some of whom inevitably will be minors), and it fails to consider that information could be collected from a source other than the individual and before that individual has directly interacted with the licensee. For example, if a consumer's information is included in a package of documents related to a potential claim, but that consumer has not yet contacted the licensee, does the licensee now need to make an affirmative effort to locate that consumer and provide a privacy notice?

criteria described in this paragraph.

(2) A licensee is not required to provide notice if the licensee no longer has access to the consumer's nonpublic personal information.

(2) For the purposes of this Act, a licensee no longer has an obligation to continue to notify a consumer if the licensee's records do not contain a valid address. An address is deemed invalid if electronic or regular mail sent to that address by the licensee has been returned as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.

~~C. (1) Termination of customer relationship. A licensee is not required to provide an annual notice to a former customer. A former customer is an individual with whom a licensee no longer has a continuing relationship.~~

~~(2) Examples.~~

~~(a) A licensee no longer has a continuing relationship with an individual if the individual no longer is a current policyholder of an insurance product or no longer obtains insurance services with or through the licensee.~~

~~(b) A licensee no longer has a continuing relationship with an individual if the individual's policy is lapsed, expired or otherwise inactive or dormant under the licensee's business practices, and the licensee has not communicated with the customer about the relationship for a period of twelve (12) consecutive months, other than to provide annual privacy notices, material required by law or regulation, or promotional materials.~~

~~(c) For the purposes of this regulation, a licensee no longer has a continuing relationship with an individual if the individual's last known address according to the licensee's records is deemed invalid. An address of record is deemed invalid if mail sent to that address by the licensee has been returned by the postal authorities as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.~~

~~(d) A licensee no longer has a continuing relationship with a customer in the case of providing real estate settlement services, at the time the customer completes execution of all documents related to the real estate closing, payment for those services has been received, or the licensee has completed all of its responsibilities with respect to the settlement, including filing documents on the public record, whichever is later.~~

~~D. Delivery. When a licensee is required by this section to deliver an annual privacy notice, the licensee shall deliver it according to Section 11.~~

Commented [LS32]: NAMIC recommends that the WG include more details here - while this provision states notice is not required if a licensee no longer has the consumer's NPI, there may be other instances where a notice should not be required. For instance, if a licensee no longer has a relationship with a consumer, but the licensee is required to keep the NPI for record retention requirements, a notice to the consumer would confuse the consumer as to why we are retaining data when they no longer have a relationship with the insurer.

Section 9~~7~~. Information to be Included in ~~Privacy~~ Notices of Information Practices

A. General rule. The initial, annual and revised ~~privacy notices~~ Notice of Information Practices that a licensee provides under Sections ~~5~~7,~~, 68~~8, and ~~3~~139 shall include each of the following items of information, in addition to any other information the licensee wishes to provide, that applies to the licensee and to the consumers to whom the licensee sends its ~~privacy notice:~~ Notice of Information Practices:

~~(1) The categories of nonpublic personal financial information that the licensee collects;~~

~~(2) The categories of nonpublic personal financial information that the licensee discloses;~~

~~(3) The categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information, other than those parties to whom the licensee discloses information under Sections 16 and 17;~~

~~(4) The categories of nonpublic personal financial information about the licensee's former customers that the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal financial information about the licensee's former customers, other than those parties to whom the licensee discloses information under Sections 16 and 17;~~

~~(5) If a licensee discloses nonpublic personal financial information to a nonaffiliated third party under Section 15 (and no other exception in Sections 16 and 17 applies to that disclosure), a separate description of the categories of information the licensee discloses and the categories of third parties with whom the licensee has contracted;~~

(1) The categories of nonpublic personal information that the licensee collects, including, but not limited to, whether information is collected from the consumer, through the consumer's transactions with affiliates or nonaffiliated third parties, or consumer reporting agencies;

(2) The categories of nonpublic personal information that the licensee discloses, including at least one example in each category. Categories may include, but are not limited to, application information, transaction information, or consumer reports;

(3) The categories of affiliates and nonaffiliated third parties, and the types of business in which they engage, to whom the licensee discloses nonpublic personal information, other than those parties to whom the licensee discloses information under Sections ~~20 and 21~~22, 23, and 24. The types of businesses may be described in general terms only if the licensee uses illustrative examples of each significant line of business;

(~~4~~6) An explanation of the consumer's right under Section 12~~A~~ to opt out of the disclosure of nonpublic personal ~~financial~~ information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;

(5) An explanation of the consumer's rights with regard to the sale of nonpublic personal information and disclosure of sensitive personal information pursuant to Sections 20 and 21;

(6) A description of the consumer's options to request access, correction, or deletion of

nonpublic personal information about the consumer as established under this Act and the instructions for exercising such options;

(7) Any disclosures that the licensee makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);

(8) The licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; by~~and~~

(a) Describing in general terms who is authorized to have access to the information; and

(b) Stating whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance with the licensee's policy. The licensee is not required to describe technical information about the safeguards it uses; and

~~(9)~~(c) Any disclosure that the licensee makes ~~under Subsection B of this section.~~ as authorized under Section 22, 23, or 24~~21~~, except that the licensee is not required to list those exceptions in the initial or annual Notice of Information Practices required by Sections ~~9~~7 and ~~10~~8. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.

~~B. Description of parties subject to exceptions. If a licensee discloses nonpublic personal financial information as authorized under Sections 16 and 17, the licensee is not required to list those exceptions in the initial or annual privacy notices required by Sections 5 and 6. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.~~

B. The licensee's notice may include:

(1) Categories of nonpublic personal information that the licensee reserves the right to disclose in the future, but does not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the right in the future to disclose, but to whom the licensee does not currently disclose, nonpublic personal information.

C. Exceptions:~~Examples.~~

If a licensee does not disclose, and does not reserve the right to disclose, nonpublic personal information about consumers to affiliates or nonaffiliated third parties except as authorized under Sections ~~20 and 21~~22, 23, or 24, the licensee shall state that in its notice, in addition to the information it shall provide under Subsections A(1) and A(8) and Subsection B of this section.

Commented [LS33]: NAMIC requests clarification on whether the "future sharing" category-based notices are intended to cover future disclosures. Further, how does the "future sharing aspect affect the obligation to provide revised notices (Section 13)? Does adding new categories trigger revised notice/material-change obligations, even if the disclosures remain within the described categories?

D. Sample Clauses and Federal Model Privacy Form.

(1) Licensees are not required to use any prescribed clauses or model form.

(2) The commissioner may determine that a Licensee's use of any of the following constitutes compliance with this Act:

(a) Sample clauses illustrating some of the notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner;

(b) Model forms illustrating notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner; or

(c) The Federal Model Privacy Forms are included in Appendix A and Appendix B, of this Act.

~~(1) Categories of nonpublic personal financial information that the licensee collects. A licensee satisfies the requirement to categorize the nonpublic personal financial information it collects if the licensee categorizes it according to the source of the information, as applicable:~~

~~(a) Information from the consumer;~~

~~(b) Information about the consumer's transactions with the licensee or its affiliates;~~

~~(c) Information about the consumer's transactions with nonaffiliated third parties; and~~

~~(d) Information from a consumer reporting agency.~~

~~(2) Categories of nonpublic personal financial information a licensee discloses.~~

~~(a) A licensee satisfies the requirement to categorize nonpublic personal financial information it discloses if the licensee categorizes the information according to source, as described in Paragraph (1), as applicable, and provides a few examples to illustrate the types of information in each category. These might include:~~

~~(i) Information from the consumer, including application information, such as assets and income and identifying information, such as name, address and social security number;~~

~~(ii) Transaction information, such as information about balances, payment history and parties to the transaction; and~~

~~(iii) Information from consumer reports, such as a consumer's creditworthiness and credit history.~~

~~(b) A licensee does not adequately categorize the information that it discloses if the~~

licensee uses only general terms, such as transaction information about the consumer.

(c) If a licensee reserves the right to disclose all of the nonpublic personal financial information about consumers that it collects, the licensee may simply state that fact without describing the categories or examples of nonpublic personal information that the licensee discloses.

(3) Categories of affiliates and nonaffiliated third parties to whom the licensee discloses.

(a) A licensee satisfies the requirement to categorize the affiliates and nonaffiliated third parties to which the licensee discloses nonpublic personal financial information about consumers if the licensee identifies the types of businesses in which they engage.

(b) Types of businesses may be described by general terms only if the licensee uses a few illustrative examples of significant lines of business. For example, a licensee may use the term financial products or services if it includes appropriate examples of significant lines of businesses, such as life insurer, automobile insurer, consumer banking or securities brokerage.

(c) A licensee also may categorize the affiliates and nonaffiliated third parties to which it discloses nonpublic personal financial information about consumers using more detailed categories.

(4) Disclosures under exception for service providers and joint marketers. If a licensee discloses nonpublic personal financial information under the exception in Section 15 to a nonaffiliated third party to market products or services that it offers alone or jointly with another financial institution, the licensee satisfies the disclosure requirement of Subsection A(5) of this section if it:

(a) Lists the categories of nonpublic personal financial information it discloses, using the same categories and examples the licensee used to meet the requirements of Subsection A(2) of this section, as applicable; and

(b) States whether the third party is:

(i) A service provider that performs marketing services on the licensee's behalf or on behalf of the licensee and another financial institution; or

(ii) A financial institution with whom the licensee has a joint marketing agreement.

(5) Simplified notices. If a licensee does not disclose, and does not wish to reserve the right to disclose, nonpublic personal financial information about customers or former customers to affiliates or nonaffiliated third parties except as authorized under Sections 16 and 17, the licensee may simply state that fact, in addition to the information it shall provide under Subsections A(1), A(8), A(9) and Subsection B of this section.

(6) Confidentiality and security. A licensee describes its policies and practices with respect to

protecting the confidentiality and security of nonpublic personal financial information if it does both of the following:

(a) Describes in general terms who is authorized to have access to the information; and

(b) States whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance with the licensee's policy. The licensee is not required to describe technical information about the safeguards it uses.

D. Short-form initial notice with opt out notice for non-customers.

(1) A licensee may satisfy the initial notice requirements in Sections 5A(2) and 8C for a consumer who is not a customer by providing a short-form initial notice at the same time as the licensee delivers an opt out notice as required in Section 8.

(2) A short-form initial notice shall:

(a) Be clear and conspicuous;

(b) State that the licensee's privacy notice is available upon request; and

(c) Explain a reasonable means by which the consumer may obtain that notice.

(3) The licensee shall deliver its short-form initial notice according to Section 10. The licensee is not required to deliver its privacy notice with its short-form initial notice. The licensee instead may simply provide the consumer a reasonable means to obtain its privacy notice. If a consumer who receives the licensee's short-form notice requests the licensee's privacy notice, the licensee shall deliver its privacy notice according to Section 11.

(4) Examples of obtaining privacy notice. The licensee provides a reasonable means by which a consumer may obtain a copy of its privacy notice if the licensee:

(a) Provides a toll-free telephone number that the consumer may call to request the notice; or

(b) For a consumer who conducts business in person at the licensee's office, maintains copies of the notice on hand that the licensee provides to the consumer immediately upon request.

E. Future disclosures. The licensee's notice may include:

(1) Categories of nonpublic personal financial information that the licensee reserves the right to disclose in the future, but does not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the right in the future to disclose, but to whom the licensee does not currently disclose, nonpublic personal financial information.

~~F. Sample Clauses and Federal Model Privacy Form. Sample clauses illustrating some of the notice content required by this section and the Federal Model Privacy Form are included in Appendix A and Appendix B, respectively, of this regulation.~~

Section 10. Short Form Initial Notice of Information Practices

A. A licensee may satisfy the initial notice requirements in Sections 7A and 13A by providing a Short Form Initial Notice of Information Practices at the same time the licensee delivers an opt-out notice as required in Section 12 if:

(1) The licensee provides the consumer a reasonable means to obtain its Notice of Information Practices; and

(2) The licensee provides the Notice of Information Practices upon request.

B. A Short Form Initial Notice of Information Practices shall meet all of the following requirements.

(1) Be clear and conspicuous;

(2) State that the licensee's Notice of Information Practices is available upon request;

(3) Explain the reasonable means to obtain the licensee's Notice of Information Practices;

(4) Contain contact information for the commissioner; and

(5) Describe how the consumer can request access to or correction of their nonpublic personal information.

C. For purposes of this section "reasonable means to obtain the licensee's Notice of Information Practices" includes:

(1) Providing a toll-free telephone number that the consumer may call to request the notice;

(2) Providing a website or other electronic medium that is easily accessible by the consumer; or

(3) Maintaining copies of the notice at the licensee's place of business to be provided upon request.

Section 11~~8~~. Form of Opt-In~~Out~~ Notice to Consumers and Opt-In~~Out~~ Methods

A. ~~(1) Form of opt-out notice.~~ If a licensee is required to provide an opt-in ~~-out~~ notice under Sections ~~12A22~~20 or ~~23~~21, it shall provide a clear and conspicuous notice to each of its consumers that accurately explains the ~~right~~ information proposed to be disclosed, the use of that information, and the consumer's option to opt in to that use.~~out under that section.~~ The notice shall state:

(1)~~a~~) ~~That T~~the licensee discloses or reserves the right to disclose nonpublic personal ~~financial~~ information about its consumer to a nonaffiliated third party;

(2~~b~~) ~~That T~~the consumer has the ~~right~~ option to opt in to ~~out of~~ that disclosure; and

Commented [LS34]: NAMIC requests clarification here: If a licensee does not have to deliver an opt-out notice, does that prevent use of the short form notice? In GLBA and Model 670, short form notice is not necessary unless applying or renewing a product or service. Under the Draft's new verbiage, insurers may be expected to deliver a sort form notice to everyone.

(3) A reasonable means by which the consumer may exercise the option to opt in~~out right~~.

B. The licensee shall not disclose that information to a nonaffiliated third party unless the consumer has affirmatively opted in to the use.

C. The opt-in must be an affirmative act by the consumer. The licensee cannot deem a failure to respond as an opt-in or use pre-checked boxes.

D. The opt-in should be obtained separately from any other communication or consent.

E. The opt-in may be revoked at any time by the consumer.

~~(2) Examples.~~

~~(a) Adequate opt out notice. A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal financial information to a nonaffiliated third party if the licensee:~~

~~(i) Identifies all of the categories of nonpublic personal financial information that it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to which the licensee discloses the information, as described in Section 7A(2) and (3), and states that the consumer can opt out of the disclosure of that information; and~~

~~(ii) Identifies the insurance products or services that the consumer obtains from the licensee, either singly or jointly, to which the opt out direction would apply.~~

~~(b) Reasonable opt out means. A licensee provides a reasonable means to exercise an opt out right if it:~~

~~(i) Designates check-off boxes in a prominent position on the relevant forms with the opt out notice;~~

~~(ii) Includes a reply form together with the opt out notice;~~

~~(iii) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the licensee's web site, if the consumer agrees to the electronic delivery of information; or~~

~~(iv) Provides a toll-free telephone number that consumers may call to opt out.~~

~~(c) Unreasonable opt out means. A licensee does not provide a reasonable means of opting out if:~~

~~(i) The only means of opting out is for the consumer to write his or her own letter to exercise that opt out right; or~~

~~(ii) The only means of opting out as described in any notice subsequent to the initial notice is to use a check off box that the licensee provided with~~

Commented [LS35]: As noted in our substantive comments, NAMIC has concerns with the opt-in architecture. GLBA currently provides an opt-out mechanism for sharing with nonaffiliated parties (unless it fits a different exception or exemption), and also allows gaining customer consents. The Draft approach here presents greater complexity than current expectations, for both consumers and licensees.

Commented [LS36]: NAMIC requests clarification on what is meant by "affirmative act."

Commented [LS37]: NAMIC requests the Working Group provide clarity on what constitutes a proper revocation, acceptable forms of revocation, degree of specificity required, and whether revocation is specific to certain sharing types.

the initial notice but did not include with the subsequent notice.

(d) Specific opt out means. A licensee may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

B. Same form as initial notice permitted. A licensee may provide the opt out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 5.

C. Initial notice required when opt out notice delivered subsequent to initial notice. If a licensee provides the opt out notice later than required for the initial notice in accordance with Section 5, the licensee shall also include a copy of the initial notice with the opt out notice in writing or, if the consumer agrees, electronically.

D. Joint relationships.

(1) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt out notice. The licensee's opt out notice shall explain how the licensee will treat an opt out direction by a joint consumer (as explained in Paragraph (5) of this subsection).

(2) Any of the joint consumers may exercise the right to opt out. The licensee may either:

(a) Treat an opt out direction by a joint consumer as applying to all of the associated joint consumers; or

(b) Permit each joint consumer to opt out separately.

(3) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all of the joint consumers.

(4) A licensee may not require all joint consumers to opt out before it implements any opt out direction.

(5) Example. If John and Mary are both named policyholders on a homeowner's insurance policy issued by a licensee and the licensee sends policy statements to John's address, the licensee may do any of the following, but it shall explain in its opt out notice which opt out policy the licensee will follow:

(a) Send a single opt out notice to John's address, but the licensee shall accept an opt out direction from either John or Mary.

(b) Treat an opt out direction by either John or Mary as applying to the entire policy. If the licensee does so and John opts out, the licensee may not require Mary to opt out as well before implementing John's opt out direction.

(c) Permit John and Mary to make different opt out directions. If the licensee does so:

(i) It shall permit John and Mary to opt out for each other;

~~(ii) If both opt out, the licensee shall permit both of them to notify it in a single response (such as on a form or through a telephone call); and~~

~~(iii) If John opts out and Mary does not, the licensee may only disclose nonpublic personal financial information about Mary, but not about John and not about John and Mary jointly.~~

~~E. Time to comply with opt out. A licensee shall comply with a consumer's opt out direction as soon as reasonably practicable after the licensee receives it.~~

~~F. Continuing right to opt out. A consumer may exercise the right to opt out at any time.~~

~~G. Duration of consumer's opt out direction.~~

~~(1) A consumer's direction to opt out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.~~

~~(2) When a customer relationship terminates, the customer's opt out direction continues to apply to the nonpublic personal financial information that the licensee collected during or related to that relationship. If the individual subsequently establishes a new customer relationship with the licensee, the opt out direction that applied to the former relationship does not apply to the new relationship.~~

~~H. Delivery. When a licensee is required to deliver an opt out notice by this section, the licensee shall deliver it according to Section 11.~~

Section 12. Form of Opt-Out Notice to Consumers and Opt-Out Methods

A. (1) If a licensee is required to provide an opt-out notice, it shall provide a clear and conspicuous notice to each consumer that accurately explains the right to opt out under that section. To the extent applicable, the notice shall state:

(a) That the licensee discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;

(b) That the consumer has the right to opt out of that disclosure; and

(c) A reasonable means by which the consumer may exercise the opt-out right.

(2) Requirements

(a) A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if the licensee:

(i) Identifies all of the categories of nonpublic personal information it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to whom the licensee discloses the information, as described in Section ~~11~~9A(2) and (3), and states the consumer can opt out of the disclosure of that information; and

Commented [LS38]: NAMIC suggests that Section 12 may benefit from additional clarification to align with current state privacy-law mechanics. In particular, the model should clarify whether opt-out mechanisms must include online methods, whether a licensee must honor opt-out preference signals or universal opt-out mechanisms where applicable, whether opt-in consent applies only to specific categories of disclosures or processing, and how these provisions interact with the Act's separate limits on targeted advertising, sale of nonpublic personal information, and disclosure of sensitive personal information.

~~Identifies the insurance products or services the consumer obtains from the licensee, either singly or jointly, to which the opt-out would apply;~~

Commented [LS39]: NAMIC suggests removal of 2(a)(ii) because (i) is sufficient. Alternatively, we suggest using more generic language than "identifies" to avoid "products or services" level specificity. That level of specificity creates operational burden and financial burden (including increased cost to consumers).

(b) A licensee provides a reasonable means to exercise an opt-out right if it:

(i) Designates check-off boxes in a prominent position on the relevant forms with the opt-out notice;

(ii) Includes a reply form together with the opt–out notice;

(iii) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the licensee's website, if the consumer agrees to the electronic delivery of information; or

(iv) Provides a toll-free telephone number that consumers may call to opt out.

(c) A licensee does not provide a reasonable means of opting out if:

(i) The only means of opting out is for the consumer to write a letter to the licensee to exercise their opt-out right; or

(ii) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the licensee provided with the initial notice but did not include with the subsequent notice.

(d) A licensee may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

B. A licensee may provide the opt-out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 7.

C. If a licensee provides the opt-out notice after it provides the initial notice, the licensee shall include a copy of the initial notice with the opt-out notice in writing or, if the consumer agrees, electronically.

D. Joint relationships.

(1) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt-out notice. The licensee's opt-out notice shall explain how the licensee will treat an opt-out direction by a joint consumer (as explained in Paragraph (2) of this subsection).

(2) Any of the joint consumers may exercise the right to opt out. The licensee may either:

(a) Treat an opt-out direction by a joint consumer as applying to all of the associated joint consumers; or

(b) Permit each joint consumer to opt out separately.

(3) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all the joint consumers.

(4) A licensee may not require all joint consumers to opt out before it implements any opt-out direction.

E. A licensee shall comply with a consumer's opt-out direction as soon as reasonably practicable but no later than 10 business days after the licensee receives it.

F. A consumer may exercise the right to opt out at any time. A consumer's direction to opt-out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.

Section 13~~9~~. Revised ~~Privacy~~ Notice of Information Practices~~s~~

A. ~~General rule.~~Except as otherwise authorized in this Act~~regulation~~, a licensee shall not, directly or through an affiliate, disclose any nonpublic personal ~~financial~~ information about a consumer to a nonaffiliated third party other than as described in the initial notice that the licensee provided to that consumer under Section ~~5~~7, unless:

(1) The licensee has provided to the consumer a clear and conspicuous revised notice that accurately describes its policies and practices;

(2) The licensee has provided to the consumer a new opt-out notice;

(3) The licensee has given the consumer a reasonable opportunity, before the licensee discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(4) The consumer does not opt out.

B. Examples.

(1) Except as otherwise permitted by Sections 1~~9~~5, 20~~16~~ and 21~~17~~, a licensee shall provide a revised notice before it:

(a) Discloses a new category of nonpublic personal ~~financial~~ information to any nonaffiliated third party; or

(b) Discloses nonpublic personal ~~financial~~ information to a new category of nonaffiliated third party.~~; or~~

~~(c) Discloses nonpublic personal financial information about a former customer to a nonaffiliated third party, if that former customer has not had the opportunity to exercise an opt out right regarding that disclosure.~~

(2) A revised notice is not required if the licensee discloses nonpublic personal ~~financial~~ information to a new nonaffiliated third party that the licensee adequately described in its prior notice.

~~C. Delivery. When a licensee is required to deliver a revised privacy notice by this section, the licensee shall deliver it according to Section 11.~~

Commented [LS40]: NAMIC suggests clarification that 10 days means 10 business days.

Additionally, NAMIC suggests inclusion of a longer response or compliance period of 15-30 days for operational feasibility, especially where systems, vendor updates, and downstream propagation are required.

Commented [LS41]: Consistent with NAMIC's comments in Section 7, this section could benefit from clarification around third-party claimants. For a third-party claimant whose nonpublic personal information is collected, used, or disclosed solely for claim investigation, adjustment, defense, settlement, payment, subrogation, fraud prevention, legal compliance, or other claim-related purposes permitted under this Act, a licensee should be able to satisfy the notice requirement including revised requirement notice (if such is ever needed) by making its notice of information practices publicly available on its website, informing the claimant how to access the notice, and providing a paper or electronic copy upon request.

© 20~~17~~26 National Association of Insurance Commissioners

Section 14~~0~~. ~~Privacy~~ Notice~~s~~ of Information Practices to Group Policyholders

Unless a licensee is providing notices of information practices~~privacy notices~~ directly to covered individuals described in Section 4~~F~~(G)2)(e)(i), (ii) or (iii), a licensee shall provide initial, annual and revised notices to the plan sponsor, group or blanket insurance policyholder or group annuity contract holder, or workers' compensation policyholder, in the manner described in Sections ~~9~~75 through 13~~9~~ of this Act~~regulation~~, describing the licensee's privacy practices with respect to nonpublic personal information about individuals covered under the policies, contracts or plans. Compliance with this section satisfies the licensees initial, annual and renewal Notice of Information Practices as required by Sections 7 and 8 and delivery provisions of Section 15.

Section 15~~1~~. Delivery

A. ~~How to provide notices.~~ A licensee shall provide any notices that this Act~~regulation~~ requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer interacts with the licensee online or in some other electronic fashion, ~~agrees,~~ electronically.

B. (1) ~~Examples of reasonable expectation of actual notice.~~ A licensee may reasonably expect that a consumer will receive actual notice if the licensee:

(a) Hand-delivers a printed copy of the notice to the consumer;

(b) Mails a printed copy of the notice to the last known address of the consumer separately, or in a policy, billing or other written communication;

(c) For a consumer who conducts transactions electronically, in accordance with UETA (insert state electronic transactions act statute), posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service;

(i) The notice should be posted in a manner that enables a consumer to print or save it using programs or apps that are widely available and free of charge.

(ii) Notice is available electronically as long as it is in force.

(d) For an isolated transaction with a consumer, such as the licensee providing an insurance quote or selling the consumer travel insurance, posts the notice and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular insurance product or service.

(e) Provides the notice by any other means authorized by the commissioner.

(2) Examples of unreasonable expectation of actual notice. A licensee may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:

(a) Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or

(b) Sends the notice via electronic mail to a consumer who does not otherwise

Commented [LS42]: Consistent with NAMIC's comments around Section 7 and 13, we suggest that Section 15 should include detail to resolve operational concerns regarding third-party claimants.

The model should clarify that, for third-party claimants whose nonpublic personal information is collected, used, or disclosed solely for claim investigation, adjustment, defense, settlement, payment, subrogation, fraud prevention, legal compliance, or other claim-related purposes permitted under the Act, a licensee may satisfy the initial and any revised notice requirement by making the notice publicly available on its website, informing the claimant how to access the notice, and providing a paper or electronic copy upon request.

© 2026~~17~~ National Association of Insurance Commissioners

communicate with ~~obtain an insurance product or service from~~ the licensee electronically.

C. ~~Annual notices only.~~ A licensee may reasonably expect that a consumer~~ustomer~~ will receive actual notice of the licensee's ~~annual privacy n~~Notice ~~if.~~ of Information Practices if:

(1) The consumer~~ustomer~~ uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a clear and conspicuous manner on the web site; or

(2) The consumer~~ustomer~~ has requested that the licensee refrain from sending any information regarding the consumer~~ustomer~~ relationship, and the licensee's current privacy notice remains available to the consumer~~ustomer~~ upon request.

D. A licensee may not provide any notice required by this Act solely by orally explaining the notice, either in person or over the telephone.

E. A licensee may provide a joint notice from the licensee and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the licensee and the other institutions. A licensee also may provide a notice on behalf of another financial institution.

F. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of Sections 7A, 8A and 13A, respectively, by providing one notice to those consumers jointly.

~~D. Oral description of notice insufficient. A licensee may not provide any notice required by this regulation solely by orally explaining the notice, either in person or over the telephone.~~

~~E. Retention or accessibility of notices for customers.~~

~~(1) For customers only, a licensee shall provide the initial notice required by Section 5A(1), the annual notice required by Section 6A, and the revised notice required by Section 9 so that the customer can retain them or obtain them later in writing or, if the customer agrees, electronically.~~

~~(2) Examples of retention or accessibility. A licensee provides a privacy notice to the customer so that the customer can retain it or obtain it later if the licensee:~~

~~(a) Hand delivers a printed copy of the notice to the customer;~~

~~(b) Mails a printed copy of the notice to the last known address of the customer; or~~

~~(c) Makes its current privacy notice available on a web site (or a link to another web site) for the customer who obtains an insurance product or service electronically and agrees to receive the notice at the web site.~~

~~F. Joint notice with other financial institutions. A licensee may provide a joint notice from the licensee and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the licensee and the other institutions. A licensee~~

~~also may provide a notice on behalf of another financial institution.~~

~~G. Joint relationships. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of Sections 5A, 6A and 9A, respectively, by providing one notice to those consumers jointly.~~

© 2026~~17~~ National Association of Insurance Commissioners

ARTICLE V~~III~~. LIMITS ON DISCLOSURES OF NONPUBLIC~~FINANCIAL~~ PERSONAL INFORMATION

Section 16. General Rules for Use and Disclosure of Nonpublic Personal Information

A. Use and Disclosure

(1) A licensee may use and disclose nonpublic personal information about a consumer for purposes of processing a business transaction requested or authorized by the consumer.

(2) A licensee may disclose nonpublic personal information with affiliates, provided the affiliates' use and disclosure comply with this Act.

(3) A licensee may use or disclose nonpublic personal information as reasonably necessary to detect, prevent, investigate, or respond to fraud, misrepresentation, unauthorized activity, security incidents, or other unlawful conduct.

Drafting Note: States have their own definitions of fraud, and should therefore include and point to that statutory reference in the fraud related provisions within this Draft so as to avoid inadvertent conflicts or discrepancies.

(3) A licensee shall not disclose nonpublic personal information to a nonaffiliated third party except as permitted by this Act.

(4) This section applies to nonpublic personal information collected before and after a consumer exercises an opt-out right under Section 19 or an opt-in right under Sections 20 and 21.

(5) If a consumer submits an opt-out request during a transaction and the requested information is necessary to complete that transaction, the licensee shall:

(a) Inform the consumer that the transaction cannot be completed without the information; and

(b) Confirm whether the consumer wishes to proceed.

B. Limits on Disclosure. Except as provided by Section 16A(1), before disclosing a consumer's nonpublic personal information to a nonaffiliated third party, whether directly or through an affiliate, a licensee shall:

(1) Provide the initial notice required by Section 7;

(2) Provide a clear and conspicuous notice to the consumer that details:

(a) The consumer's right to opt out of disclosure for targeted advertising under Section 19;

(b) The consumer's option to opt in to the sale of nonpublic personal information under Section 20; or

(c) The consumer's option to opt in to the disclosure of sensitive personal information Section 21.

Commented [LS43]: NAMIC suggests that Section 16 should expressly recognize fraud prevention, detection, investigation, and response as permitted purposes for use and disclosure of NPI. Without such clarification, fraud-related activity may need to be inferred from claim handling, legal compliance, or anticipated civil/criminal proceedings. These categories alone may be too narrow because fraud prevention and investigation can occur before litigation, regulatory action, or criminal proceedings are reasonably anticipated.

Fraud controls are an essential part of underwriting, policy administration, billing, claims handling, payment integrity, SIU investigations, subrogation, salvage, vendor oversight, and consumer protection. The model should therefore permit use and disclosure of NPI for fraud-related and security-related purposes.

Commented [LS44]: To ensure alignment with state laws and fraud definitions therein, NAMIC suggests this drafting note to allow states to specifically reference and incorporate their fraud statutory references.

Commented [LS45]: NAMIC suggests that this paragraph is redundant - can the Working Group please explain the intended purpose and how it avoids redundancy?

Commented [LS46]: NAMIC suggests that these provisions introduce operational complexity. For instance, it may not be feasible to pause a transaction process currently underway, so what is the expected or anticipated operational approach from the Working Group's perspective? Additionally, how is compliance to be confirmed?

© 2026~~17~~ National Association of Insurance Commissioners

(3) Provide a reasonable opportunity for the consumer to exercise any applicable opt-out right before disclosure; and

(4) Obtain and document the consumer's opt-in or opt-out election, as applicable.

~~**Section 12. Limits on Disclosure of Nonpublic Personal Financial Information to Nonaffiliated Third Parties**~~

~~A. (1) Conditions for disclosure. Except as otherwise authorized in this regulation, a licensee may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer to a nonaffiliated third party unless:~~

~~(a) The licensee has provided to the consumer an initial notice as required under Section 5;~~

~~(b) The licensee has provided to the consumer an opt out notice as required in Section 8;~~

~~(c) The licensee has given the consumer a reasonable opportunity, before it discloses the information to the nonaffiliated third party, to opt out of the disclosure; and~~

~~(d) The consumer does not opt out.~~

~~(2) Opt out definition. Opt out means a direction by the consumer that the licensee not disclose nonpublic personal financial information about that consumer to a nonaffiliated third party, other than as permitted by Sections 15, 16 and 17.~~

~~(3) Examples of reasonable opportunity to opt out. A licensee provides a consumer with a reasonable opportunity to opt out if:~~

~~(a) By mail. The licensee mails the notices required in Paragraph (1) of this subsection to the consumer and allows the consumer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within thirty (30) days from the date the licensee mailed the notices.~~

~~(b) By electronic means. A customer opens an on-line account with a licensee and agrees to receive the notices required in Paragraph (1) of this subsection electronically, and the licensee allows the customer to opt out by any reasonable means within thirty (30) days after the date that the customer acknowledges receipt of the notices in conjunction with opening the account.~~

~~(c) Isolated transaction with consumer. For an isolated transaction such as providing the consumer with an insurance quote, a licensee provides the consumer with a reasonable opportunity to opt out if the licensee provides the notices required in Paragraph (1) of this subsection at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction, whether to opt out before completing the transaction.~~

~~B. Application of opt out to all consumers and all nonpublic personal financial information.~~

~~(1) A licensee shall comply with this section, regardless of whether the licensee and the~~

~~consumer have established a customer relationship.~~

~~(2) Unless a licensee complies with this section, the licensee may not, directly or through any affiliate, disclose any nonpublic personal financial information about a consumer that the licensee has collected, regardless of whether the licensee collected it before or after receiving the direction to opt out from the consumer.~~

~~C. Partial opt out. A licensee may allow a consumer to select certain nonpublic personal financial information or certain nonaffiliated third parties with respect to which the consumer wishes to opt out.~~

Section 17~~3~~. Limits on Redisclosure and Reuse of Nonpublic Personal ~~Financial~~ Information

A. ~~(1) Information the licensee receives under an exception.~~ If a licensee receives nonpublic personal ~~financial~~ information from a nonaffiliated third-party service provider~~financial institution~~ under an exception in ~~Sections 20~~16 ~~or 17 or~~ Article VI of this Act~~regulation~~, ~~the licensee's disclosure and use of that information is limited as follows:~~

~~(a) The licensee may disclose the information to the affiliates of the financial institution from which the licensee received the information;~~

~~(b) The licensee may disclose the information to its affiliates, but the licensee's affiliates may, in turn, disclose and use the information only to the extent that the licensee may disclose and use the information; and~~

~~(a)~~ ~~t~~The licensee may use and disclose the information ~~pursuant to an exception in Sections 16 or 17 of this regulation,~~ in the ordinary course of business to carry out the activity covered by the exception under which the licensee received the information.

~~(2) Example. If a licensee receives information from a nonaffiliated financial institution for claims settlement purposes, the licensee may disclose the information for fraud prevention, or in response to a properly authorized subpoena. The licensee may not disclose that information to a third party for marketing purposes or use that information for its own marketing purposes.~~

B. (1) ~~Information a licensee receives outside of an exception.~~ If a licensee receives nonpublic personal ~~financial~~ information from a nonaffiliated third-party service provider~~financial institution~~ other than under an exception in ~~Sections 20 or~~ Article VI~~16 or 17~~ of this Act~~regulation~~, the licensee may disclose the information only to the following, provided the disclosure is consistent with this Act:

(a) ~~To the A~~affiliates of the third party-service provider~~financial institution~~ from which the licensee received the information; and

(b) ~~To its A~~affiliates of the licensee who may~~, but its affiliates may, in turn,~~ disclose the information only to the extent that the ~~licensee may disclose the information;~~disclosure would be permissible by the licensee pursuant to this Act. ~~and~~

Commented [LS47]: NAMIC suggests that Section 17 should clarify that NPI received under a permitted fraud-prevention, fraud-detection, investigation, security, or unlawful-conduct exception may be redisclosed or reused for that same permitted purpose. Without such clarification, downstream recipients may be uncertain whether they can share information needed to investigate suspected insurance fraud, organized fraud activity, misrepresentation, identify theft, payment fraud, or related unlawful conduct.

Commented [LS48]: NAMIC also suggests that Section 17 should clarify that a recipient of nonpublic personal information disclosed under a permitted exception may reuse or redisclose the information as reasonably necessary to carry out the same permitted purpose, including claim investigation, adjustment, defense, settlement, payment, subrogation, salvage, recovery, reinsurance, fraud prevention, legal compliance, regulatory reporting, or other purposes permitted by the Act. Without clarification, downstream recipients may face uncertainty in ordinary insurance operations.

Commented [LS49]: NAMIC requests the Working group clarify the difference between "nonaffiliated third party" and "nonaffiliated third party service provider throughout this section.

~~(c) To any other person, if the disclosure would be lawful if made directly to that person by the financial institution from which the licensee received the information.~~

(2) Example. If a licensee obtains a customer list from a nonaffiliated third-party service provider~~financial institution~~ outside of the exceptions in ~~Sections 16 or 17;~~20 ~~or~~ Article VI:

(a) The licensee may use that list for its own purposes~~; and~~ consistent with this Act; and

(b) The licensee may disclose that list to another nonaffiliated third-party service provider only as permitted by this Act.~~if the financial institution from which the licensee purchased the list could have lawfully disclosed the list to that third party. That is, the licensee may disclose the list in accordance with the privacy policy of the financial institution from which the licensee received the list, as limited by the opt-out direction of each consumer whose nonpublic personal financial information the licensee intends to disclose, and the licensee may disclose the list in accordance with an exception in Sections 16 or 17, such as to the licensee's attorneys or accountants.~~

C. ~~Information a licensee discloses under an exception.~~ If a licensee discloses nonpublic personal ~~financial~~ information to a nonaffiliated third-party service provider under an exception in S~~ections 16 or 17~~ 20 ~~or~~ Article VI of this Act~~of this regulation~~, the third party-service provider:~~ may disclose and use that information only as follows:~~

(1) ~~The third party~~ M~~m~~ay disclose the information to the licensee's affiliates; and

~~(2) The third party may disclose the information to its affiliates, but its affiliates may, in turn, disclose and use the information only to the extent that the third party may disclose and use the information; and~~

(2~~3~~) ~~The third party~~ M~~m~~ay disclose and use the information ~~pursuant to an exception in Sections 16 or 17~~ in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

D. ~~Information a licensee discloses outside of an exception.~~ If a licensee discloses nonpublic personal ~~financial~~ information to a nonaffiliated third-party service provider other than under an exception in ~~Sections~~ 20 ~~16 or 17 or~~ Article VI of this Act~~regulation~~, the third-party service provider may disclose the information only:

(1) To the licensee's affiliates~~;~~ who may disclose the information only to the extent that it would be permissible for the licensee to disclose the information pursuant to this Act: and

~~(2) To the third party's affiliates, but the third party's affiliates, in turn, may disclose the information only to the extent the third party can disclose the information; and~~

(2~~3~~) To any other person, if the disclosure would be lawful if the licensee made it directly to that person.

Section 18~~14~~. Limits on Sharing Access Number or Access Code~~Account Number~~ Information for Marketing

Purposes

A. ~~General prohibition on disclosure of account numbers.~~ A licensee shall not, directly or through an affiliate, disclose, other than to a consumer reporting agency, a policy number or similar form of access number or access code for a consumer's policy or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

B. Exceptions. Subsection A of this section does not apply if a licensee discloses a policy number or similar form of access number or access code:

(1) To the licensee's service provider solely in order to perform marketing for the licensee's own products or services, as long as the service provider is not authorized to directly initiate charges to the account;

(2) To a licensee who is a producer solely in order to perform marketing for the licensee's own products or services; or

(3) To a participant in an affinity or similar program where the participants in the program are identified to the consumer~~ustomer~~ when the consumer~~ustomer~~ enters into the program.

(4) Where the policy number, or similar form of access number or access code, is in an encrypted form, as long as the licensee does not provide a means to decode the access number or access code.

~~C. Examples.~~

~~(1) Policy number. A policy number, or similar form of access number or access code, does not include a number or code in an encrypted form, as long as the licensee does not provide the recipient with a means to decode the number or code.~~

~~(2) Policy or transaction account. For the purposes of this section, a policy or transaction account is an account other than a deposit account or a credit card account. A policy or transaction account does not include an account to which third parties cannot initiate charges.~~

Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted ~~Marketing~~ Advertising

A. Except as otherwise authorized in this Act, a licensee may not, directly or through any affiliate, disclose for the purpose of targeted advertising any nonpublic personal information about a consumer to a nonaffiliated third party unless the consumer has been provided clear and conspicuous notice and a reasonable opportunity to opt out of targeted advertising in accordance with the requirements of Section 12 of this Act.

B. A licensee shall act on a consumer's request to opt out within 15 business days of receipt.

C. A licensee is under no obligation to obtain additional information to execute the opt-out request.

D. A licensee may not solicit the consumer to change their election to opt ~~-~~out for twelve months.

Commented [LS50]: NAMIC suggests that Section 19 should clarify that processing or disclosure of nonpublic personal information for fraud prevention, fraud detection, identity verification, authentication, security, abuse prevention, or investigation of unlawful conduct is not targeted advertising.

Insurers may use online signals, device information, IP addresses, behavioral indicators, and other data to detect suspicious activity or prevent fraud, and those uses should not be treated as advertising merely because they involve digital processing or analytics.

Commented [LS51]: NAMIC suggests that the WG clarify that targeted advertising does not include first-party communications, contextual advertising, communications in response to a consumer request, service/renewal/claim communications, or processing for measurement, frequency, reach, fraud prevention, security, or compliance purposes.

Commented [LS52]: NAMIC suggests this clarification that 15 days means 15 business days.

© 2026~~17~~ National Association of Insurance Commissioners

E. A consumer has the right to opt out at any time.

Section 20. Limits on Sale of Nonpublic Personal Information

Before a licensee may sell nonpublic personal information:

A. The licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

B. The consumer must affirmatively opt in to the sale of their nonpublic personal information.

Section 21. Limits on Disclosure of Sensitive Personal Information

A. Except as provided by Subsection B below, a licensee may disclose a consumer's sensitive personal information only for those purposes and uses identified in Article VI and as expressly permitted or required by Article VI or other provisions of this Act.

B. Before a licensee may disclose a consumer's sensitive personal information for purposes other than those specified in subsection A of this section:

(1) A licensee shall provide a clear and conspicuous notice to the consumer in accordance with the requirements of Section 11; and

(2) The consumer must affirmatively opt in to disclosure of their sensitive personal information.

Commented [LS53]: NAMIC strongly suggests that this Model not go beyond requirements of other state laws and existing privacy frameworks.

Requiring an opt in to "sale" of NPI will uniquely disadvantage licensees, as other industries (often covered under state privacy laws) are subject to an opt out framework. The issues here are exacerbated by the broad definition of "sell" and could be expected to lead to diminished capacity to leverage modern marketing systems, tools, or partners.

Further, if licensees are communicating less to the public because the marketing arrangement could be considered a "sale" of NPI and they cannot collect mass opt-ins, it is not difficult to imagine how non-licensed actors might try to dominate the insurance sales space and steer consumers away from safe, regulated bodies.

Commented [LS54]: NAMIC suggests that Section 21 should include a fraud-prevention and security exception for sensitive personal information. While sensitive personal information should receive heightened protection, insurers may need to use or disclose limited sensitive information to verify identity, detect fraud, investigate misrepresentation, prevent unauthorized activity, respond to security incidents, or comply with anti-fraud obligations. The exception should be limited to uses and disclosures reasonably necessary for those purposes.

© 2026~~17~~ National Association of Insurance Commissioners

ARTICLE ~~I~~V[I]. EXCEPTIONS TO LIMITS ON DISCLOSURES OF ~~FINANCIAL~~ NONPUBLIC PERSONAL INFORMATION

Section 22~~5~~. Exception to Opt-Out Requirements for Disclosure of Nonpublic Personal ~~Financial~~ Information for Service Providers and Joint Marketing

A. General rule.

(1) The opt-out requirements in Sections 12~~-8~~ and ~~16~~219 do not apply when a licensee provides nonpublic personal ~~financial~~ information to a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf, if the licensee:

(a) Provides the initial notice in accordance with Section ~~9~~57; and

(b) Enters into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in Sections ~~25~~16 ~~or 26~~1723 or 24 in the ordinary course of business to carry out those purposes.

(2) Example. If a licensee discloses nonpublic personal ~~financial~~ information under this section to a financial institution with which the licensee performs joint marketing, the licensee's contractual agreement with that institution meets the requirements of Paragraph (1)(b) of this subsection if it prohibits the institution from disclosing or using the nonpublic personal ~~financial~~ information except as necessary to carry out the joint marketing or under an exception in Sections ~~25~~16 ~~or 26~~1723 or 24 in the ordinary course of business to carry out that joint marketing.

B. Service may include joint marketing. The services a nonaffiliated third party performs for a licensee under Subsection A of this section may include marketing of the licensee's own products or services or marketing of financial products or services offered pursuant to joint agreements between the licensee and one or more financial institutions.

C. Definition of "joint agreement." For purposes of this section, "joint agreement" means a written contract pursuant to which a licensee and one or more financial institutions jointly offer, endorse or sponsor a financial product or service.

Section 23~~16~~. Exceptions to Notice and Opt-Out Requirements for Disclosure of Nonpublic Personal ~~Financial~~ Information for Processing and Servicing Transactions

A. Exceptions for processing transactions at consumer's request. The requirements for initial notice in Section ~~9~~75A(2), the opt-out in Sections 12~~8~~ and ~~16~~219, and service providers and joint marketing in Section ~~24~~1522 do not apply if the licensee discloses nonpublic personal ~~financial~~ information as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Servicing or processing an insurance product or service that a consumer requests or authorizes;

© 2026~~17~~ National Association of Insurance Commissioners

(2) Maintaining or servicing the consumer's account with a licensee, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity;

(3) A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer; or

(4) Reinsurance or stop loss or excess loss insurance.

B. "Necessary to effect, administer or enforce a transaction" means that the disclosure is:

(1) Required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or

(2) Required, or is a usual, appropriate or acceptable method:

(a) To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer's account in the ordinary course of providing the insurance product or service;

(b) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

(c) To provide a confirmation, statement or other record of the transaction, or information on the status or value of the insurance product or service to the consumer or the consumer's agent or broker;

(d) To accrue or recognize incentives or bonuses associated with the transaction that are provided by a licensee or any other party;

(e) To underwrite insurance at the consumer's request or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects or as otherwise required or specifically permitted by federal or state law; or

Drafting Note: States have their own definitions of fraud, and should therefore include and point to that statutory reference in the fraud related provisions within this Draft so as to avoid inadvertent conflicts or discrepancies.

Commented [LS55]: To ensure alignment with state laws and fraud definitions therein, NAMIC suggests this drafting note to allow states to specifically reference and incorporate their fraud statutory references.

(f) In connection with:

(i) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited or otherwise paid using a debit, credit or other payment card, check or account number, or by other payment means;

(ii) The transfer of receivables, accounts or interests therein; or

© 2026~~17~~ National Association of Insurance Commissioners

(iii) The audit of debit, credit or other payment information.

C. For purposes of this section, processing or servicing an insurance transaction includes activities reasonably necessary to detect, prevent, investigate, or respond to fraud, misrepresentation, unauthorized activity, security incidents, identity theft, payment irregularities, or other unlawful conduct related to underwriting, policy administration, billing, claims, subrogation, salvage, recovery, or other insurance operations.

Drafting Note: States have their own definitions of fraud, and should therefore include and point to that statutory reference in the fraud related provisions within this Draft so as to avoid inadvertent conflicts or discrepancies.

Commented [LS56]: NAMIC suggests this inclusion to clarify that processing and servicing insurance transactions includes fraud prevention, fraud detection, investigation, payment integrity, identity verification, authentication, and security activities related to underwriting, policy administration, billing, claims, subrogation, salvage, recovery, and other insurance operations. Fraud controls are integral to insurance transaction processing and should be expressly included.

Commented [LS57]: To ensure alignment with state laws and fraud definitions therein, NAMIC suggests this drafting note to allow states to specifically reference and incorporate their fraud statutory references.

Section 2417. Other Exceptions to Notice and Opt-Out Requirements for Disclosure of Nonpublic Personal ~~Financial~~ Information

A. Exceptions to opt out requirements. The requirements for initial notice to consumers in Section 957A(2), the opt-out in Sections 128 and 1692, and service providers and joint marketing in Section 2419522 do not apply when a licensee discloses nonpublic personal ~~financial~~ information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

(2) (a) To protect the confidentiality or security of a licensee's records pertaining to the consumer, service, product or transaction;

(b) To protect against or prevent actual or potential fraud or unauthorized transactions;

(c) For required institutional risk control or for resolving consumer disputes or inquiries;

(d) To persons holding a legal or beneficial interest relating to the consumer; or

(e) To persons acting in a fiduciary or representative capacity on behalf of the consumer;

(f) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted nonpublic personal information.

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating a licensee, persons that are assessing the licensee's compliance with industry standards, and the licensee's attorneys, accountants and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the federal Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, the Securities and Exchange Commission, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53,

Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance authority, and the Federal Trade Commission), self-regulatory organizations or for an investigation on a matter related to public safety;

(5) (a) To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or

(b) From a consumer report reported by a consumer reporting agency;

(6) In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal ~~financial~~ information concerns solely consumers of the business or unit;

(7) (a) To comply with federal, state or local laws, rules and other applicable legal requirements;

(b) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities; or

(c) To respond to judicial process or government regulatory authorities having jurisdiction over a licensee for examination, compliance or other purposes as authorized by law; or

(8) For purposes related to the replacement of a group benefit plan, a group health plan, a group welfare plan or a workers' compensation plan.

B. Example of revocation of consent. A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under Section ~~12~~8F.~~.~~12F.

Drafting Note: Because the notice requirements of this Act ~~regulation~~ could be a financial burden on a company in liquidation or receivership and negatively impact the ability of the liquidator or receiver to pay claims, regulators may want to consider adding an additional exception providing that licensees in liquidation or receivership are not subject to the notice provisions of this ~~.~~ Act~~regulation~~.

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 2518. When Authorization Required for Disclosure of Nonpublic Personal Health Information

A. A licensee shall not disclose nonpublic personal health information about a consumer ~~or customer~~ unless an authorization is obtained from the consumer ~~or customer~~ whose nonpublic personal health information is sought to be disclosed.

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee: ~~claims administration; claims adjustment and management; detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity; underwriting; policy placement or issuance; loss control; ratemaking and guaranty fund functions; reinsurance and excess loss insurance; risk management; case management; disease management; quality assurance; quality improvement; performance evaluation; provider credentialing verification; utilization review; peer review activities; actuarial, scientific, medical or public policy research; grievance procedures; internal administration of compliance, managerial, and information systems; policyholder service functions; auditing; reporting; database security; administration of consumer disputes and inquiries; external accreditation standards; the replacement of a group benefit plan or workers compensation policy or program; activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit; any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services; disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes; and any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with legal process. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable to the interest of consumers.~~

(1) Claims administration any processing~~claims~~;

(2) Claims adjustment and management;

(3) Detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity;

Drafting Note: States have their own definitions of fraud, and should therefore include and point to that statutory reference in the fraud related provisions within this Draft so as to avoid inadvertent conflicts or discrepancies.

Commented [LS58]: To ensure alignment with state laws and fraud definitions therein, NAMIC suggests this drafting note to allow states to specifically reference and incorporate their fraud statutory references.

(4) Underwriting;

(5) Policy placement or issuance;

(6) Loss control;

(7) Ratemaking and guaranty fund functions;

(8) Reinsurance and excess loss insurance;

© 2026~~17~~ National Association of Insurance Commissioners

(9) Risk management;

(10) Case management;

(11) Disease management;

(12) Quality assurance;

(13) Quality improvement;

(14) Performance evaluation;

(15) Provider credentialing verification;

(16) Utilization review;

(17) Peer review activities;

(18) Actuarial, scientific, medical or public policy research;

(19) Grievance procedures;

(20) Internal administration of compliance, managerial, and information systems;

(21) Policyholder service functions;

(22) Auditing;

(23) Reporting;

(24) Database security;

(25) Administration of consumer disputes and inquiries;

(26) External accreditation standards;

(27) The replacement of a group benefit plan or workers' compensation policy or program;

(28) Activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit;

(29) Any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services or other applicable laws;

(30) Disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes including subrogation, and

(31) Any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with the legal process.

C. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable

Section ~~19~~26. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article VII shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer ~~or customer~~ who is the subject of the nonpublic personal health information;

(2) A general description of the types of nonpublic personal health information to be disclosed;

(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

~~–~~(4) The signature, including electronic signatures, of the consumer ~~or customer~~ who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer ~~or customer~~ may revoke the authorization at any time and the procedure for making a revocation.

(6) Any additional information necessary to comply with HIPAA or any other applicable law.

B. An authorization for the purposes of this Article VII shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer ~~or customer~~ who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article VII at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

E. A signed copy of the authorization shall be provided to the consumer.

Commented [LS59]: NAMIC requests clarification on whether the Authorization needs to be HIPAA compliant for non-protected health insurance.

Section 27.0. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer ~~or a customer~~ as part of an opt-out notice pursuant to Section ~~15~~12, provided that the request and the authorization form are clear and conspicuous. An authorization form is not required to be delivered to the consumer ~~or customer~~ or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section ~~18~~25A.

Commented [LS60]: "Protected health information" is a defined term under HIPAA; to avoid confusion, NAMIC suggests the WG consider alternative phrasing here.

Section 28. Relationship to Federal Rules

A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

This Act shall not apply to nonprofits, such as the National Association of Insurance Commissioners or the National Insurance Crime Bureau, when processing or sharing information solely for investigating criminal or fraudulent insurance acts. ~~Irrespective of whether a licensee is subject to the federal Health Insurance Portability and Accountability Act privacy rule as promulgated by the U.S. Department of Health and Human Services [insert cite] (the "federal rule"), if a licensee complies with all requirements of the federal rule except for its effective date provision, the licensee shall not be subject to the provisions of this Article V.~~

Drafting Note: States have their own definitions of fraud, and should therefore include and point to that statutory reference in the fraud related provisions within this Draft so as to avoid inadvertent conflicts or discrepancies.

Commented [LS61]: To ensure alignment with state laws and fraud definitions therein, NAMIC suggests this drafting note to allow states to specifically reference and incorporate their fraud statutory references.

~~**Drafting Note:** The drafters note that the effective date of this Act regulation is July 1, 2001. The HHS regulation is anticipated to be promulgated in late 2000, thereby becoming effective in late 2002. As of July 1, 2001, if the licensee is in compliance with all requirements of the HHS regulation except its effective date provision, the licensee is not subject to the provisions of this articlethis Article. If the licensee comes into compliance with the HHS regulation after that date, the licensee is no longer subject to the provisions of this aArticle as of the date the licensee comes into compliance with the HHS regulation.~~

Section 29. Relationship to State Laws

Nothing in ~~this article~~this Article shall preempt or supersede ~~supercede~~ existing state law related to medical records, consumer data privacy, health or insurance information privacy.

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 3023. Protection of Fair Credit Reporting Act

Nothing in this ~~regulation~~ Act shall be construed to modify, limit or supersede the operation of the ~~federal~~ Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and no inference shall be made ~~drawn on the basis of the provisions of this regulation Act~~ regarding whether information is transaction or experience information under Section 603 of that Act.

Section 3124. Nondiscrimination

A. A licensee shall not unfairly discriminate against any consumer ~~or customer~~ because that consumer ~~or customer~~ has opted out from the disclosure of his or her nonpublic personal ~~financial~~ information pursuant to the provisions of this ~~regulation~~Act.

B. A licensee shall not unfairly discriminate against a consumer ~~or customer~~ because that consumer ~~or customer~~ has not granted authorization for the disclosure of his or her nonpublic personal health information pursuant to the provisions of this ~~regulation~~Act.

Section 3225. Violation

Drafting Note: Cite state unfair trade practices act or other applicable state law.

Section 3326. Severability

If any section or portion of a section of this ~~regulation~~ Act or its applicability to any person or circumstance is held invalid by a court, the remainder of the ~~regulation~~ Act or the applicability of the provision to other persons or circumstances shall not be affected.

Section 34. Individual Remedies

This Act may not be construed to create or imply a private cause of action for violation of its provisions, nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Commented [LS62]: NAMIC strongly encourages preserving this aspect that private causes of action are not created or implied here. The Working Group might consider bolstering this provision by clarifying that if a state's unfair trade practices act includes a private right of action, Section 34 disallows it.

Section 3527. Effective Date

A. Effective date. This Act~~regulation~~ has been~~is~~ effective since November 13, 2000. The amendments to this Act are effective [Insert Effective Date]. In order to provide sufficient time for licensees to establish policies and systems to comply with the amendments~~requirements~~ to~~of~~ this ~~regulation~~Act, the commissioner has extended the time for compliance with the~~is~~ amendments to this Act~~regulation~~ until [Insert Compliance Date]~~July 1, 2001~~.

B. ~~(1)~~ By [Insert Compliance Date], a licensee shall provide an initial notice, as required by Section 7, to any existing consumer who has not previously received a notice that complies with the amendments to this Act. ~~Notice requirement for consumers who are the licensee's customers on the compliance date. By July 1, 2001, a licensee shall provide an initial notice, as required by Section 5, to consumers who are the licensee's customers on July 1, 2001.~~

~~(2) Example. A licensee provides an initial notice to consumers who are its customers on [Insert Date]July 1, 2001, if, by that date, the licensee has established a system for providing an initial notice to all new customers and has mailed the initial notice to all the licensee's existing customers.~~

C. Two-year grandfathering of service agreements. Until [Insert Compliance Date]~~July 1, 2002~~, a contract that a licensee has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf satisfies the provisions of Section ~~15~~22A(1)(b) of this ~~regulation~~Act, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the licensee entered into the agreement on or before [Insert Compliance Date]~~July 1, 2000~~.

APPENDIX A – SAMPLE CLAUSES

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A-1–Categories of information a licensee collects (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section ~~7A~~9A(1) to describe the categories of nonpublic personal information the licensee collects.

Sample Clause A-1:

We collect nonpublic personal information about you from the following sources:

Information we receive from you on applications or other forms;
Information about your transactions with us, our affiliates or others; and
Information we receive from a consumer reporting agency.

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-1 expires on July 1, 2019.~~

A-2–Categories of information a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use one of these clauses, as applicable, to meet the requirement of Section ~~7A~~9A(2) to describe the categories of nonpublic personal information the licensee discloses. The licensee may use these clauses if it discloses nonpublic personal information other than as permitted by the exceptions in Sections ~~15~~22, ~~16~~ 23 and ~~17~~24.

Sample Clause A-2, Alternative 1:

We may disclose the following kinds of nonpublic personal information about you:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premiums, and payment history"]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your creditworthiness and credit history"].

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-2, Alternative 1 expires on July 1, 2019.~~

Sample Clause A-2, Alternative 2:

We may disclose all of the information that we collect, as described [describe location in the notice, such as "above" or "below"].

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-2, Alternative 2 expires on July 1, 2019.~~

© 2026~~17~~ National Association of Insurance Commissioners

A-3–Categories of information a licensee discloses and parties to whom the licensee discloses (institutions that do not disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirements of Sections ~~7A~~9A(2) and~~,~~ (3)~~, and (4)~~ to describe the categories of nonpublic personal information ~~about customers and former customers that~~ the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses. A licensee may use this clause if the licensee does not disclose nonpublic personal information to any party, other than as permitted by the exceptions in Sections ~~16~~ 23 and ~~17~~24.

Sample Clause A-3:

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-3 expires on July 1, 2019.~~

A-4–Categories of parties to whom a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section ~~7A~~9A(3) to describe the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information. This clause may be used if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections ~~15~~22, ~~16~~ 23 and ~~17~~24~~, as well as when permitted by the exceptions in Sections 16 and 17~~.

Sample Clause A-4:

We may disclose nonpublic personal information about you to the following types of third parties:

Financial service providers, such as [provide illustrative examples, such as "life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents"];

Non-financial companies, such as [provide illustrative examples, such as "retailers, direct marketers, airlines, and publishers"]; and

Others, such as [provide illustrative examples, such as "non-profit organizations"].

We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-4 expires on July 1, 2019.~~

A-5–Service provider/joint marketing exception
A licensee may use one of these clauses, as applicable, to meet the requirements of Section ~~7A~~9A(~~5~~2) related to the exception for service providers and joint marketers in Section ~~15~~22. If a licensee discloses nonpublic personal information under this exception, the licensee shall describe the categories of nonpublic personal information the licensee discloses and the categories of third parties with which the licensee has contracted.

Sample Clause A-5, Alternative 1:

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

Information we receive from you on applications or other forms, such as [provide illustrative examples, such as

"your name, address, social security number, assets, income, and beneficiaries"];

Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premium, and payment history"]; and

Information we receive from a consumer reporting agency, such as [provide illustrative examples, such as "your creditworthiness and credit history"].

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-5, Alternative 1 expires on July 1, 2019.~~

Sample Clause A-5, Alternative 2:

We may disclose all of the information we collect, as described [describe location in the notice, such as "above" or "below"] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-5, Alternative 2 expires on July 1, 2019.~~

A-6–Explanation of opt- out right (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section ~~7A~~9A(~~6~~4) to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. The licensee may use this clause if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections ~~15~~22, ~~16~~ 23 and ~~17~~24.

Sample Clause A-6:

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, you may [describe a reasonable means of opting out, such as "call the following toll-free number: (insert number)].

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-6 expires on July 1, 2019.~~

A-7–Confidentiality and security (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section ~~7A~~9A(8) to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A-7:

We restrict access to nonpublic personal information about you to [provide an appropriate description, such as "those employees who need to know that information to provide products or services to you"]. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

~~**Drafting Note:** The safe harbor of compliance for use of sample clause A-7 expires on July 1, 2019.~~

APPENDIX B – FEDERAL MODEL PRIVACY FORM

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the Federal Model Privacy Form, if the Form is accurate for each institution that uses the Form. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A. General Instructions

1. How the Model Privacy Form is used.

(a) The Model Form may be used, at the option of a "licensee"~~)~~, including a group of licensees or other financial institutions that use a common privacy notice, to meet the content requirements of the privacy notice and opt-out notice set forth in [insert citation for sections of statute or regulation sections that parallel Sections ~~7~~ 9and ~~8~~ 11 of the NAIC *Privacy of Consumer ~~Financial and Health~~ Information ~~Act~~Regulation*]

(b) The Model Form is a standardized form, including page layout, content, format, style, pagination, and shading. Licensees seeking to obtain the safe harbor through use of the Model Form may modify it only as described in these Instructions.

(c) Note that disclosure of certain information, such as assets, income, and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act (FCRA), codified at 15 U.S.C. §§ 1681-1681x, such as a requirement to permit a consumer to opt out of disclosures to affiliates, or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.

(d) The word "consumer~~ustomer~~" may be replaced by the word "member," whenever it appears in the Model Form, as appropriate.

2. The Contents of the Model Privacy Form

The Model Form consists of two pages, which may be printed on both sides of a single sheet of paper or may appear on two separate pages. Where a licensee provides a long list of licensees or financial institutions at the end of the Model Form in accordance with Instruction B3(a)(i), or provides additional information in accordance with Instruction B3(c) and such list or additional information exceeds the space available on Page Two of the Model Form, such list or additional information may extend to a third page.

(a) Page One. The first page consists of the following components:

(1) Date last revised (upper right-hand corner)
(2) Title
(3) Key frame (Why? What? How?)
(4) Disclosure table ("Reasons we can share your personal information")
(5) "To limit our sharing" box, as needed, for the licensee's opt-out information
(6) "Questions" box, for customer service contact information
(7) Mail-in opt-out form, as needed

(b) Page Two. The second page consists of the following components:

(1) Heading (Page 2)
(2) Frequently Asked Questions ("Who we are" and "What we do")
(3) Definitions
(4) "Other important information" box, as needed

3. The format of the Model Privacy Form.

The format of the Model Form may be modified only as described below.

(a) Easily readable type font. Licensees that use the Model Form must use an easily readable type font. While a number of factors together produce easily readable font, licensees are required to use a minimum of 10-point font (unless otherwise expressly permitted in these Instructions) and sufficient spacing between lines.

(b) Logo. A licensee may include a corporate logo on any page of the notice, so long as it does not interfere with the readability of the Model Form or the space constraints of each page.

(c) Page size and orientation. Each page of the Model Form must be printed in portrait orientation, the size of which must be sufficient to meet the layout and minimum font size requirements, with sufficient white space on the top, bottom, and sides of the content.

(d) Color. The Model Form must be printed on white or light color paper (such as cream) with black or other contrasting ink color. Spot color may be used to achieve visual interest, so long as the color contrast is distinctive and the color does not detract from the readability of the Model Form. Logos may also be printed in color.

(e) Languages. The Model Form may be translated into languages other than English.

B. Information Required in the Model Privacy Form

The information in the Model Form may be modified only as described below:

1. Name of licensee or group of affiliated licensees or institutions providing the notice
Insert the name of the licensee providing the notice, or a common identity of the affiliated licensees or financial institutions jointly providing the notice on the form, wherever [name of licensee] appears.

2. Page One

(a) Last revised date. The licensee must insert in the upper right-hand corner the date on which the notice was last revised. The information shall appear in minimum 8-point font as "rev. [month/year]" using either the name or number of the month, such as "rev. July 2016" or "rev. 7/16."

(b) General instructions for the "What?" box

(i) The bulleted list identifies the types of personal information that the licensee collects and shares. All licensees must use the term "Social Security Number" in the first bullet.

(ii) A licensee must use five (5) of the following terms, to complete the bulleted list: income; account balances; payment history; transaction history; transaction or loss history; credit history; credit scores; assets; investment experience; credit-based insurance scores; insurance claim history; medical information; overdraft

history; purchase history; account transactions; risk tolerance; medical-related debts; credit card or other debt; mortgage rates and payments; retirement assets; checking account information; employment information; wire transfer instructions.

(c) General instructions for the disclosure table. The left column lists reasons for sharing or using personal information. Each reason correlates to a specific legal provision described in Paragraph 2(d) of this Instruction. In the middle column, each licensee must provide a "Yes" or "No" response that accurately reflects its information-sharing policies and practices with respect to the reason listed on the left. In the right column, each licensee must provide in each box one of the following three (3) responses, as applicable, that reflects whether a consumer can limit such sharing:

"Yes," if it is required to or voluntarily provides an opt-out; "No," if it does not provide an opt-out; or

"We don't share," if it answers "No" in the middle column.

Only the sixth row ("For our affiliates to market to you") may be omitted at the option of the licensee. See Paragraph 2(d)(6) of this instruction.

(d) Specific disclosures and corresponding legal provisions

(i) For our everyday business purposes. This reason incorporates sharing information under [insert citation for sections of statute or regulation sections that parallel Sections ~~16~~ 23 and ~~17~~ 24 of NAIC model *Privacy of Consumer ~~Financial and Health~~ Information ~~Regulation~~Act*] and with service providers pursuant to [insert citation for section of statute or regulation that parallels Section ~~15~~ 22 of NAIC *Privacy of Consumer ~~Financial and Health~~ Information Act~~Regulation~~*] other than the disclosures described in Paragraphs (2)(d)(ii) or (2)(d)(iii) of this instruction.

(ii) For our marketing purposes. This reason incorporates sharing information with service providers by a licensee for its own marketing pursuant to [insert citation for section of statute or regulation that parallels Section ~~15~~ 22 of NAIC *Privacy of Consumer ~~Financial and Health~~Information ~~Regulation~~Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iii) For joint marketing with other financial companies. This reason incorporates sharing information under joint marketing agreements between 2 or more licensees or financial institutions and with any service provider used in conjunction with such agreement pursuant to [insert citation for section of statute or regulation that parallels Section ~~15~~ 22 of NAIC *Privacy of Consumer ~~Financial and Health~~Information ~~Regulation~~Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iv) For our affiliates' everyday business purposes – information about transactions and experiences. This reason incorporates sharing information specified in Sections 603(d)(2)(A)(i) and (ii) of the FCRA. A licensee that shares information for this reason may choose to provide an opt-out.

(v) For our affiliates' everyday business purposes – information about creditworthiness. This reason incorporates sharing information pursuant to Section 603(d)(2)(A)(iii) of the FCRA. A licensee that shares information for this reason must provide an opt-out.

(vi) For our affiliates to market to you. This reason incorporates sharing information specified in Section 624 of the FCRA. This reason may be omitted from the disclosure table when: the licensee does not have affiliates (or does not disclose personal information to its affiliates); the licensee's affiliates do not use personal information in a manner that requires an opt-out; or the licensee provides the affiliate marketing notice separately. Licensees

that include this reason must provide an opt-out of indefinite duration. A licensee that is required to provide an affiliate marketing opt-out, but does not include that opt-out in the Model Form under this part, must comply with Section 624 of the FCRA and [insert citation for statute or regulation that parallels NAIC *Privacy of Consumer ~~Financial and Health~~ Information Act~~Regulation~~*], with respect to the initial notice and opt-out and any subsequent renewal notice and opt-out. A licensee not required to provide an opt-out under this subparagraph may elect to include this reason in the Model Form.

(vii) For nonaffiliates to market to you. This reason incorporates sharing described in [insert citation for sections of statute or regulation sections that parallel Sections ~~8~~ 11 and ~~12(A)~~16(B) of NAIC *Privacy of Consumer ~~Financial and Health~~ Information Act~~Regulation~~*]. A licensee that shares personal information for this reason must provide an opt-out.

(e) To limit our sharing. A licensee must include this section of the Model Form only if it provides an opt-out. The word "choice" may be written in either the singular or plural, as appropriate. Licensees must select one or more of the applicable opt-out methods described: telephone, such as by a toll-free number; a web site; or use of a mail-in opt-out form. Licensees may include the word "toll-free" before telephone, as appropriate. A licensee that allows consumers to opt out online must provide either a specific web address that takes consumers directly to the opt-out page or a general web address that provides a clear and conspicuous direct link to the opt-out page. The opt-out choices made available to the consumer who contacts the licensee through these methods must correspond accurately to the "Yes" responses in the third column of the disclosure table. In the part entitled "Please note," licensees may insert a number that is 30 days or greater in the space marked "[30]." Instructions on voluntary or state privacy law opt-out information are in Paragraph 2(g)(v) of these Instructions.

(f) Questions box. Customer service contact information must be inserted as appropriate where [phone number] or [web site] appear. Licensees may elect to provide either a phone number, such as a toll-free number, or a web address, or both. Licensees may include the words "toll-free" before the telephone number, as appropriate.

(g) Mail-in opt-out form. Licensees must include this mail-in form only if they state in the "To limit our sharing" box that consumers can opt out by mail. The mail-in form must provide opt-out options that correspond accurately to the "Yes" responses in the third column of the disclosure table. Licensees that require consumers to provide only name and address may omit the section identified as "[account #]." Licensees that require additional or different information, such as a random opt-out number or a truncated account number to implement an opt-out election should modify the "[account #]" reference accordingly. This includes licensees that require customers consumers with multiple accounts to identify each account to which the opt-out should apply. A licensee must enter its opt-out mailing address in the far right of this form (see version 3); or below the form (see version 4). The reverse side of the mail-in opt-out form must not include any content of the Model Form.

(i) Joint accountholder. Only licensees that provide their joint accountholders the choice to opt out for only one accountholder, in accordance with Paragraph 3(a)(5) of these Instructions, must include in the far left column of the mail-in form the following statement:

If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.

□ Apply my choice(s) only to me.

The word "choice" may be written in either the singular or plural, as appropriate. Licensees that provide insurance products or services, provide this option, and elect to use the Model Form may substitute the word "policy" for "account" in this statement. Licensees that do not provide this option may eliminate this left column from the mail-in form.

(ii) FCRA Section 603(d)(2)(A)(iii) opt-out. If the licensee shares personal information pursuant to Section 603(d)(2)(A)(iii) of the FCRA, it must include in the mail-in opt-out form the following statement:

□ Do not share information about my creditworthiness with your affiliates for their everyday business purposes.

(iii) FCRA Section 624 opt-out. If the licensee uses Section 624 of the FCRA, in accord with paragraph 2(d)(6) of these Instructions, it must include in the mail-in opt-out form the following statement:

□ Do not allow your affiliates to use my personal information to market to me.

(iv) Nonaffiliate opt-out. If the licensee shares personal information pursuant to [insert citation for section of statute or regulation that parallels Section ~~12(A)~~16(B) of NAIC *Privacy of Consumer ~~Financial and Health~~ Information-Act~~Regulation~~*], it must include in the mail-in opt-out form the following statement:

□ Do not share my personal information with nonaffiliates to market their products and services to me.

(v) Additional opt-outs. Licensees that use the disclosure table to provide opt-out options beyond those required by Federal law must provide those opt-outs in this section of the Model Form. A licensee that chooses to offer an opt-out for its own marketing in the mail-in opt-out form must include one of the two following statements:

□ Do not share my personal information to market to me. or

□ Do not use my personal information to market to me.

A licensee that chooses to offer an opt-out for joint marketing must include the following statement:

□ Do not share my personal information with other financial institutions to jointly market to me.

(h) Barcodes. A licensee may elect to include a barcode and/or "tagline" (an internal identifier) in 6-point type at the bottom of page one, as needed for information internal to the licensee, so long as these do not interfere with the clarity or text of the form.

3. Page Two

(a) General Instructions for the Questions. Certain Questions on the Model Form may be customized as follows:

(i) "Who is providing this notice?" This question may be omitted where only one licensee provides the Model Form and that licensee is clearly identified in the title on Page One. Two or more licensees or financial institutions that jointly provide the Model Form must use this question to identify themselves as required by [insert citation for section of statute or regulation that parallels Section ~~11(F)~~15(E) of NAIC model *Privacy of Consumer ~~Financial and Health~~ Information Act~~Regulation~~*]. Where the list of licensees or financial institutions exceeds four (4) lines, the licensee must describe in the response to this question the general types of licensees or financial institutions jointly providing the notice and must separately identify those licensees or financial institutions, in minimum 8-point font, directly following the "Other important information" box, or, if that box is not included in the licensee's form, directly following the "Definitions." The list may appear in a multi- column format.

(ii) "How does [name of licensee] protect my personal information?" The licensee may only provide additional information pertaining to its safeguards practices following the designated response to this question. Such information may include information about the licensee's use of cookies or other measures it uses to safeguard personal information. Licensees are limited to a maximum of 30 additional words.

(iii) "How does [name of licensee] collect my personal information?" Licensees must use five (5) of the following terms to complete the bulleted list for this question: open an account; deposit money; pay your bills; apply for a loan; use your credit or debit card; seek financial or tax advice; apply for insurance; pay insurance premiums; file an insurance claim; seek advice about your investments; buy securities from us; sell securities to us; direct us to buy securities; direct us to sell your securities; make deposits or withdrawals from your account; enter into an investment advisory contract; give us your income information; provide employment information; give us your employment history; tell us about your investment or retirement portfolio; tell us about your investment or retirement earnings; apply for financing; apply for a lease; provide account information; give us your contact information; pay us by check; give us your wage statements; provide your mortgage information; make a wire transfer; tell us who receives the money; tell us where to send the money; show your government-issued ID; show your driver's license; order a commodity futures or option trade.

Licensees that collect personal information from their affiliates and/or credit bureaus must include the following statement after the bulleted list: "We also collect your personal information from others, such as credit bureaus, affiliates, or other companies." Licensees that do not collect personal information from their affiliates or credit bureaus but do collect information from other companies must include the following statement instead: "We also collect your personal information from other companies." Only licensees that do not collect any personal information from affiliates, credit bureaus, or other companies can omit both statements.

(iv) "Why can't I limit all sharing?" Licensees that describe state privacy law provisions in the "Other important information" box must use the bracketed sentence: "See below for more on your rights under state law." Other licensees must omit this sentence.

(v) "What happens when I limit sharing for an account I hold jointly with someone else?" Only licensees that provide opt-out options must use this question. Other licensees must omit this question. Licensees must choose one of the following two statements to respond to this question: "Your choices will apply to everyone on your account." or "Your choices will apply to everyone on your account—unless you tell us otherwise." Licensees may substitute the word "policy" for "account" in these statements.

(b) General Instructions for the Definitions. The licensee must customize the space below the responses to the three definitions in this section. This specific information must be in italicized lettering to set off the information from the standardized definitions.

(i) Affiliates. As required by [insert citation for section of statute or regulation that parallels Section ~~7~~9(A)(3) of NAIC *Privacy of Consumer ~~Financial and Health~~ Information ~~Regulation~~Act*], where [affiliate information] appears, the licensee must:

(a) If it has no affiliates, state: "[name of licensee] has no affiliates";

(b) If it has affiliates but does not share personal information with them, state: "[name of licensee] does not share with our affiliates"; or

(c) If it shares with its affiliates, state, as applicable: "Our affiliates include companies with a [common corporate identity of licensee] name; financial companies such as [insert illustrative list of companies]; nonfinancial companies, such as [insert illustrative list of companies]; and others, such as [insert illustrative list]."

(ii) Nonaffiliates. As required by [insert citation for section of statute or regulation that parallels Section ~~7(C)~~(9)(A)(3) of NAIC *Privacy of Consumer ~~Financial and Health~~ Information ~~Act~~Regulation*], where [nonaffiliate information] appears, the licensee must:

(a) If it does not share with nonaffiliated third parties, state: "[name of licensee] does not share with nonaffiliates so they can market to you"; or

(b) If it shares with nonaffiliated third parties, state, as applicable: "Nonaffiliates we share with can include [list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations]."

(iii) Joint Marketing. As required by [insert citation for section of statute or regulation that parallels Section ~~15~~ 22 of NAIC *Privacy of Consumer ~~Financial and Health~~ Information Act~~Regulation~~*], where [joint marketing] appears, the licensee must:

(a) If it does not engage in joint marketing, state: "[name of licensee] doesn't jointly market"; or

(b) If it shares personal information for joint marketing, state, as applicable: "Our joint marketing partners include [list categories of companies such as credit card companies]."

(c) General instructions for the "Other important information" box. This box is optional. The space provided for information in this box is not limited, and an additional page may be used if necessary. Only the following types of information can appear in this box:

(i) State and/or international privacy law information; and/or

(ii) A form by which the consumer may acknowledge receipt of the notice.

Chronological Summary of Actions (all references are to the Proceedings of the NAIC)

2000 Proc. 3rd Quarter 7, 10, 14-36, 904 (adopted).
2002 Proc. 3rd Quarter12, 13, 71, 72-73 (amended).
2017 Spring National Meeting (amended).

© 2026~~17~~ National Association of Insurance Commissioners

Version 1:
Model Form with No Opt-Out

Rev. [insert date]

FACTS	WHAT DOES [Name of Licensee] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores] When you are *no longer* our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

Questions?	Call [phone number] or go to [web site]

© 2026~~17~~ National Association of Insurance Commissioners

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026~~17~~ National Association of Insurance Commissioners

Version 2: Model Form with Opt-Out by Telephone and/or Online

Rev. [insert date]

FACTS	WHAT DOES [NAME OF LICENSEE] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

To limit our sharing	■ Call [phone number] —our menu will prompt you through your choice(s) **or** ■ Visit us online: [web site] **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

© 2026~~17~~ National Association of Insurance Commissioners

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

Rev. [insert date

Version 3: Model Form with Mail-in Opt-Out Form

FACTS	**WHAT DOES [NAME OF LICENSEE] DO WITH YOUR PERSONAL INFORMATION?**
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ▪ Social Security number and [income] ▪ [account balances] and [payment history] ▪ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

© 2026~~17~~ National Association of Insurance Commissioners

Page 2

To limit our sharing	▪ Call [phone number] —our menu will prompt you through your choice(s) ▪ Visit us online: [web site] or ▪ Mail the form below **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

Mail-in Form

Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless your mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me.	
	Name	
	Address	
	City, State, Zip	
	[Account #]	
Mail To:	[Name of Licensee] [Address] [City], [ST] [ZIP]	

Page 3

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ▪ [open an account] or [deposit money] ▪ pay your bills] or [apply for a loan] ▪ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ▪ sharing for affiliates' everyday business purposes—information about your creditworthiness ▪ affiliates from using your information to market to you ▪ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ▪ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ▪ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ▪ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026~~17~~ National Association of Insurance Commissioners

Version 4: Optional Mail-in Form

Mail-in Form	
Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me. **Name** **Address** **City, State, Zip** **[Account #]**
Mail To:	[Name of Licensee], [Address 1], [Address 2], [City], [ST] [ZIP]

NICB National Insurance Crime Bureau

September 22, 2026

Re: Comments on Revised Model #672

Dear Chair Dwyer, Co-Vice Chairs Houdek and Cornelius, and Members:

On behalf of the National Insurance Crime Bureau (NICB), I write to express our appreciation for the Privacy Protections Working Group's open and collaborative efforts on the Full Exposure Draft of Revised Model #672, the *Privacy of Consumer Information Act* ("Exposure Draft"). NICB applauds the balance struck by the Exposure Draft, which ensures fraud-fighters like NICB—in direct partnership with the NAIC—can continue in our mission of combating insurance crimes that needlessly raise costs on all Americans.

With an almost 115-year history, NICB is the nation's premier non-profit organization exclusively committed to detecting, preventing, and deterring insurance fraud and related crimes through intelligence-driven operations. While NICB provides value to our members through education and subject matter expertise, we also serve a significant public benefit by helping regulators and law enforcement stem the estimated billions of dollars in economic harm that insurance crime causes every year.

Key to this work is the ability for industry, regulators, and law enforcement to retain and timely exchange information—pursuant to state reporting obligations—that helps identify and disrupt organized crime and fraud networks. For decades, NICB's Fraud Bureau Reporting Program has worked in direct partnership with the NAIC in ensuring this timely exchange of fraud information through the NAIC's Online Fraud Reporting System (OFRS).

NICB's comments on the Exposure Draft are twofold, as follows, and are guided by our mission stated above.

First, Section 28 ("Relationship to Federal Rules") of the Exposure Draft should remain intact as drafted. Consistent with data privacy laws already enacted in 22 states across the country, the Exposure Draft exempts and thereby protects the vital role of non-profits like the NAIC and NICB—in particular, our joint mission and the pro-consumer benefits of the NICB-NAIC-facilitated exchange of information to combat insurance fraud, financial exploitation, and related crimes—all of which is provided at no cost to state regulators. In this regard, Section 28 of the Exposure Draft strikes an appropriate and well-established balance to protect both privacy and public safety.

NICB Headquarters Office
1515 W. 22nd Street
Suite 1300W
Oak Brook, IL 60523

Phone:
800-447-6282
847-544-7000

NICB.org

Second, to further ensure the protection of vital fraud-fighting information that carriers identify and report to regulators, we recommend the Exposure Draft incorporate language recently adopted by the California legislature in the *Insurance Information and Privacy Protection Act* (SB 354) that protects against the detrimental disclosure or deletion of fraud information that is vital to protecting consumers.

Specifically, NICB would encourage the Working Group to draw from language in SB 354's Sections 791.08(d)(3), 791.09(h), and 791.13(i)(4) that protects the availability and integrity of information used to combat fraud.

In Article III, Section 6(A)(2) of the Exposure Draft—and based on SB 354's Section 791.08(d)(3)—we recommend that licensees not be required to *disclose* "information pertaining to an anticipated or active fraud investigation or the detection or prevention of fraud, or information shared in accordance with the reporting of suspected insurance fraud" under a state's insurance fraud reporting laws.

In Article III, Section 6(C)(2) of the Exposure Draft—and based on SB 354's Section 791.09(h) and 791.13(i)(4)—we also recommend that licensees not be required to *delete* "information pertaining to an anticipated or active fraud investigation or the detection or prevention of fraud, or information shared in accordance with the reporting of suspected insurance fraud" under a state's reporting laws, nor "information related to tracking or detection of fraud or information related to a consumer's claims history."

We thank you for your consideration of our comments. Please contact me if NICB can provide any additional information or assistance.

Respectfully,



Kyle T. McCollum
Vice President
Strategy, Policy, and Government Affairs
National Insurance Crime Bureau



September 22, 2026

Re: Request for comments on Full Draft of Revised Model #672

Thank you for the opportunity for Verisk to provide comments on the Full Draft of Revised Model #672. To best understand our perspective, please note that Verisk and its subsidiaries provide information (including statistics, underwriting and claims information), actuarial analyses, policy language, and consulting and technical services in connection with multiple lines of property/casualty insurance, as well as catastrophe models and information about specific properties. Our customers include insurers and reinsurers, as well as agents, brokers, self-insureds, risk managers, financial services firms, regulators, and various government and law enforcement agencies.

After reviewing the full draft, we offer the following comments:

Fraud Exemptions

Verisk believes that draft Model #672 should include an expanded fraud carve-out covering the detection and prevention of fraud. While individuals may have certain rights under applicable privacy laws to access, correct, or request deletion of personal information, these rights are generally subject to exceptions for fraud prevention, security, law enforcement, and other legitimate business purposes. It is imperative to maintain a fraud detection and prevention carve-out to help ensure that information necessary to detect, investigate, prevent, or prosecute fraudulent activity is not deleted, obscured, or otherwise made unavailable. Allowing individuals engaged in, or suspected of engaging in, fraudulent conduct to access information relating to detection, prevention, investigations or to delete information significantly diminishes its value to the insurance industry and undermines fraud prevention efforts.

The draft addresses detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity under Section 25 (When Authorization Required for Disclosure of Nonpublic Personal Health Information). However, the fraud detection and prevention carve-out found in privacy laws across the country, including the CCPA is not recognized in the draft model. Insurance fraud costs the industry over $308 billion annually, which costs the average U.S. family between $400 and $700 per year in the form of increased premiums.

We suggest utilizing language from recently passed insurance privacy legislation. These clarifications would expand the fraud-carve outs to nonprofits and other entities while supporting consumer protections by preserving fraud-prevention capabilities and maintaining the draft model law’s privacy objectives. Therefore, we have removed the nonprofit carve-out in Section 28 to prevent duplication. Strong fraud protections lower costs for honest policyholders and support Departments of Insurance anti-fraud efforts.

Model Consistency

The draft appropriately recognizes that certain categories of information are already subject to comprehensive federal privacy frameworks, including the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA). The Driver's Privacy Protection Act (DPPA) similarly establishes a detailed federal framework governing the collection, use, disclosure, redisclosure, and protection of personal information obtained from state motor vehicle records. Because DPPA-regulated information is already subject to specific federal restrictions and permitted-use requirements, the absence of a comparable carve-out creates

the potential for overlapping, conflicting, and duplicative compliance obligations. Adding a DPPA provision promotes consistency with the model's treatment of GLBA and HIPAA.

Opt-In Framework

We appreciate the NAIC's goal of enhancing consumer privacy protections; however, privacy legislation enacted across the country by more than half the state legislatures has contained an opt-out framework and an opt-in framework would be a major shift from existing statutes. Insurance operations rely on the responsible use and sharing of information. Requiring affirmative consent for insurance activities would effectively treat consumer nonresponse as a prohibition, potentially limiting a licensee's ability to access information necessary to serve policyholders. In addition, an opt-in approach would introduce substantial operational complexity, increase compliance costs, and create inconsistencies with the long-established GLBA-based privacy framework, which already provides consumers with notice, transparency, and meaningful opt-out rights.

Thank you again for the opportunity to provide comments on the Full Draft of Revised Model #672. We appreciate the Committee's efforts to develop a balanced privacy protection model. Please feel free to contact me should you require additional information concerning our position relative to these matters.

Sincerely,



Nancy Crespo

Proposed Amendments

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

A. A consumer may file the following requests with a licensee, which shall be processed in accordance with the following standards:

(1) Within 45 days of receiving an authenticated request from a consumer for their nonpublic personal information, a licensee shall disclose:

(a) All nonpublic personal information about the consumer that is maintained by the licensee or any contracted third-party service provider; and

(b) A list of all third-party service providers to whom the licensee disclosed the consumer's nonpublic personal information.

(2) A licensee shall not be required to disclose the following:

(a) A consumer's Social Security Number, driver's license number or other government-issued identification number, financial account number(s), any health insurance or medical identification number, any account password(s), security questions and answers, unique biometric data or other information that could create a high risk of identity theft. The licensee may instead disclose the types of nonpublic personal information maintained by listing each type of nonpublic personal information it has about the consumer;

(b) Duplicative nonpublic personal information, if it is described in a manner reasonably understandable by the consumer and the consumer is offered an opportunity to review the nonpublic personal information for inconsistencies; or

(c) Information that is outside the scope of the request, if the consumer has requested only specified items or categories of information.

(d) Information pertaining to an anticipated, suspected, or active fraud investigation or the detection or prevention of fraud, or information shared in accordance with the reporting of suspected insurance fraud under state mandatory fraud reporting, related immunity, and confidentiality statute(s).

Drafting Note: Insert applicable mandatory fraud reporting, related immunity, and confidentiality statute(s).

B. Correction of nonpublic personal information.

(1) A consumer may make an authenticated request for the correction of their nonpublic personal information by filing a request with the licensee that:

(a) Identifies the specific nonpublic personal information the consumer wishes to correct; and

(b) Provides an explanation of why the nonpublic personal information is incorrect.

(2) Within 45 days of receipt of the request under this subsection, a licensee shall take one of the following actions and notify the consumer:

(a) Correct the nonpublic personal information in dispute as requested by the consumer;

(b) Delete the nonpublic personal information in dispute; or

(c) Deny the request and provide:

(i) The basis for refusal to correct the nonpublic personal information as requested;

(ii) Information about how the consumer may appeal the denial; and

(iii) An explanation of how the appeal will be reviewed and how the consumer will be notified of the decision on appeal.

(3) A licensee may deny a request for correction if:

(a) The nonpublic personal information is accurate and complete and if the licensee provides a process for appeal of the decision; or

(b) The nonpublic personal information that is the subject of the request was not created by the licensee, unless there is a reasonable basis to believe that the originator of the nonpublic personal information is no longer available to act on the requested correction, and the consumer has independently demonstrated the information is incorrect; or

(c) The nonpublic personal information that is the subject of the request pertains to an anticipated, suspected, or active fraud investigation or the detection or prevention of fraud, or information shared in accordance with the reporting of suspected insurance fraud under state mandatory fraud reporting, related immunity, and confidentiality statute(s).

Drafting Note: Insert applicable mandatory fraud reporting, related immunity, and confidentiality statute(s).

C. Deletion of nonpublic personal information.

(1) Within 45 days of an authenticated request from a consumer, a licensee shall delete the nonpublic personal information about the consumer that is maintained by the licensee or direct a third-party service provider to delete the nonpublic personal information on the licensee's behalf.

(2) The licensee is not required to delete nonpublic personal information if:

(a) The licensee is required by law or regulation to retain the nonpublic personal information;

(b) The nonpublic personal information may be necessary to perform the contract or service requested by or benefiting the consumer;

(c) The information is necessary to comply with a legal obligation; or

(d) The information is maintained in reasonable anticipation of a claim or civil or criminal proceeding; or

(e) The information pertains to an anticipated, suspected, or active fraud investigation or the detection or prevention of fraud, or information shared in accordance with the reporting of suspected insurance fraud under state mandatory fraud reporting, related immunity, and confidentiality statute(s).

Drafting Note: Insert applicable mandatory fraud reporting, related immunity, and confidentiality statute(s)

(3) A licensee may delay fulfilling a consumer's request, up to 45 days, to delete nonpublic personal information stored on an archived or backup system. A licensee must notify the consumer of such delay.

Section 28. Relationship to Federal Rules

A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

Personal data collected, processed, sold, or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994 (18 U.S.C. § 2721 et seq.) shall be deemed to comply with the requirements of this Act.

~~This Act shall not apply to nonprofits, such as the National Association of Insurance Commissioners or the National Insurance Crime Bureau, when processing or sharing information solely for investigating criminal or fraudulent insurance acts.~~

Section 29. Relationship to State Laws

Nothing in this Article shall preempt or supersede existing state law related to medical records, consumer data privacy, health or insurance information privacy, or other mandatory reporting requirements, related immunity, or confidentiality requirements.

Consumer Representative Comments:

Chris Dion

Christopher L. Dion
Consulting Attorney
expertbiasreport.substack.com
www.exposingexpertbias.com
805.298.1152

August 6, 2026

Re: Comment on the July 24, 2026 Full Exposure Draft of Model #672; Proposed Redline Amendments, and the Draft's Interaction with Model Acts #670, #880, and #900 and Model Regulations #902 and #910

Dear Ms. Neuerburg and Members of the Working Group:

I am a California-licensed attorney whose work for the past decade has focused on the insurance industry's use of financially dependent experts to pretextually deny and underpay claims, which is a form of institutional bad faith, and on the evidentiary record required to identify that practice when it occurs.

This letter follows my comment letter of July 30, 2025 and my inquiry letter of May 18, 2026. Your response of May 21, 2026 directed that the next submission come during the comment period opened for the full exposure draft, that comments focus on the current work, and that the chairs "prefer redlined language where possible." This letter and the accompanying Addendum A are that submission. Addendum A contains fourteen proposed amendments in redline form, keyed to the July 24, 2026 draft, each with its own explanation.

I request four minutes to present these comments orally at the Working Group's open meeting on August 13, 2026 at the Summer National Meeting in Columbus, Ohio. This letter is limited to those matters essential to raising awareness of the issues, and I respectfully reserve the right to supplement this filing in the written comment period closing September 22, 2026.

EXECUTIVE SUMMARY

The issue. This draft authorizes the destruction of records that, in most states, existing retention law does not require a licensee to keep. Three findings combine to produce that result.

1. **The retention rule the states actually adopted measures an insurer's duty by whether its *activities* can be reconstructed.** Model #902 § 4(B) requires

documentation sufficient "to permit reconstruction of the insurer's activities relative to each claim," and the data set at § 4(A) records that a claim was denied and when, with no field for why. Model #910 § 6(A) is better, requiring "claim investigation documentation" and "correspondence used for determining and concluding claim payments or denials." But the NAIC's own state page, ST-910 (Fall 2022), records "NO CURRENT ACTIVITY" for thirty-nine of fifty-one jurisdictions, California, Texas, Florida, Illinois, Pennsylvania, Ohio, Georgia, New Jersey, and Michigan among them. The state page for Model #902 records no activity for sixteen. The states adopted the model that measures the duty by activity and declined the model that names the denial correspondence.

2. **This draft sets the destruction schedule by the licensee's own hand.** Section 5(A)(2) compels a licensee's vendors to destroy records "to meet the record retention requirements of the licensee." The licensee writes those requirements. They are filed with no one and approved by no one: "approval" appears once in the entire draft, at § 25(C), on an unrelated subject; § 9's eight items of required notice content omit retention; and § 13 requires a revised notice only before a new category of third-party disclosure, so a schedule may be shortened without informing anyone.

3. **The current draft of Model #672 supplies no link to the retention law of any state.** Across thirty-five sections it imposes one record-maintenance obligation, at § 6(D)(3)(b), covering the consumer's statement of disagreement. Its § 29 savings clause is confined to Article VII and to privacy subject matter, while the deletion provisions sit in Articles II and III. The one provision addressed to other retention law, § 6(C)(2)(a), grants a permission: a licensee "is not required to delete" what another law requires it to retain.

California illustrates all three. Its claim-file rule, 10 Cal. Code Regs. § 2695.3, sets a five-year period and defines the file's contents by whether "pertinent events and the dates of the events can be reconstructed and the licensee's actions pertaining to the claim can be determined." It enumerates no documents, and the NAIC's state page for Model #910 lists California under "NO CURRENT ACTIVITY." No California claims regulation located here requires a licensee to retain the claim investigation documentation or the report on which a denial rests.

What is asked. Two things. That this Act stop authorizing the destruction of claim-evaluation records, and that it impose a narrow duty to preserve and index them. **The second is a records-retention duty consistent with NAIC model acts and regulations.** It is drafted to supply what Model #900's "general business practice" standard requires and

what Models #902 and #910 leave unpreserved. Fourteen items inside Model #672, set out and explained in Addendum A, and three conforming amendments to Model Regulations #902 and #910.

The records at issue are narrower than claim files generally and exclude the litigation file. Two related categories, gathered in Addendum A as the *claim-evaluation record*: the accountability record behind a retained professional (identity, assignment history, outcome distribution, compensation), and the licensee's own account of why it decided the claim as it did, **whether or not any professional was retained.**

Why they matter. Courts have ordered discovery of other insureds' claim files for at least eleven distinct purposes, catalogued at § II.B. Five involve no retained professional, and a sixth usually does not. Two features of the law make the cross-claim record difficult to substitute for. Model #900 requires proof that conduct occurred "with such frequency to indicate a general business practice," which is a cross-claim standard by construction. And *State Farm Mutual Automobile Insurance Co. v. Campbell*, 538 U.S. 408 (2003), while confirming that other conduct bears on reprehensibility, requires a "nexus to the specific harm suffered by the plaintiff," *id.* at 422, which channels the inquiry toward same-insurer, same-provision, same-stated-reason or grounds evidence.

California and this draft fail in opposite directions. SB 354 kept the destruction mandate (data minimization) and supplied the connection: § 791.13(i)(3)(C) requires a licensee to "securely destroy, delete, or deidentify" information no longer needed, while § 791.39(d) preserves "existing records retention periods," § 791.39(e) preserves discovery rights, and § 791.13(i)(2) requires a written retention schedule "available to the commissioner upon request." This draft dropped the mandate, which is an improvement, and supplied no counterpart to any of those three. Neither instrument produces the records, because a savings clause preserves what exists, and what exists in California is a duration attached to a duty that never reached these records.

Enforcement does not supply the answer. In its Decision and Order of June 9, 2014 in the PacifiCare matter, the California Department of Insurance described the case before it as "the first, and only, UIPA case ever litigated to either a proposed or final decision," adding that "[a]ll the other matters settled long before the litigation and penalty phase." That Decision is reproduced in *PacifiCare Life & Health Insurance Co. v. Lara*, No. G056160, 2022 WL 1315467 (Cal. Ct. App. May 3, 2022) (unpublished); an earlier appeal in the same matter is reported at 27 Cal. App. 5th 391 (2018). The 2014 decision has not become final in the eighteen years since the Order to Show Cause. California is the model's most favorable test, because it adopted Model #900's framework and then set a lower liability threshold. See § IV.E.

I. WHAT IS REQUESTED

This letter asks the Working Group to do two things, and the second is the substantial one:

First, that this Act stop authorizing the destruction of claim-evaluation records. Second, that it impose a duty to preserve and index them, defined narrowly, so that the enforcement models the NAIC has already written can operate as they were designed to.

The second request is a records-retention duty. Proposed § 5A (Addendum item 7) requires a licensee to preserve claim-evaluation records, to index them by source, by policy provision applied, and by decision-maker, and to retain them for stated periods: five years after claim closure for the claim-level records, and ten years for the source's assignment list and compensation record, neither of which contains any consumer's identity. Addendum item 14 supplies its transition rule, and item 8 requires compliance with the retention duties other law already imposes.

The duty is drafted to supply what Model #900 § 3 already requires and what Models #902 and #910 leave unpreserved. Section 3 conditions liability on conduct "committed with such frequency to indicate a general business practice," which is a cross-claim standard; §§ IV.A through IV.C set out what the records models do and do not keep. **Section 5A is drafted to close that gap and to do nothing else.**

The category is defined, and it is narrow. Section 5A reaches claim-evaluation records as Addendum item 3 defines them. It excludes the litigation file and settlement communications. It does not reach claim files at large, and it imposes no general retention obligation on any other record a licensee holds.

The set is severable. Fourteen items amend Model #672. Item 7 is the substantial request and is identified as such wherever it appears. Three further amendments, at § V.C, address Model Regulations #902 and #910, because the destruction this draft authorizes and the retention those regulations require form one question. Where within the NAIC each amendment is taken up is a matter for the NAIC.

Section 33 of the draft is a broad severability clause, and every request in Addendum A stands independently of every other. The Working Group may adopt one, several, or all fourteen.

II. THE RECORDS AT ISSUE, AND THE USES THEY SERVE

A. Why the opinion alone will rarely answer the question

Claim decisions in contested matters frequently rest on the opinion of a retained professional: a medical reviewer's finding that a claimant is not disabled, an industrial hygienist's conclusion about contamination, a forensic engineer's causation opinion. These opinions are generally experientially based, which is to say professional judgments drawing on training and experience rather than on a method whose error rate or external benchmark can be examined on the face of the opinion.

What arrives in the claim file is a conclusion. A single file will sometimes disclose bias directly, through an internal communication or an abandoned first opinion, and where it does the cross-claim record is unnecessary. More often the principal available measure is the reviewer's record across many claims of the same kind: whether comparable inputs produce systematically one-sided outputs, whether stated criteria are applied consistently, and whether the licensee selects the reviewer because the record makes the outcome predictable. Those indicators are held in records other than the claimant's own file.

B. Eleven purposes for which courts already order this discovery

The Working Group is not being asked to recognize a new use for these records. A review of the reported decisions in which discovery of other insureds' claim files was sought or ordered yields at least eleven distinct evidentiary purposes. The list is **not exclusive**.

1. **Biased subjective or experiential opinions**: to show biased opinions and lack of credibility supporting a breach-of-contract claim.
2. **Erroneous or inconsistent opinions**: to show the reviewer's erroneous or inconsistent interpretation or application of principles, methodologies, and facts.
3. **Interpretation or application of policy terms**: to show the insurer's erroneous or inconsistent interpretation of policy terms across insureds.
4. **Biased claim investigations**: to show selection or compensation bias supporting a bad-faith claim.
5. **Bad-faith claims adjusting**: to show specific bad-faith patterns and practices.
6. **Genuine-dispute doctrine**: to oppose the insurer's genuine-dispute defense by showing the investigation was biased and unfair.
7. **Insurer's intent**: to show conscious disregard supporting a bad-faith claim.

8. **Excusable error**: to oppose the insurer's mistake, inadvertence, or negligence defense.
9. **Punitive damages**: to show conscious disregard and recidivist conduct.
10. **Unfair practices laws**: to show a violation of a state unfair claims settlement practices act, unfair trade practices act, or unfair competition law.
11. **Class certification**: to identify other insureds whose claims share common policy provisions or claim-handling practices.

Two observations follow. *First, a substantial share of these purposes concern the licensee's own personnel rather than any expert.* Purposes 3, 5, 8, 10, and 11 involve no retained professional, and purpose 7 usually involves none. They concern which provision the adjusters applied, what they relied upon, and whether they construed the same language the same way for the next insured. **This is why the preservation duty at Addendum item 7 applies whether or not an expert was retained.** A duty drawn narrowly around expert bias would preserve the record in the claims where a second independent record already exists, and destroy it where the licensee's own correspondence is the only record there is.

Second, the same condition defeats all eleven. Courts have resolved privacy objections for four decades by the mechanisms described at § II.D, so privacy leaves each purpose intact. The absence of the records defeats every one, and deletion is unappealable, unreviewable, and invisible.

The underlying case catalog can be supplied on request and is expected to accompany the September 22 submission.

C. Two illustrations

In *Hangarter v. Provident Life & Accident Insurance Co.*, 373 F.3d 998 (9th Cir. 2004), cross-claim discovery established that a reviewing physician had found against the claimant in thirteen of thirteen reviews. In *Bagramyan v. Government Employees Insurance Co.*, No. B315018 (Cal. Ct. App. 2023), the court affirmed judgment for the insurer because the plaintiff could not establish an inference of bias, and then enumerated the categories of evidence that would have sufficed: outcome rates across retentions, financial-dependence metrics, and priming evidence. Each of those categories resides in the claim files of other insureds.

Where the records exist, the practice is provable. Where they are gone, the claim fails for want of the evidence that would identify the practice, whether or not the practice occurred.

D. Courts have already reconciled privacy with access

Courts have reconciled the preservation of these records with consumer privacy for four decades, through protective orders, temporal and geographic narrowing, redaction, and opt-in consent procedures for sensitive health information. **A protective order preserves both the privacy interest and the evidence. Deletion eliminates the evidence, and with it the setting in which the privacy question arose.**

Addendum A item 4 is built on this point. It asks that de-identification be permitted to remove the consumer's identity from the analytical record while preserving the linkages among source, methodology, outcome, and compensation, and among the policy provision applied, the reason given, the decision-maker, and the disposition. It asks for a better de-identification standard, not a weaker one.

The consumer's identity is absent from the retained records and cannot be recovered from them by any third party. It remains recoverable by the licensee, through a segregated and access-controlled association required at Addendum item 8, and only to give a consumer notice and an opportunity to consent or object before their identity is produced. This is pseudonymization of the analytical record rather than irreversible anonymization, deliberately so: a regime that destroyed the association would destroy the mechanism courts have used to reconcile these interests, because an opt-in letter presupposes that someone can address it. *Van Duyn v. American Security Insurance Co.*, No. CV 08-5748-GW(CTx), 2009 WL 10672575 (C.D. Cal. Apr. 14, 2009), is representative. The court weighed the Gramm-Leach-Bliley Act and the California Financial Information Privacy Act against the discovery need under Rule 26, and ordered an opt-in letter offering non-party insureds a choice between release of the claim file without restriction and release with the insured's "name, address, telephone numbers, and all other identifying information deleted from it." *Id.* at 4. Insureds electing the second level "may respond by including only their claim number in lieu of a signature, name, and address." *Ibid.*

One further point. A retained physician, engineer, or file reviewer is a commercial counterparty of the licensee rather than a consumer, and that person's identity, assignment history, and compensation are accordingly outside "nonpublic personal information" under §§ 4(Q) and 4(R)(1) and outside the Act's scope under § 2(A)(1). Preserving the accountability record costs this Act's privacy purpose nothing.

III. THE JULY 24, 2026 DRAFT

A. The Act's single record-maintenance obligation

Across thirty-five sections, the one affirmative record-maintenance obligation is § 6(D)(3)(b), which requires a licensee to maintain the consumer's written statement of disagreement with a refusal to correct or delete.

B. The provisions that authorize destruction

1. Deletion on request, reaching closed files. Section 6(C)(1) requires that "[w]ithin 45 days of an authenticated request from a consumer, a licensee shall delete the nonpublic personal information about the consumer." Section 6(D)(2) provides that "[t]here shall be no cap on the number of requests." Nothing limits the right to open or recent claims.

2. Every exception is permissive, including the one addressed to other law. Section 6(C)(2) provides that "[t]he licensee **is not required to delete** … if" one of four conditions obtains. The form of that sentence governs all four.

Subparagraph (a) applies wherever another law requires retention. In California a closed claim file is such a record, because 10 Cal. Code Regs. § 2695.3(b)(3) requires claim files to be kept "for the current year and the preceding four years." So this Act addresses the conflict between its own deletion command and a state retention rule, and resolves it by telling the licensee that it *may* obey the state rule. A licensee that deletes instead has complied with the mandatory sentence at § 6(C)(1) and passed up an option. **Addendum A item 8 makes subparagraph (a) mandatory. That is one sentence, and it creates no retention duty; it requires compliance with duties that already exist elsewhere.**

Subparagraph (d) applies where information "is maintained in reasonable anticipation of a claim or civil or criminal proceeding." Whether one insured's file survives for the benefit of a different insured's proceeding rests with the party who would be the defendant in it. Subparagraph (d) is also not by its terms limited to a proceeding involving the requesting consumer, which is correct as drafted and which Addendum item 8 asks the Working Group to confirm, because the narrowing reading will be argued.

3. Vendor-side destruction on a schedule this Act leaves unregulated. Section 5(A)(2) requires the licensee's contract to compel a third-party service provider "to delete nonpublic personal information after it is no longer necessary to fulfill a legal requirement or **to meet the record retention requirements of the licensee**." The licensee sets that schedule, this Act leaves it unregulated, and the model then compels the vendors to run on it. Because expert reports, referral instructions, and compensation records are frequently held by vendors, this is the provision that reaches the records this letter concerns.

The schedule is filed with no one and approved by no one. "Approval" appears once in this draft, at § 25(C), where additional insurance functions "may be added with the approval of the commissioner." Nothing requires a licensee to file its retention schedule or obtain approval of it. Section 9, listing what a Notice of Information Practices must contain, enumerates eight items, and retention is absent. Section 9(D)(1) provides that "[l]icensees are not required to use any prescribed clauses or model form." And § 13 requires a revised notice only before disclosure of a new category of information to a nonaffiliated third party, so shortening a schedule triggers nothing. The nearest thing to review anywhere in the NAIC's records models is Model #910 § 9(B), which requires computer-based records to be maintained under "written procedures developed and adhered to by the insurer," available "to the commissioner during an examination." That is availability after the fact.

4. De-identification as an unregulated alternative. Section 5(A)(2) authorizes "de-identify" as an alternative to deletion. Section 4(J) defines de-identified data, and § 4(Q) excludes it from "nonpublic personal information" and therefore from the Act. Nothing constrains *how* de-identification is performed. A licensee that strips source identifiers, or partitions records so that outcome no longer joins to source, destroys the analytical value of the category without performing a "deletion." No deletion has occurred for anyone to challenge.

C. The current draft authorizes what the earlier drafts commanded

The Working Group has dropped the standalone data-minimization article that appeared in earlier drafts. That is an improvement. The change is from a command to a permission, and in this setting the two tend to produce the same records at the end: the decision belongs to a party whose interest runs one way, no minimum retention period constrains it, and the choice carries no consequence. **The Act does not order the file destroyed. It removes every reason not to.**

D. California and this draft, compared

A legislature has examined provisions of this kind twice, and the two instruments diverge in opposite directions on the two questions that decide whether records survive.

The destruction command. California kept it; this draft dropped it. SB 354's findings state data minimization as a governing purpose, § 791.13(i)(1) requires that retention "be reasonably necessary and proportionate," and § 791.13(i)(3)(C) provides that once information "is no longer needed," a licensee "shall take reasonable steps to securely destroy, delete, or deidentify" it. This draft carries no counterpart.

The connection to existing retention law. California supplied it; this draft did not. The May 23, 2025 version of SB 354 made no reference to existing records-retention law, preempted inconsistent state law, and exempted its implementing regulations from the Administrative Procedure Act. The July 25, 2026 version differs in four respects:

- The Administrative Procedure Act exemption is **gone**.
- Section 791.39(d): *"This article shall not be construed to reduce or eliminate any existing records retention periods or supersede any legal requirements pertaining to records retention."*
- Section 791.39(e): *"This article shall not be construed to abridge or limit the rights of litigants, including parties to administrative proceedings, under the laws, or case law, of discovery of this state."*
- Section 791.13(i)(2) requires a licensee to "develop a written records retention policy and records retention schedule and shall make it available to the commissioner upon request," reviewed at least every three years.

The July 24 draft contains no counterpart to any of the four.

A savings clause is only as strong as the duty it saves. Section 791.39(d) preserves what exists and creates nothing. In California what exists is § 2695.3: a five-year period attached to a duty whose content is fixed by the chronology test at § 2695.3(a), and which enumerates no documents. See § IV.C. **So in California that clause preserves a duration. It does not preserve a requirement that the report behind a denial or the claim investigation documentation be kept, because no located California claims regulation imposes one.**

Neither instrument produces the records. The lesson is therefore narrower than adopting California's language, and this letter does not propose that: **a legislature that examined provisions of this kind closely concluded that an article of this kind requires an express records-retention savings clause, an express discovery savings clause, and a written schedule the regulator can ask to see.** Addendum item 12 supplies the records-retention savings clause and item 13 the discovery protection, and item 8 requires compliance with the retention law those clauses would preserve. Items 3 and 7 do what no savings clause can, by naming the category the retention law never named.

This letter takes no position on whether the California bill resolves the concerns raised about it in that forum, and further concerns continue to be raised there. No inference is drawn about how either instrument came to contain what it contains.

E. Three provisions that will supply the answering argument

Section 6(D)(1)(b)(i) excuses compliance where information "is not locatable or retrievable by the licensee," and its Drafting Note directs examiners to review a licensee's irretrievability justifications. There is no counterpart Drafting Note for deletion decisions. The review attaches to the licensee's claim that it *cannot* produce, and not to its decision that it *need not* preserve.

Section 28 deems a HIPAA-governed licensee that "maintains nonpublic personal information in the same manner as protected health information" to be "deemed to comply with the requirements of this Act." Health claims are where independent medical examination, file review, and peer review practices concentrate, so without a conforming change a health insurer could assert blanket deemed compliance.

Section 29 provides that "[n]othing in this Article shall preempt or supersede existing state law related to medical records, consumer data privacy, health or insurance information privacy." It is limited to Article VII, while the provisions authorizing destruction sit in Articles II and III. The Working Group recently revised this clause to add "consumer data privacy," having therefore revisited what belongs in it, and records retention is still not among the subjects.

IV. THE OTHER MODELS, AND WHAT THEY REQUIRE TO BE KEPT

A. The enforcement models require cross-claim proof: Models #900 and #880

Model #900 § 3 provides that it is an improper claims practice to commit an act defined in § 4 if "[i]t is committed **flagrantly and in conscious disregard** of this Act" or "[i]t has been committed with such **frequency to indicate a general business practice**." Liability requires either flagrancy or frequency.

Section 4(C) ("Failing to adopt and implement reasonable standards for the prompt investigation and settlement of claims") and § 4(F) ("Refusing to pay claims without conducting a reasonable investigation") are the provisions a systematically biased expert practice violates. They are also the provisions a single file will rarely establish, because on the face of any one file the licensee did investigate: it retained a credentialed professional and relied on the report. Model #880 is built the same way. **The NAIC's enforcement model requires the category of evidence its records models leave unpreserved.**

B. What Models #902 and #910 require a licensee to keep

1. The duty measures what the insurer did, and not what it relied upon. Model #902 § 4(B) states the whole documentation requirement in one sentence: "[d]etailed documentation shall be contained in each claim file in order to permit reconstruction of **the insurer's activities** relative to each claim." A claim file showing every step the adjuster took, in order, with dates, satisfies that sentence. Section 4(A) confirms it by enumerating the data an insurer must produce: "the claim number, line of coverage, date of loss and date of payment of the claim, date of denial or date closed without payment." Six items, recording that a claim was denied and when, with no field for why.

2. The one model that does better has largely not been adopted. Model #910 § 6(A) uses the same measure in its opening sentences, requiring claim files "sufficiently clear and specific so that pertinent events and dates of these events can be reconstructed." But it then provides that a claim file "shall, **at a minimum**, include the following items," and that list operates as a floor. Two listed items reach the substance of a decision in all three lines of business: "claim investigation documentation" and "correspondence used for determining and concluding claim payments or denials." A third, "any claim manuals or other information necessary for reviewing the claim," appears in the property and casualty list at § 6(A)(1) and in neither § 6(A)(2) nor § 6(A)(3). Model #910 therefore requires the denial correspondence to be kept.

The NAIC's own state page for that model, ST-910 (Fall 2022), records "NO CURRENT ACTIVITY" for thirty-nine of the fifty-one jurisdictions listed, and a citation for twelve. Among the thirty-nine are California, Texas, Florida, Illinois, Pennsylvania, Ohio, Georgia, New Jersey, and Michigan. The state page for Model #902 (Fall 2023) records no activity for sixteen. **The states adopted the model that measures the duty by the insurer's activities and declined the model that names the denial correspondence.** These are the NAIC's own compilations; the NAIC states that they are not formal legal opinions and that readers should consult state law, and they are cited here for the pattern rather than for the status of any particular state.

3. The expert record is never named. The terms "expert," "consultant," "independent medical," "peer review," "engineer," and "appraiser" appear zero times in Model #900, #902, and #910. Model #910 § 6(A)(1) lists the property and casualty claim file down to police reports and salvage documentation, and omits the report on which a denial rests where the denial rests on a retained professional, along with what that professional was paid. The health list at § 6(A)(3) comes closest, with "health facility pre-admission certification or utilization review documentation," showing that the drafters named a reviewer's work product where they intended to, in one line of business.

4. The duty is defined by the examiner's needs, and confined to the single claim. Model #902 § 4 opens "To aid in such examination"; Model #910 § 2 states its purpose as retention "for market conduct purposes"; Model #910 § 4(A) requires records so the commissioner can ascertain compliance "during an examination." **A duty defined by its beneficiary will be read to end where that beneficiary's interest ends**, which is why a minimum retention period tends to be treated as the maximum. The same construction confines it to the individual claim: Model #902 § 4(B) reaches the insurer's activities "relative to each claim," which leaves out the reviewer's other assignments and the outcome distribution across them. Compensation sits further outside still. What a licensee pays a claim-evaluation source is ordinarily held in its accounting records, under the vendor, and not in any claim file, so no claim-file rule was ever going to reach it.

5. Duration. Model #902 § 4(A) requires data for "the current year and the two preceding years." Model #910 § 6(A) requires the claim file for "the calendar year in which the claim is closed plus three (3) years," with a Drafting Note contemplating five years for some states. Both are shorter than the period over which a pattern becomes visible.

The NAIC already knows how to write a records-integrity rule. Model #910 § 9(B) requires computer-based records to be "archival in nature, so as to preclude the alteration of the record after the initial transfer." Addendum A asks the NAIC to extend requirements it has already written.

C. California's claims regulations, and the conflict already in place

California's Fair Claims Settlement Practices Regulations, 10 Cal. Code Regs. § 2695.3, impose a documentation and retention duty in three parts. **Subsection (a)** requires claim files to "contain all documents, notes and work papers (including copies of all correspondence) which reasonably pertain to each claim **in such detail that** pertinent events and the dates of the events can be reconstructed **and** the licensee's actions pertaining to the claim can be determined." **Subsection (b)(1)** requires claim data "accessible, legible and retrievable for examination," available "for the current year and the four preceding years." **Subsection (b)(3)** requires that claim files "be maintained for the current year and the preceding four years."

First, the words that set the measure describe a chronology. Events, dates, and what the licensee did. A file permitting complete reconstruction of the sequence satisfies subsection (a), whether or not it records the facts and opinions relied upon, the policy language applied, or the reason given. Subsection (b)(1) confirms it: the required data is claim number, line of coverage, dates, and whether the claim was accepted, denied, or closed without payment. As in Model #902 § 4(A), there is no field for why.

Second, the regulation enumerates no documents, and no California analogue to Model #910 has been located. The NAIC's ST-902 state page records this subchapter as California's counterpart to Model #902. Its ST-910 state page lists California under "NO CURRENT ACTIVITY." So the one place in the NAIC's models where a claim file must contain "claim investigation documentation" and "correspondence used for determining and concluding claim payments or denials" appears to have no California counterpart. **No located California claims regulation requires a licensee to retain the claim investigation documentation or the report on which a denial rests.** This is a statement about what has been located, and about claims regulations. California may impose record-retention obligations elsewhere in its law; none bearing on claim handling has been found.

Third, the five-year duty this draft would override is real, and these regulations are not marginal. Section 6(C)(1) requires deletion within forty-five days, and the draft speaks to the conflict only at § 6(C)(2)(a), which says the licensee may keep the file. Section 29 does not reach it, for the reasons at § III.E. These are also the regulations at issue in the one adjudicated enforcement action described at § IV.E: the insurer there challenged §§ 2695.1(a), 2695.2(l), and 2695.2(y) as facially invalid, prevailed below, and was reversed on appeal, which upheld all three. Section 2695.3 was itself never litigated, but the subchapter containing it is the one an insurer contested for a decade.

D. *Campbell*, and the case for an affirmative duty

Two features of *State Farm Mutual Automobile Insurance Co. v. Campbell*, 538 U.S. 408 (2003), bear on what this draft would permit.

The nexus requirement. *Campbell* confirms that a defendant's other conduct is probative of reprehensibility while constraining which other conduct qualifies. Such conduct "must have a nexus to the specific harm suffered by the plaintiff." *Id.* at 422. "A defendant's dissimilar acts, independent from the acts upon which liability was premised, may not serve as the basis for punitive damages." *Id.* at 422–423. Read together, these direct the inquiry toward evidence of conduct **similar** to that which harmed the plaintiff: the same insurer, the same provision, the same stated reason, the same reviewer. That evidence resides principally in the licensee's own records, and is usable only where the licensee has kept them and can retrieve them by something other than claim number.

Why an anti-destruction rule alone would be insufficient. Justice Ginsburg's dissent, quoting the trial court, recites that State Farm made "systematic" efforts to destroy internal documents "that might reveal its scheme"; that an in-house attorney "instructed Utah claims management to search their offices and destroy a wide range of material of the sort

that had proved damaging in bad-faith litigation in the past"; and that State Farm "admitted that it destroyed every single copy of claim-handling manuals … on file in its historical department as of 1988." *Id.* at 434–435 (Ginsburg, J., dissenting) (quoting the trial court). The finding that matters most here follows: the trial court found that "in recent years State Farm has gone to **extraordinary lengths to stop damaging documents from being created in the first place**," and that the company "kept no records at all on excess verdicts in third-party cases, or on bad-faith claims or attendant verdicts." *Id.* at 435.

This is the dissent's recitation of the trial court's findings, offered as illustration. It is no holding of the Court, and no conduct is attributed to any present licensee. The point is one about drafting: **a rule prohibiting destruction answers the first set of findings and leaves the second untouched.** Where the aggregate record is never compiled, there is nothing to destroy and nothing to preserve, every individual claim file remains complete, and no litigant can point to a missing document. That is why Addendum item 7 asks for a duty to preserve **and to index**. A savings clause preserves a cause of action; an indexing requirement causes the underlying evidence to exist.

It is noted with appreciation that § 34 of the July 24 draft has been revised to add that the Act may not "be construed to curtail a private cause of action which would otherwise exist in the absence of this Act." Addendum item 13 is drafted to build on that clause rather than to strike it.

E. Enforcement

This section describes a result produced by the ordinary operation of the models' own design, and implies no criticism of any regulator. It is confined to California and rests on one matter, described from the filings in it.

The finding. In its Decision imposing the largest penalty in the Department's history, the California Department of Insurance described the matter before it in its own words:

"[T]his is the first, and only, UIPA case ever litigated to either a proposed or final decision. All the other matters settled long before the litigation and penalty phase."

The Unfair Insurance Practices Act, Insurance Code § 790 et seq., is California's enactment of the framework Model #900 carries, added by Stats. 1959, ch. 1737. The statement appears in the Commissioner's Decision and Order of June 9, 2014, which was later set aside on judicial review; the sentence quoted is the Department's account of its own enforcement history, and nothing in the subsequent proceedings has disturbed it. Matters were initiated, and settlement disposed of all of them before any adjudication. **The finding is bounded, and correction of it is invited.** It says nothing about consent orders,

complaint mediation, or market conduct examinations, none of which adjudicates. If the NAIC holds data showing a materially different picture, that data would change the analysis and would be welcome.

What the one adjudicated case produced. In May 2007 the Department opened a targeted market conduct examination of a health insurer's claims handling, concluding that the insurer had violated the Insurance Code nearly one million times and recommending penalties of approximately $325 million. The Order to Show Cause issued January 25, 2008. The evidentiary hearing ran from December 7, 2009 to June 27, 2013: more than 230 hearing days, more than 60 witnesses, some 2,000 exhibits, and a record exceeding 50,000 pages. On August 5, 2013 the administrative law judge found 883,735 violations and proposed a penalty of $11,518,350. On June 9, 2014 the Commissioner rejected that proposed decision, found 908,547 violations, imposed a penalty of $173,603,750, and designated the decision a precedent decision.

Nothing in that decision has taken effect. On judicial review the trial court invalidated three of the claims-handling regulations and then, in September 2017, set aside all nineteen penalty categories. The Court of Appeal reversed the regulatory ruling and upheld all three regulations, *PacifiCare Life & Health Ins. Co. v. Lara*, 27 Cal. App. 5th 391 (2018), then reversed the penalty judgment as well and remanded for what it called a do-over, No. G056160, 2022 WL 1315467 (Cal. Ct. App. May 3, 2022). On remand the matter was retried. In August 2023 judgment was again entered for the insurer, and a writ issued directing the Commissioner to vacate the administrative decision.

In April 2024 the trial court awarded the insurer $66,153.13 in costs. The largest component, $49,827.50, was the insurer's attorney fees for preparing the administrative record of the Department's own enforcement action, awarded on a finding that the Commissioner had not produced an adequate record in the twelve months after the insurer requested it, and that the insurer's work assembling a complete one was "not just reasonable, but essential." **That finding deserves attention in a letter about records.** A records regime built to serve the examiner failed to produce a usable evidentiary record even for the examiner, in the one case where everything depended on it.

Two appeals remained pending as of the most recent filing reviewed here, the Commissioner's reply brief of January 9, 2026. Eighteen years after the Order to Show Cause there has been no final adjudication of the underlying conduct. *This account is drawn from the filings and ends at January 9, 2026. The costs award is itself on appeal and is not final.*

Why California is the model's most favorable test. The natural inference is that California's statute is weak or its Department under-resourced. California in fact adopted a liability threshold lower than Model #900's. Where § 3 of the model reaches an act "committed flagrantly and in conscious disregard of this Act," California's § 790.03(h) reaches acts "[k]nowingly committing or performing with such frequency as to indicate a general business practice." Knowledge is the lower bar, and it is lower by a wide margin for a practice conducted through credentialed intermediaries, which is built to look measured. A jurisdiction took the model, made liability easier to establish, and applied the result to an insurer against which its own examiners had found nearly a million violations. The result was one adjudicated case in sixty-seven years and no final determination in eighteen.

The two statutes also differ in the penalties they authorize, and this letter leaves that difference out deliberately. The size of an authorized penalty explains what an action recovers and says nothing about whether one is brought. The constraint lies in the procedural and economic reality of contested adjudication conducted by a sole public enforcer, and Model #900 § 1, Model #910 § 1, and § 34 of this draft each bar a private right of action, making the enforcer sole.

Model #670. A search of California's counterpart to the model this draft would replace has located no enforcement action in approximately forty-five years. California enacted Model #670 as the Insurance Information and Privacy Protection Act, Insurance Code § 791 et seq., in 1980; the Senate Judiciary Committee's analysis of SB 354 records that "[t]he IIPPA was enacted in 1980, well before the digital revolution transformed how data is collected, stored, and shared." This finding rests on a search of reported decisions and publicly available administrative records. It does not capture consent orders, unappealed administrative actions, or informally resolved matters, and it concerns one state. If the framework being replaced has not operated, then what this draft adds is a set of deletion provisions layered onto a protection with no demonstrated enforcement history. The Working Group is in a position to establish or refute that premise.

Two further lines of analysis are reserved for the September 22 comment period: the comparative enforcement records of insurance commissioners and of the attorneys general and privacy agencies that enforce general consumer-privacy statutes against insurers; and the 2004 multistate regulatory settlement concerning disability claim handling.

F. The questions posed in May, which remain open

The inquiry letter of May 18, 2026 posed twenty-one requests for information. The May 21 response confirmed that the chairs had reviewed the letter and directed that comments be filed in the present window. **It did not address any of the twenty-one questions.** They are respectfully renewed, with an emphasis on the following five:

Each asks for identification of specific matters and materials. Where the NAIC holds no responsive information, a statement to that effect would be equally useful, and is requested in the alternative.

1. **Adjudicated enforcement under Models #900 and #880.** Please identify each matter under Model #900, Model #880, or a state counterpart that has been litigated to a proposed or final decision determining that an insurer engaged in an unfair claims settlement practice, giving for each the jurisdiction, the case or docket name and number, the date of decision, and the disposition. Consent orders, informal resolutions, and examinations closed without adjudication are outside the request. Please also identify any database, compilation, or examination-tracking record from which the NAIC or its members draw such matters, and any guidance, analysis, or survey addressing what a state must show to establish the "general business practice" element of Model #900 § 3.

2. **Model #670 enforcement.** Please identify each enforcement action brought under Model #670 or a state counterpart in any jurisdiction, giving the jurisdiction, the respondent, the citation or docket number, the date, and the disposition. The search described at § IV.E located none under California's counterpart in approximately forty-five years, and it reaches one state and does not capture consent orders or informally resolved matters, so any list the NAIC holds would materially change the analysis in this letter.

3. **The retention of financially dependent experts.** Please identify each enforcement action, investigation, market conduct examination finding, regulation, bulletin, or written guidance, in any jurisdiction, addressing an insurer's retention, selection, supervision, or compensation of a person whose opinion is relied upon in evaluating a claim. Citations or docket numbers, jurisdictions, and dates are requested for each.

4. **The conflict with Model Regulation #902 and with state claims regulations.** Please identify any analysis, memorandum, drafting note, staff assessment, or comment received by the Working Group addressing the interaction between this draft's deletion provisions and Model Regulation #902's claim-file retention and documentation requirements, or the corresponding state regulations. Please also

state which instrument the NAIC understands to control where this draft permits destruction of a record that #902, or a state regulation adopted from it, requires an insurer to retain. Section IV.C sets out California's, which requires five years and which this draft would override on forty-five days' notice.

5. **What remains.** Please identify any assessment the NAIC has made of what enforcement mechanism for Models #900 and #880 remains available if the cross-claim record on which both regulators and private litigants depend may lawfully be destroyed on the licensee's own schedule, together with any document in which that assessment is recorded.

These are questions the amendments are designed to make unnecessary. If the answers show an active enforcement record, the amendments cost the NAIC very little, since on that assumption they constrain conduct that is already absent. If the answers are unavailable, the amendments are the least expensive protection against a consequence no one intends.

V. THE PROPOSED AMENDMENTS

Addendum A sets out fourteen items. Nine are redlines against the July 24 draft, reproducing the baseline text verbatim; four propose new sections; and one supplies definitions keyed to alphabetical insertion points. Each states why the amendment is asked for, so this section states only what is needed to weigh them.

A. The duty: item 7

Item 7, new § 5A: preservation and repository of claim-evaluation records. This is the records-retention duty this letter asks for. It requires a licensee to preserve claim-evaluation records, to retain them in a repository retrievable by the identity of the claim-evaluation source, by each policy provision cited or applied, and by the individual who made or approved the claim decision, and to keep them for five years after claim closure, with ten years for the source's assignment list and compensation record, neither of which contains any consumer's identity.

Section 5A requires a repository, and not a larger claim file. That distinction matters for one category in particular. What a licensee pays a claim-evaluation source is ordinarily held in the accounting system, under the vendor, rather than in any claim file, and § 5A(A) is drafted accordingly: it requires that the records be retained and retrievable together, and leaves the licensee to decide where they physically reside. Nothing in it enlarges the claim file or requires an insurer to move accounting data into one.

Two further features answer the objections it will draw. The duty reaches the basis and manner of a licensee's claim decisions **whether or not a professional was retained**, for the reason at § II.B: at least five of the eleven purposes for which courts order this discovery involve no expert. And the indexing requirement, not the retention period, is what makes the records usable, because a practice becomes visible along those three axes and rarely on the face of one file. Section 5A is drafted to supply what Model #900 § 3's "general business practice" standard requires and what §§ IV.B and IV.C show the records models leave unpreserved. It reaches no record outside the defined category, and it excludes the litigation file and settlement communications.

Items 1, 2, 3, 5, 6, and 14 are conforming. Item 3 carries the definitions, of which *claim-evaluation record* is the substantive one: its subparagraph (D) covers every written communication to a consumer that states or explains a claim decision **or any reason given for it**, which is the category defined by the reason given that the retention models never named. Item 14 supplies the transition rule, without which a purely prospective reading would leave records already in existence outside the duty.

B. The amendments that limit what this Act permits

Seven items explained in Addendum A. In the order they arise in the Act: **item 4** requires that de-identification under § 4(J) preserve cross-claim linkage, which is the least visible route to destruction in the draft and the amendment most worth the Working Group's attention; **item 8** makes § 6(C)(2)(a) mandatory so that compliance with other retention law is a duty rather than an option, confirms that § 6(C)(2)(d) is not limited to a proceeding involving the requesting consumer, and adds a carve-out at (e) that protects the requesting consumer more thoroughly than the current draft does; **item 9** bars solicitation of deletion requests, and describes no conduct attributed to anyone; **item 10** extends § 24(A)(7) to party-served discovery, arbitration, and appraisal, none of which the operative text presently names; **item 11** carves § 5A out of the § 28 HIPAA deeming clause and leaves that clause otherwise intact; **item 12** preserves stronger state retention law, which Articles II and III presently lack any savings clause for; and **item 13** supplies a right of action confined to the record-retention obligations, a rebuttable presumption from non-preservation, and a provision that compliance with this Act is no defense to a preservation duty arising elsewhere.

C. Three conforming amendments to Models #902 and #910

This draft would authorize the destruction of records those regulations require a licensee to keep, and each was written without reference to the other. The three amendments

below would resolve that conflict from the other side. They are offered for whatever use the Working Group finds for them.

1. **Name the record.** Add to #910 § 6(A) a category for the reports, opinions, and evaluations of any retained professional or vendor relied upon or referenced in a claim decision, with the identity of the source and the compensation paid.
2. **Extend the duty past the individual claim.** Amend #902 § 4(B) and #910 § 4(A) so that a licensee's use of a given claim-evaluation source can be reconstructed **across claims**, indexed by source identity. **This asks for indexing and adds no retention period. It is the most consequential of the three.**
3. **State the beneficiary.** Amend the purpose clauses at #902 § 4 and #910 § 2 so the retention duty is not defined solely by examination convenience.

Redlined language will accompany the September 22 submission.

VI. CONCLUSION

The Working Group is respectfully requested to:

1. Adopt Addendum item 7, the preservation and indexing duty, together with its transition rule at item 14. This is the substantial request, and it is drafted to supply what Model #900's "general business practice" standard requires and what Models #902 and #910 leave unpreserved;
2. Adopt the remaining items at Addendum A, which limit what this Act permits or clarify what it already permits, and which are severable from item 7 and from each other;
3. Consider the three conforming amendments to Model Regulations #902 and #910 at § V.C; and
4. Provide the information requested at § IV.F, or state that the NAIC holds none responsive.

Should it assist the Working Group, I would be glad to walk through the redlined language and the questions at § IV.F by telephone during the week of August 10. Fourteen amendments do not fit in four minutes, and a call before the meeting may be a more efficient use of the Working Group's time. I am available on short notice at 805.298.1152 or cdion@exposingexpertbias.com.

Thank you for the Working Group's consideration.

Respectfully submitted,

/s/ Christopher L. Dion

Consulting Attorney

Addendum A, Proposed Amendments to Model #672, redlined from the July 24, 2026 Full Exposure Draft, is submitted concurrently with this letter.

ADDENDUM A

Proposed Amendments to Model #672

Redlined from the July 24, 2026 Full Exposure Draft

Submitted with the comment letter of Christopher L. Dion dated August 6, 2026

ARTICLE I. GENERAL PROVISIONS

Item 1. § 1 (Purpose):

Redline.

Purpose. This Act governs the treatment of nonpublic personal health information and nonpublic personal information about individuals by all licensees of the state insurance department. This Act:

A. Requires a licensee to provide notice to individuals about its privacy policies and practices;

B. Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal information about individuals to affiliates and nonaffiliated third parties; and

C. Provides methods for individuals to prevent a licensee from disclosing that information.

Why. Absent a purpose hook, § 5A is exposed to a "beyond the stated purpose of the Act" objection. The purpose is stated in two facets, source neutrality and the basis for and manner of claim evaluation, because a purpose clause limited to the first would narrow § 5A by implication. *Conforming to item 7.*

Item 2. § 2(A) (Scope): confirm the Act reaches these records after de-identification

Redline.

A. Scope. This Act applies to:

(1) Nonpublic personal information about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. This Act does not apply to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes; and

(2) All nonpublic personal health information

Why. Because § 4(Q) excludes de-identified data from "nonpublic personal information," a de-identified claim-evaluation record could be argued out of the Act's scope entirely, taking § 5A's duties with it. This places the records within the Act's coverage for the limited purpose of § 5A, without making them nonpublic personal information. *Conforming to item 7.*

Item 3. § 4 (Definitions): eight insertions

Drafting instruction to the Working Group. Insert each definition at its alphabetical position and re-letter subsequent subsections accordingly. Anchor points below are keyed to the July 24, 2026 lettering, which runs A through V and then X through AA: twenty-six definitions, **with no subsection W**. Two of these eight are fundamental definitions: ***claim-evaluation record*** and ***claim-evaluation source***. The remaining six are supporting definitions used within them.

Insert before § 4(A) ("Affiliate"):

Insert after § 4(B) ("Biometric data"), before § 4(C) ("Clear and conspicuous"), in this order:

Insert after § 4(G) ("Consumer"), before § 4(H) ("Consumer reporting agency"):

Insert after § 4(L) ("Financial product or service"), before § 4(M) ("Insurance product or service"):

Insert after § 4(N) ("Licensee"), before § 4(O) ("Nonaffiliated third party"):

Why. Eight insertions, two of which do the substantive work. *Claim-evaluation record* defines the category by function. Its subparagraph (D) supplies what Models #902 and #910 do not: it covers every written communication to a consumer that states or explains a claim decision **or any reason given for it**, whether or not any source is referenced. That category, defined by the reason given, is the one the retention models never named. *Claim-evaluation source* covers any person whose facts or opinions are relied upon in a claim decision, regardless of any exclusion that would otherwise apply under another definition in the Act. Subparagraphs (A)–(C) and (F)–(G) of the record definition are source-keyed by their nature; (D) and (E) are not. The litigation and settlement carve-out in *claim decision* is confirmatory, and is deliberately **not** phrased in terms of privilege or work product, for the reason given at item 7. The remaining six definitions support these two, and each is tied to an alphabetical insertion point in the July 24 lettering.

Item 4. § 4(J) ("De-identified data"): de-identification must preserve cross-claim linkage

Redline.

J. "De-identified data" means information that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual.

Why. Section 5(A)(2) authorizes de-identification as an alternative to deletion, and § 4(Q) places the result outside the Act. Nothing constrains *how* the removal is performed. A licensee that removes the consumer's identity without retaining a stable claim-level identifier, or that partitions the reports, the correspondence, and the consumer's objections into stores that cannot be joined, has complied with every word of § 4(J) and

destroyed the usefulness of the records, leaving no deletion to challenge and no missing document for anyone to notice. **This is the least visible route to destruction in the draft.** Two operations both remove the consumer's identity: one leaves the record analyzable across claims, the other does not. This amendment asks only that the permitted operation be the first. The operative text is at § 5A(D), which requires that de-identification preserve the cross-claim linkages, the integrity of each claim as a single reviewable transaction, and a persistent claim identifier. It is **privacy-enhancing on its face**: it removes the consumer's identity from the analytical record while leaving the accountability data intact. It seeks a better de-identification standard, not a weaker one, and § 4(Q) is deliberately left untouched, because that exclusion is what makes the compromise work in both directions.

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Item 5. Article II heading: conforming

Redline.

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Why. Proposed § 5A sits most naturally after § 5, because § 5 is the provision that mandates vendor-side destruction. The current Article heading does not accommodate a preservation duty. Retitling is the minimal-ripple fix. *Conforming to item 7*.

Item 6. § 5(A)(2): conforming carve-out from vendor-side destruction

Redline.

(2) Requires the third-party service provider to delete, destroy, de-identify or return all nonpublic personal information to the licensee when requested by the licensee; or to delete nonpublic personal information after it is no longer necessary to fulfill a legal requirement or to meet the record retention requirements of the licensee or third-party service provider and to notify the licensee of the action taken;

Why. The trigger for mandatory downstream destruction is "the record retention requirements of the licensee", which is a schedule this Act nowhere regulates. Because expert reports, referral instructions, compensation records, and often the claim

correspondence itself are held by vendors rather than by the licensee, this is the provision that reaches the records at issue.

Item 7. new § 5A: Preservation and Repository of Claim-Evaluation Records

Proposed text.

Drafting Note (proposed, to follow Section 5A).

This Section establishes an affirmative, continuing duty to preserve records bearing on the reliability and neutrality of the sources on whose facts and opinions claim decisions rest, and on the basis for and manner of the licensee's own evaluation and decision of claims. The second category is not conditioned on the involvement of any retained professional. The duty is independent of, and additional to, any preservation obligation arising from pending or anticipated litigation; it is not a litigation hold and does not depend on one. Subsection A requires that the records be retrievable by source identity, by policy provision applied, and by the individual who made or approved the decision, because each is an axis along which a practice becomes visible that no single claim file discloses. Subsection D permits removal of the consumer's identity from the retained record. That identity remains recoverable only by the licensee, only through the segregated association at Section 6(C)(2)(e), and only for notice and consent under judicial supervision; it is not recoverable by any other person from the retained records. Subsection E confirms that neither this Section nor any other provision of this Act creates a confidentiality, privilege, or privacy objection to production in an adjudicative process. The consequence of non-preservation is addressed at Section 34(C).

Why. This is the records-retention duty the accompanying letter asks for.

The gap it closes. No provision of this Act requires preservation of any record bearing on a source's reliability or neutrality, or on the basis for a claim decision; across thirty-five sections the sole affirmative record-maintenance obligation is § 6(D)(3)(b), covering the consumer's written statement of disagreement. Nor do the NAIC's records models supply it. Model #902 § 4(B) measures an insurer's documentation duty by whether "the insurer's activities" can be reconstructed, and its § 4(A) data set records that a claim was denied and when, with no field for why. California's 10 Cal. Code Regs. § 2695.3(a) uses the same measure: pertinent events, dates, and the licensee's actions. Model #910 § 6(A) does require "claim investigation documentation" and "correspondence used for determining and concluding claim payments or denials," and the NAIC's own state page, ST-910 (Fall 2022), records "NO CURRENT ACTIVITY" for thirty-nine of fifty-one jurisdictions, California, Texas, Florida, Illinois, Pennsylvania, Ohio, Georgia, New Jersey, and Michigan among

them. So in most states nothing located requires a licensee to keep the report on which a denial rests. Compensation sits further outside still: what a licensee pays a claim-evaluation source is ordinarily held in its accounting records, under the vendor, and not in any claim file, so no claim-file rule was ever going to reach it.

What it supports. Model #900 § 3 conditions liability on conduct "committed with such frequency to indicate a general business practice," which is a cross-claim standard. Section 5A is drafted to supply what that standard requires and to reach no record outside the defined category.

The duty rests on two facets, not one. It reaches source neutrality **and** the basis and manner of claim evaluation, because most of the purposes for which courts order this discovery do not involve a retained professional. Subsection (B) states the scope accordingly, and Subsection (D)(5) states the permitted uses; a use limitation confined to expert neutrality would preserve the records and forbid the analysis for which the rest of them are probative.

A repository, not a larger claim file. Subsection (A) requires that these records be retained together and retrievable together. It does not require that any of them be placed in a claim file, and it does not enlarge the claim file. This matters for the compensation record in particular, which ordinarily sits in the licensee's accounting system under the vendor. The Section leaves the licensee to decide where a record physically resides, and requires only that it survive and be retrievable.

Indexing is the working requirement. Subsection (A) requires retention in a repository retrievable by the identity of the claim-evaluation source, by each policy provision cited or applied, and by the individual who made or approved the claim decision. Each is a line along which a practice may become visible that a single claim file will rarely disclose: the reviewer who always finds the same way, the exclusion construed one way for one insured and the opposite way for the next, the adjuster whose files follow a common pattern. No existing NAIC model requires retrieval along any of them, and that absence is why a retention period by itself would accomplish little.

The remaining subsections. Subsection (C) sets retention at five years after claim closure for the claim-level records, and ten years for the source's assignment list and compensation record, neither of which contains any consumer's identity. Subsection (D) permits removal of consumer identity while preserving analytical linkage, and states permitted uses without limiting any person's use, production, or admissibility of the records. Subsection (E) confirms that nothing in this Act creates a confidentiality or privilege objection to production in an adjudicative process. Subsection (F) confirms that this Act does not displace preservation duties arising elsewhere.

What § 5A leaves out. The litigation file is excluded, as are settlement communications. That carve-out, drafted at item 3, avoids the language of privilege and work product deliberately, because a privilege recital in a preservation section would operate as a grant of protection in jurisdictions whose law presumes the claims file open in first-party bad faith.

Placement. Section 5A is proposed for Article II, immediately after § 5, because Article II contains the vendor-side destruction provision. Final placement and numbering are the Working Group's.

ARTICLE III. CONSUMER REQUESTS

Item 8. § 6(C)(2): mandatory compliance with other retention law, deletion carve-out, and consumer-protection production gate

Redline.

(2) The licensee is not required to delete nonpublic personal information if:

(a) The licensee is required by law or regulation to retain the nonpublic personal information;

(b) The nonpublic personal information may be necessary to perform the contract or service requested by or benefiting the consumer;

(c) The information is necessary to comply with a legal obligation; or

(d) The information is maintained in reasonable anticipation of a claim or civil or criminal proceeding

Drafting note. The amendment to subparagraph (a) is drafted as an insertion within the existing subparagraph so that the lettering of (b) through (e) is undisturbed and no cross-reference elsewhere in the Act requires conforming. The Working Group may prefer to lift the duty out into a separate paragraph; the substance is the same either way.

Why. Section 6(C)(2) opens "The licensee **is not required to delete** … if," and that opening governs all four conditions. Every one supplies an option. Subparagraph (a) applies wherever another law requires retention, which for a closed claim file in California is 10

Cal. Code Regs. § 2695.3(b)(3). So the Act addresses the conflict between its own deletion command and a state retention rule, and resolves it by telling the licensee that it may obey the state rule. **The amendment to subparagraph (a) changes that permission to a duty. It imposes no retention period and creates no new obligation. It requires compliance with retention obligations that already exist elsewhere.**

The remaining amendments address the closed claim file directly. Subparagraph (d) as it stands leaves the decision whether to preserve one insured's file for another insured's benefit with the party that benefits from destruction; the amendment to (d) confirms that it is not limited to a proceeding involving the requesting consumer, and new subparagraph (e) converts the permission into a rule for this category. It also protects the requesting consumer **more thoroughly than the current draft does**: the record is retained, the consumer's identity is de-identified out of it, and that identity is produced only on court order after notice and an opportunity to object. The retained association is what makes that notice possible. *The accompanying letter discusses this conflict at §§ III.B.2 and IV.C.*

Item 9. new § 6(D)(4): no solicitation of deletion requests

Proposed text.

Why. Section 31 bars penalizing a consumer for exercising these rights and is silent on *inducing* their exercise, and the Act contains no dark-patterns provision. Section 6(D)(2) affirmatively removes any cap on the number of requests. A licensee that placed a deletion control in a policyholder portal or claim-closing letter would reduce its own closed claim files one authenticated request at a time, while occupying the posture of a party complying with a mandatory statutory duty. **This item describes no conduct attributed to anyone and is offered as no accusation.** It protects the consumer's right from the one direction the draft leaves open.

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES

Item 10. § 24(A)(7): reach party-served discovery, arbitration, and appraisal

Redline.

(7) (a) To comply with federal, state or local laws, rules and other applicable legal requirements;

(b) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities; or

(c) To respond to judicial process or government regulatory authorities having jurisdiction over a licensee for examination, compliance or other purposes as authorized by law;

or

Why. Subparagraph (b) reaches subpoenas "by federal, state or local authorities"; (c) pairs "judicial process" with "government regulatory authorities" in a series whose other members are governmental. The strings "arbitrat-" and "apprais-" appear nowhere in the operative text of the July 24 draft. A licensee served with a party's document demand, an arbitrator's subpoena, or an appraisal demand has no clear permission under this Act to produce, and a colorable argument that it may not. Given how many insurance disputes resolve in appraisal and arbitration rather than in court, this gap is likely to be encountered often.

ARTICLE VII. RULES FOR HEALTH INFORMATION

Item 11. § 28: narrow carve-out from the HIPAA deeming clause

Redline.

A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

Why. Health claims are where independent medical examination, file review, peer review, and utilization review practices concentrate. Section 28 deems a HIPAA-governed licensee that "maintains nonpublic personal information in the same manner as protected health information" to be "deemed to comply with the requirements of this Act," so without a conforming change a health insurer could assert blanket deemed compliance and escape § 5A entirely. **The carve-out is narrowed to § 5A alone and leaves the deeming clause**

otherwise intact. Retaining these records is consistent with the uses § 25(B) already permits without authorization; combined with § 5A(D)'s removal of consumer identity, the health-privacy concern is addressed by the Act's own text.

ARTICLE VIII. ADDITIONAL PROVISIONS

Item 12. new § 30A: preserve stronger state retention and preservation law

Proposed text.

Why. Section 29 is limited to Article VII and directed at privacy subject matter; Articles II and III, which contain the destruction provisions, are covered by no savings clause at all. The clause above is confined to one direction: it preserves greater state *retention, preservation, and accessibility* law. A generic privacy floor would preserve stronger *deletion* law and, by negative implication, suggest stronger retention law is not preserved. **Section 29 is left untouched.** This item corresponds to Cal. Ins. Code § 791.39(d), which the accompanying letter discusses at § III.D. Note the limit of what any savings clause accomplishes: § 791.39(d) preserves "existing records retention periods" and other "legal requirements pertaining to records retention," so it preserves what exists and creates nothing. Where a state's existing claim-file rule fixes content by a chronology test, as California's 10 Cal. Code Regs. § 2695.3(a) does, this clause preserves a duration and not a requirement that the report behind a denial be kept. That is why item 7 is asked for alongside it. Placement and final numbering are the Working Group's.

Item 13. § 34 (Individual Remedies): a narrow private right, a presumption, and the completion of the Working Group's own clause

Redline.

Section 34. Individual Remedies

This Act may not be construed to create or imply a private cause of action for violation of its provisions, nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Why. The new non-curtailment clause is a real improvement and should be credited. But a savings clause preserves the *cause of action*; it does not preserve the *record*, and it does not stop this Act from supplying the defense. A licensee that deletes under § 6(C)(1) answers a spoliation claim by saying it destroyed nothing it was entitled to keep. Section 34 does not reach that answer, and its own words confine it to actions "which would otherwise exist **in the absence of this Act**," while the destruction is what the Act *supplies*. Subsection (E) closes that gap in one sentence, creating no remedy and imposing no duty. Subsections (A) through (D) are the more substantial request: a right of action confined to the record-retention, preservation, and anti-destruction obligations, with damages deliberately omitted, leaving injunctive relief, fees, and the rebuttable presumption at (C) that records not preserved would have been unfavorable.

Item 14. new § 35(D): transition and anti-destruction

Proposed text.

Why. Section 35 says nothing about records already in existence or claims already closed. A purely prospective reading would leave those records outside the duty, and § 35(A)'s compliance extension would operate as a period in which they could lawfully be destroyed before the duty attached. Paragraph (3) therefore attaches the duty not to destroy on the date of enactment, and confines the compliance extension to the building of the repository. *Conforming to item 7.*

End of Addendum A.

Christopher L. Dion
Consulting Attorney
expertbiasreport.substack.com
www.exposingexpertbias.com
805.298.1152

September 22, 2026

Re: Comment on the July 24, 2026 Full Exposure Draft of Model #672; Proposed Redline Amendments (Addendum A); the Regulatory Record of the 2004–2005 Unum Settlements **and What It Shows About This Draft (Addendum B); and the Draft's Interaction with Model Acts #670, #880, and #900 and Model Regulations #902 and #910**

Dear Ms. Neuerburg and Privacy Protections (H) Working Group Members:

I am a California-licensed attorney whose work for the past decade has focused on the insurance industry's use of financially dependent experts to pretextually deny and underpay claims, which is a form of institutional bad faith, and on the evidentiary record required to identify that practice when it occurs.

This letter is my submission for the written comment period closing September 22, 2026. It supplements my comment letter of August 6, 2026, which is incorporated by reference, and it delivers the analysis that letter reserved for this period: the 2004 multistate regulatory settlement concerning disability claim handling, and what that record shows about a model act that authorizes licensees to destroy closed claim files.

Two addenda accompany this letter. **Addendum A** restates the fourteen proposed amendments in redline form, keyed to the July 24, 2026 draft, each with its own explanation. They are unchanged in substance from August 6. **Addendum B**, *Designed to Deny: The Unum Scandal, Biased Medical Experts, and the Failure of the Regulatory Settlements*, is a study of the largest proceeding insurance regulators have brought against a disability insurer for its use of biased medical reviewers, of the remedy they wrote, and of what the courts have found in the twenty-one years since. Part II of this letter summarizes it. The rest of this letter carries forward the analysis of August 6, revised where the Unum record bears on it.

EXECUTIVE SUMMARY

The issue. This draft authorizes licensees to destroy closed claim files, and the vendor files behind them, on a schedule the licensee writes and no one reviews. The August 6 letter showed that, in most states, no located retention law requires the reports and compensation records at issue to be kept, whatever the period." This letter adds the second half of the picture. The records this draft permits a licensee to destroy are the only records from which the neutrality of a claim-evaluation expert has ever been tested in this industry. The regulators who examined that practice, in the largest proceeding ever brought against a disability insurer, did not test it. The courts did, and every

fact they used came from records beyond the claimant's own file: other insureds' claim files and the compensation records behind them.

The Unum record, in brief. In November 2004 the chief insurance regulators of forty-eight states and the District of Columbia, joined by the United States Department of Labor, settled a targeted multistate market conduct examination of the UnumProvident companies, then the largest disability insurer in the country. California proceeded separately, by Accusation, and settled in October 2005. The examiners inferred that the companies' excessive reliance on in-house medical professionals "often resulted in a Company bias," and California found the companies "selectively using independent medical examinations (IMEs) to Respondents' own advantage." The remedy prohibited selecting examiners by reference to prior results and required selection on "objective, professional criteria." It then required no record of what any examiner was paid, how often any examiner was used, how any examiner's opinions came out, or on what basis any examiner was chosen, and it measured compliance by a file-level error rate. An insurer that sent every examination to a physician who had never found a claimant disabled would have passed that test with a documented rationale and an error rate of zero.

Every fact now in the public domain about any Unum examiner's compensation, volume, or outcome history came instead from a claimant who sued, obtained records beyond the claimant's own file over the insurer's objection, and left a written record a later claimant could use. In 2013 a court compelled Unum to disclose that one reviewer had averaged some 250 Unum claims a year at an average of $237,500 a year; Unum obtained an order restricting access to that order two days later, then settled. In 2016 Unum asked the Department of Labor to delete the one federal provision directed at how reviewers are selected, because it "potentially invites broad discovery."

Sections 5(A)(2) and 6(C) of this draft permit a licensee to destroy those records on its own schedule, and § 5(A)(2) reaches the vendor layer where much of the engagement record is held. Public enforcement will not replace them: the multistate examination and the California proceeding were the strongest instance of public enforcement the industry has produced, and they wrote a remedy incapable of detecting whether the practice stopped. The industry's objection to the federal rule went to the inquiry, not to whether the evidence could be counted. An argument about what a number means is a reason to preserve the material and let the parties contest it.

The three findings of August 6 stand. First, the retention rule the states adopted, Model #902 § 4(B), measures an insurer's duty by whether its *activities* can be reconstructed, and its data set records that a claim was denied and when, with no field for why. Model #910 § 6(A) is better, and the NAIC's own state page records "NO CURRENT ACTIVITY" for thirty-nine of fifty-one jurisdictions. Second, this draft sets the destruction schedule by the licensee's own hand: § 5(A)(2) compels vendors to destroy records "to meet the record retention requirements of the licensee," and nothing requires that schedule to be filed, approved, or disclosed. Third, the draft supplies no link to the retention law of any state: across thirty-five sections it imposes one record-maintenance obligation, at § 6(D)(3)(b), and its one provision addressed to other retention law, § 6(C)(2)(a), grants a permission.

What is asked. Two things. That this Act stop authorizing the destruction of claim-evaluation records, and that it impose a narrow duty to preserve and index them. The second is a records-retention duty consistent with the NAIC's own models. It is drafted to supply what Model #900's "general business practice" standard requires and what Models #902 and #910 leave unpreserved. Fourteen items inside Model #672, set out and explained in Addendum A, and four conforming amendments to Model Regulations #902 and #910 at § VI.C. Section 5A, at Addendum item 7, would require the two records the Unum settlements omitted: the compensation and engagement record for each claim-evaluation source, and the expert reports themselves, retained in a repository retrievable by the identity of the source.

The records at issue are narrower than claim files generally and exclude the litigation file. Two related categories, gathered in Addendum A as the *claim-evaluation record*: the accountability record behind a retained professional (identity, assignment history, outcome distribution, compensation), and the licensee's own account of why it decided the claim as it did, whether or not any professional was retained. The consumer's identity is absent from the retained records. A retained physician, engineer, or file reviewer is a commercial counterparty of the licensee rather than a consumer, and that person's identity, assignment history, and compensation are outside "nonpublic personal information" under §§ 4(Q) and 4(R)(1). Preserving the accountability record costs this Act's privacy purpose nothing.

I. WHAT IS REQUESTED

This letter asks the Working Group to do two things, and the second is the substantial one:

First, that this Act stop authorizing the destruction of claim-evaluation records. Second, that it impose a duty to preserve and index them, defined narrowly, so that the enforcement models the NAIC has already written can operate as they were designed to.

The second request is a records-retention duty. Proposed § 5A (Addendum item 7) requires a licensee to preserve claim-evaluation records, to index them by source, by policy provision applied, and by decision-maker, and to retain them for stated periods: five years after claim closure for the claim-level records, and ten years for the source's assignment list and compensation record, neither of which contains any consumer's identity. Addendum item 14 supplies its transition rule, and item 8 requires compliance with the retention duties other law already imposes.

The duty is drafted to supply what Model #900 § 3 already requires and what Models #902 and #910 leave unpreserved. Section 3 conditions liability on conduct "committed with such frequency to indicate a general business practice," which is a cross-claim standard; §§ V.A through V.C set out what the records models do and do not keep. Section 5A is drafted to close that gap and to do nothing else.

The category is narrowly defined. Section 5A reaches claim-evaluation records as Addendum item 3 defines them. It excludes the litigation file and settlement communications. It does not reach claim files at large, and it imposes no general retention obligation on any other record a licensee holds.

The set is severable. Fourteen items amend Model #672. Item 7 is the substantial request and is identified as such wherever it appears. Four further amendments, at § VI.C, address Model Regulations #902 and #910, because the destruction this draft authorizes and the retention those regulations require form one question. Where within the NAIC each amendment is taken up is a matter for the NAIC.

Section 33 of the draft is a broad severability clause, and every request in Addendum A stands independently of every other. The Working Group may adopt one, several, or all fourteen.

II. THE UNUM RECORD, AND WHAT IT SHOWS ABOUT THIS DRAFT

The August 6 letter argued from the text of the models that the records this draft would permit a licensee to destroy are the records the NAIC's enforcement models require. This Part argues from the record of the largest proceeding in which regulators examined the practice those records reveal. Addendum B sets out that record in full, with citations. What follows is limited to what bears on the July 24 draft, with references to the Parts of Addendum B where each point is developed.

A. What the regulators found, and what the remedy required

In November 2004 the UnumProvident companies, their domestic regulators, and the United States Department of Labor entered into a Regulatory Settlement Agreement subscribed to by forty-eight states and the District of Columbia. California did not join. It issued an Accusation, the companies waived hearing, and in October 2005 the Commissioner entered a Decision and Order finding that the companies had "in certain instances" engaged in twenty-eight enumerated acts or practices in violation of Insurance Code §§ 700 and 704. (Addendum B, Parts III.A and III.C.)

Both proceedings identified the use of medical opinion. The multistate examiners inferred that the companies' "excessive reliance upon in-house medical professionals also suggests the Companies' employment of such professionals often resulted in a Company bias and the inappropriate interpretation or construction of medical reports, to the detriment of claimants." California found the companies "[s]electively using independent medical examinations (IMEs) to Respondents' own advantage"; overruling in-house personnel "who supported a finding of disability or the need for specific objective testing"; and making substantive claim decisions in roundtable sessions the files did not document. Neither examination examined the examiners. The multistate samples were drawn by company, line of business, claim category, and state of residence, and none was drawn by reviewer or examiner. No finding addresses what any examiner was paid, how many engagements any examiner received, how any examiner's opinions came out across engagements, or how the companies selected examiners. (Addendum B, Parts III.A and III.B.)

The remedy prohibited the practice without requiring a record by which the prohibition could be tested. The Regulatory Settlement Agreement requires the companies to select examiners "solely on the basis of objective, professional criteria" and "without regard to results of previous IMEs or FCEs conducted by such individuals." Neither settlement requires the companies to record what an examiner was paid, how often the examiner was used, or how the examiner's opinions came out, and neither states the "objective, professional criteria" or requires that they be written down.

Compliance was measured by an error rate of no more than seven percent in random samples of claim files. The 2008 re-examination reported error rates of 4, 4, 0, and 3 percent and said nothing about how examiners were selected. Under that test, an insurer that sent every examination to a physician who had never found a claimant disabled would show a credentialed examination, a documented rationale, and an error rate of zero. (Addendum B, Parts IV.A, IV.E, and IV.F.)

The form such a record could take was already in California law. A neutral arbitrator must disclose any current arrangement or recent discussion concerning compensated service for a party, and must disclose the names of the parties and the results of every prior case in which the arbitrator served for any party or party's lawyer within the preceding five years. Cal. Code Civ. Proc. § 1281.9. The California Settlement Agreement applied that model to the one neutral the Department appointed itself. Candidates for Independent Review Director were required to "disclose any financial interests or business relationships likely to affect impartiality or that might create an appearance of partiality," and either party could seek removal of a reviewer who "has engaged in a pattern or practice" of unfair review. The examiners the companies hired were subject to no comparable requirement. (Addendum B, Part IV.G.)

Three requirements would have closed the gap: a per-claim disclosure by the examiner, in the file, of engagements accepted, compensation received, and the disposition of prior engagements; retention by the insurer of the compensation and engagement record for each examiner and vendor; and retention of the expert reports themselves, indexed by examiner. The companies already bore the obligation to keep the files, and adding the examiner to the index would have cost them a field. Proposed § 5A supplies the second and third. Section VI.C below proposes the first as a conforming amendment to Model #910.

B. Where the facts about examiners came from

What is publicly known about any examiner's compensation, volume, or outcome history has come from litigation, and from records beyond the claimant's own file. In *Hangarter v. Provident Life & Accident Insurance Co.*, 373 F.3d 998 (9th Cir. 2004), decided five months before the multistate settlement, cross-claim discovery established that Paul Revere had used Dr. Aubrey Swartz nineteen times between 1995 and 2000, and that "in thirteen out of thirteen cases involving claims for total disability, Dr. Swartz rejected the insured's claim that he or she was totally disabled." Provident's former vice-president and medical director testified to "searching for the 'right physician to do the IME because we want to get the answer we want.'" In *Waggener v. Unum Life Insurance Co. of America*, 238 F. Supp. 2d 1179 (S.D. Cal. 2002), the court ordered Unum to answer, for each independent contractor who evaluated the claim, "the number of times [Unum has] employed that person to participate in evaluating or handling a claim . . . [and] the total amount of compensation paid on each occasion." The 2004 multistate examination report cites neither decision. (Addendum B, Part II.)

After the settlements, the same questions were answered the same way. In *Kelly v. Provident Life & Accident Insurance Co.*, No. 1:09-CV-70, 2010 WL 3259997 (D. Vt. Aug. 17, 2010), the employee responsible for "locating and hiring IMEs" testified that Unum had "no formal rating or evaluation system" for the examiners it hired, and that the only recorded evaluation of the two examiners at

issue was a note in a provider directory recording "a very good turnaround time and extensive report." A company that records nothing about its reviewers' conclusions cannot be shown to have selected on them, and it cannot show that it did not. The administrator in *Demer v. IBM Corp. LTD Plan*, 835 F.3d 893, 903 (9th Cir. 2016), "could have maintained records of its reviewers' findings on claims to show their neutrality in practice, but it did not," and so "missed an opportunity to negate any inference of a financial conflict of interest." In *Boles v. Unum Life Insurance Co. of America*, No. 4:11-cv-03031 (D. Neb. Jan. 22, 2013), the court compelled Unum to answer interrogatories on its conflict of interest and recited the answers: the reviewing physician had averaged some 250 Unum claims a year and an average of $237,500 a year for work on Unum files. Two days later, on Unum's emergency motion, the court restricted access to the order. The case settled one hundred and eight days after the order, and the order remains restricted. The figures are public only because a claimants' bar association quoted them to the Department of Labor in a rulemaking three years later. (Addendum B, Parts IV.C, IV.G, V.A, and VI.H.)

The route runs in one direction. A claimant seeking discovery outside the administrative record must first show that the conflict infected the decision. The structural conflict alone does not suffice, *Stallman v. First Unum Life Insurance Co.*, Civ. No. 23-20975, 2024 WL 4988603 (D.N.J. Dec. 5, 2024), and neither does disagreement with the reviewer on the merits, *Jacob v. Unum Life Insurance Co. of America*, No. 1:19-cv-131, 2019 WL 13298916 (E.D. Tenn. Dec. 17, 2019). The showing requires an extrinsic fact about the reviewer: a compensation figure, an engagement count, a distribution of prior conclusions. The predicate a claimant must supply in order to obtain conflict discovery is the evidence that conflict discovery would produce, and restricting the *Boles* order removed that predicate for every claimant who came after. The settlements have not filled the gap. In *Braun v. Unum Life Insurance Co. of America*, No. 22 C 1223, 2023 WL 4205536 (N.D. Ill. June 27, 2023), the court found that Unum's structural conflict did not influence its decision because Unum "has been acting pursuant to the [Regulatory Settlement Agreement] for almost twenty years." In *Stallman*, the court was "not convinced that First Unum's entry into the [Regulatory Settlement Agreement] some twenty years ago creates a reasonable suspicion" that the decision was affected by a conflict. (Addendum B, Parts V.A, VI.A, and VI.G.)

Where the reports have been produced, they have established the pattern on their own. In *Chacko v. AT&T Umbrella Benefit Plan No. 3*, 690 F. Supp. 3d 1123 (E.D. Cal. 2023), a case involving a different disability plan and a reviewer engaged through a vendor, the plan produced the conclusion pages of eighty-eight reviews in lieu of answering interrogatories; counsel tabulated them; and the court, comparing the tabulation against the pages, found that "plaintiff's representations are accurate and supported by the conclusion pages themselves," with fifty of sixty-one claimants found not disabled. Such material rarely travels further. Of the twelve actions in which bias discovery was ordered against Unum or its affiliates and whose dockets are available, eight settled or were dismissed by stipulation, four of them within four months of the order. Where the material is produced, it is covered by a protective order, and when the case ends it goes no further. (Addendum B, Parts VI.H and VII.F.)

Under this draft, the claim files and reports from which those facts were drawn could lawfully have been destroyed before the litigant who needed them filed suit, and the litigant would have had no way to know. Section 6(C)(1) requires deletion within forty-five days of a consumer's request, with

no limit to open or recent claims and no cap on the number of requests, and § 5(A)(2) compels vendors to delete on the licensee's own schedule. Closed claim files, and the records behind them, therefore serve a function that the interests of the claimant whose file it is do not exhaust.

C. The industry's own statement that the evidence matters

In 2016 the Department of Labor amended the ERISA claims regulation. New paragraph (b)(7) of 29 C.F.R. § 2560.503-1 requires that decisions regarding "hiring, compensation, termination, promotion, or other similar matters" with respect to a medical or vocational expert "not be made based upon the likelihood that the individual will support the denial of benefits." The preamble states that a plan cannot contract with a medical expert based on the expert's "reputation for outcomes in contested cases," and extends the duty to experts engaged through third parties, which the plan must address "in the terms of its service contract and ongoing monitoring." 81 Fed. Reg. 92,316, 92,319–20 (Dec. 19, 2016). (Addendum B, Parts I.E and VII.F.)

On January 19, 2016, Unum Group asked the Department to delete both halves of the rule. It gave these reasons:

> "The concern with the proposal as currently drafted is that it potentially invites broad discovery and will increase litigation expense substantially. . . . With respect to medical experts, the preamble refers to an expert's 'reputation for outcomes in disputed cases.' In practice and in theory, there is no way to measure 'reputation' in this context. Again, this invites litigation."

The harm Unum identified was the inquiry. When Unum said reputation could not be measured, the measurement had already been made, in *Boles*, from Unum's own interrogatory answers, and every neutral arbitrator in California was measuring and disclosing case outcomes under Cal. Code Civ. Proc. § 1281.9. Unum's trade association, in the same rulemaking, asked the Department not to disqualify an adjudicator "based solely on a 'reputational standard' such as the volume of claim denials," because a high volume "may" have innocent explanations. The explanation presupposes a number that can be counted. The Department kept the rule, reaffirmed the preamble statement as "one way that the independence and impartiality standard could be violated," and added that the rule does not "prescribe limits on the extent to which information about consulting experts would be discoverable in a court proceeding as part of an evaluation of the extent to which the claims administrator or insurer was acting under a conflict of interest." No reported decision applying § 2560.503-1(b)(7) to a challenge to the selection of a reviewer has been located. A rule that requires no record produces no evidence for a court to apply it to. (Addendum B, Parts I.E and VII.F.) The same is true of the settlement's selection rule at § B.3.d, which no decision examined for Addendum B has enforced.

III. THE RECORDS AT ISSUE, AND THE USES THEY SERVE

A. Why the opinion alone will rarely answer the question

Claim decisions in contested matters frequently rest on the opinion of a retained professional: a medical reviewer's finding that a claimant is not disabled, an industrial hygienist's conclusion about contamination, a forensic engineer's causation opinion. These opinions are generally

experientially based, which is to say professional judgments drawing on training and experience rather than on a method whose error rate or external benchmark can be examined on the face of the opinion.

What arrives in the claim file is a conclusion. A single file will sometimes disclose bias directly, through an internal communication or an abandoned first opinion, and where it does the cross-claim record is unnecessary. More often the principal available measure is the reviewer's record across many claims of the same kind: whether comparable inputs produce systematically one-sided outputs, whether stated criteria are applied consistently, and whether the licensee selects the reviewer because the record makes the outcome predictable. Those indicators are held in records other than the claimant's own file.

The Unum record illustrates the point in a form courts have accepted. In *Dwyer v. Unum Life Insurance Co. of America*, 548 F. Supp. 3d 468 (E.D. Pa. 2021), a reviewer's written opinion treated the claimant's "infrequent fills of small amounts of antiemetic medication" as inconsistent with the claimed symptoms. Under deposition, the reviewer testified to having treated about five patients with the condition, the last one likely in 2006, and to having nothing to recommend beyond what the claimant's specialist had recommended. The court found the claimant disabled. Nothing in the file showed the premise on which the opinion rested, and nothing in either Unum settlement required anyone to record it. (Addendum B, Part V.E.)

B. Eleven purposes for which courts already order this discovery

The Working Group is not being asked to recognize a new use for these records. A review of the reported decisions in which discovery of other insureds' claim files was sought or ordered yields at least eleven distinct evidentiary purposes. The list is **not exclusive**.

(A) **Biased subjective or experiential opinions**: to show biased opinions and lack of credibility supporting a breach-of-contract claim.

(B) **Erroneous or inconsistent opinions**: to show the reviewer's erroneous or inconsistent interpretation or application of principles, methodologies, and facts.

(C) **Interpretation or application of policy terms**: to show the insurer's erroneous or inconsistent interpretation of policy terms across insureds.

(D) **Biased claim investigations**: to show selection or compensation bias supporting a bad-faith claim.

(E) **Bad-faith claims adjusting**: to show specific bad-faith patterns and practices.

(F) **Genuine-dispute doctrine**: to oppose the insurer's genuine-dispute defense by showing the investigation was biased and unfair.

(G) **Insurer's intent**: to show conscious disregard supporting a bad-faith claim.

(H) **Excusable error**: to oppose the insurer's mistake, inadvertence, or negligence defense.

(I) **Punitive damages**: to show conscious disregard and recidivist conduct.

(J) **Unfair practices laws**: to show a violation of a state unfair claims settlement practices act, unfair trade practices act, or unfair competition law.

(K) **Class certification**: to identify other insureds whose claims share common policy provisions or claim-handling practices.

Two observations follow. *First, a substantial share of these purposes concern the licensee's own personnel rather than any expert.* Purposes (C), (E), (H), (J), and (K) involve no retained professional, and purpose (G) usually involves none. They concern which provision the adjusters applied, what they relied upon, and whether they construed the same language the same way for the next insured. **This is why the preservation duty at Addendum item 7 applies whether or not an expert was retained.** A duty drawn narrowly around expert bias would preserve the record in the claims where a second independent record already exists, and destroy it where the licensee's own correspondence is the only record there is. The Unum record supports the same conclusion from the other direction. California found that the companies made substantive claim decisions in roundtable sessions the files did not document, and the *Hangarter* record showed a directive that company doctors not record disability opinions in the file. Where the decisive reasoning is kept out of the file, the licensee's own correspondence across claims is what remains.

Second, the same condition defeats all eleven. Courts have resolved privacy objections for four decades by the mechanisms described at § III.D, so privacy leaves each purpose intact. The absence of the records defeats every one, and deletion is unappealable, unreviewable, and invisible.

Addendum B serves as the case catalog for the disability line. Its Parts V and VI collect the post-settlement decisions and discovery orders involving Unum and its affiliates, with citations. The cross-line catalog from which the eleven purposes are drawn will be provided on request.

C. Illustrations

Part II describes how the records of other claims established in *Hangarter*, *Boles*, and *Chacko* what no single file could. The same point appears from the other side in *Bagramyan v. Government Employees Insurance Co.*, No. B315018, 2023 WL 4636118 (Cal. Ct. App. July 20, 2023) (unpublished), where the court applied an inference-of-bias standard to an insurer's retained expert and found the showing wanting because the plaintiff "presented no evidence reflecting the number of times [the expert] has given opinions favorable to GEICO in similar cases, nor did he present evidence that GEICO had somehow primed [the expert] to produce a favorable report." Evidence of both kinds resides in the claim files of other insureds.

Where the records exist, the practice is provable. Where they are gone, the claim fails for want of the evidence that would identify the practice, whether or not the practice occurred.

D. Courts have already reconciled privacy with access

Courts have reconciled the preservation of these records with consumer privacy for four decades, through protective orders, temporal and geographic narrowing, redaction, and opt-in consent procedures for sensitive health information. **A protective order preserves both the privacy interest and the evidence. Deletion eliminates the evidence, and with it the setting in which the privacy question arose.**

One of the earliest of the Unum-related orders shows the method. In *Small v. Provident Life & Accident Insurance Co.*, No. 2:98-cv-02934, 1999 WL 1128945 (E.D. Pa. Dec. 8, 1999), the insured subpoenaed the examining physician's records of forensic examinations. The court held that "the existence of a pro-insurance bias on the part of Dr. Bromberg is germane" to the bad faith claim, found that reports prepared to determine eligibility for insurance benefits carry "a somewhat reduced expectation of privacy," limited the subpoena to examinations performed for insurers since 1990, and ordered the medical records redacted so that they "contain only the name of the insurance company for whom the record was prepared, Dr. Bromberg's analysis, and the recommendation made." Redaction has been the answer for twenty-seven years. It preserves the evidence while removing the privacy interest. (Addendum B, Part IV.C.)

Addendum A item 4 is built on this point. It asks that de-identification be permitted to remove the consumer's identity from the analytical record while preserving the linkages among source, methodology, outcome, and compensation, and among the policy provision applied, the reason given, the decision-maker, and the disposition. It asks for a better de-identification standard, not a weaker one.

The consumer's identity is absent from the retained records and cannot be recovered from them by any third party. It remains recoverable by the licensee, through a segregated and access-controlled association required at Addendum item 8, and only to give a consumer notice and an opportunity to consent or object before their identity is produced. This is pseudonymization of the analytical record rather than irreversible anonymization, deliberately so: a regime that destroyed the association would destroy the mechanism courts have used to reconcile these interests, because an opt-in letter presupposes that someone can address it. *Van Duyn v. American Security Insurance Co.*, No. CV 08-5748-GW(CTx), 2009 WL 10672575 (C.D. Cal. Apr. 14, 2009), is representative. The court weighed the Gramm-Leach-Bliley Act and the California Financial Information Privacy Act against the discovery need under Rule 26, and ordered an opt-in letter offering non-party insureds a choice between release of the claim file without restriction and release with the insured's "name, address, telephone numbers, and all other identifying information deleted from it." *Id.* at 4. Insureds electing the second level "may respond by including only their claim number in lieu of a signature, name, and address." *Ibid.*

One further point. A retained physician, engineer, or file reviewer is a commercial counterparty of the licensee rather than a consumer, and that person's identity, assignment history, and compensation are accordingly outside "nonpublic personal information" under §§ 4(Q) and 4(R)(1) and outside the Act's scope under § 2(A)(1). Preserving the accountability record costs this Act's privacy purpose nothing. What a claimant sought in every order described in Part II was the reviewer's analysis, the reviewer's conclusion, and the company's record of engaging and paying the reviewer. No order described there granted the other insured's identity or medical history.

IV. THE JULY 24, 2026 DRAFT

A. The Act's single record-maintenance obligation

Across thirty-five sections, the one affirmative record-maintenance obligation is § 6(D)(3)(b), which requires a licensee to maintain the consumer's written statement of disagreement with a refusal to correct or delete.

B. The provisions that authorize destruction

1. Deletion on request, reaching closed files. Section 6(C)(1) requires that "[w]ithin 45 days of an authenticated request from a consumer, a licensee shall delete the nonpublic personal information about the consumer." Section 6(D)(2) provides that "[t]here shall be no cap on the number of requests." Nothing limits the right to open or recent claims.

2. Every exception is permissive, including the one addressed to other law. Section 6(C)(2) provides that "[t]he licensee **is not required to delete** … if" one of four conditions obtains. The form of that sentence governs all four.

Subparagraph (a) applies wherever another law requires retention. In California a closed claim file is such a record, because 10 Cal. Code Regs. § 2695.3(b)(3) requires claim files to be kept "for the current year and the preceding four years." So this Act addresses the conflict between its own deletion command and a state retention rule, and resolves it by telling the licensee that it *may* obey the state rule. A licensee that deletes instead has complied with the mandatory sentence at § 6(C)(1) and passed up an option. **Addendum A item 8 makes subparagraph (a) mandatory. That is one sentence, and it creates no retention duty; it requires compliance with duties that already exist elsewhere.**

Subparagraph (d) applies where information "is maintained in reasonable anticipation of a claim or civil or criminal proceeding." Whether one insured's file survives for the benefit of a different insured's proceeding rests with the party who would be the defendant in it. Subparagraph (d) is also not by its terms limited to a proceeding involving the requesting consumer, which is correct as drafted and which Addendum item 8 asks the Working Group to confirm, because the narrowing reading will be argued.

3. Vendor-side destruction on a schedule this Act leaves unregulated. Section 5(A)(2) requires the licensee's contract to compel a third-party service provider "to delete nonpublic personal information after it is no longer necessary to fulfill a legal requirement or **to meet the record retention requirements of the licensee**." The licensee sets that schedule, this Act leaves it unregulated, and the model then compels the vendors to run on it. Because expert reports, referral instructions, and compensation records are frequently held by vendors, this is the provision that reaches the records this letter concerns.

The Unum record shows how much already sits in that layer. The referral in *Hangarter* was contended to have come through Genex, a UnumProvident subsidiary, and by 2010 Unum's Independent Assessment Network was responsible for "locating and hiring IMEs." The physicians in *De Mello v. First Unum Life Insurance Co.*, No. 25-cv-7933, 2026 WL 2032059 (S.D.N.Y. July 14,

2026), and *Leung v. Unum Life Insurance Co. of America*, No. 22-cv-00767, 2023 WL 4056041 (S.D. Cal. June 15, 2023), were engaged through Dane Street. In *De Mello*, Unum represented that the amounts it paid Dane Street were "meaningless in isolation" and that it did not have the amounts Dane Street paid the reviewing physicians. In *Leung*, the court accepted a declaration stating the total Unum paid Dane Street and required no further production. The 2016 federal rule requires a plan to address its vendor's selection practices "in the terms of its service contract and ongoing monitoring." Section 5(A)(2) instructs the opposite: it requires the licensee's contract to compel the vendor to delete the reports and engagement records that carry consumer information, and nothing in this draft requires the vendor to keep the compensation record that remains. (Addendum B, Parts II, V.B, and VI.C.)

The schedule is filed with no one and approved by no one. "Approval" appears once in this draft, at § 25(C), where additional insurance functions "may be added with the approval of the commissioner." Nothing requires a licensee to file its retention schedule or obtain approval of it. Section 9, listing what a Notice of Information Practices must contain, enumerates eight items, and retention is absent. Section 9(D)(1) provides that "[l]icensees are not required to use any prescribed clauses or model form." And § 13 requires a revised notice only before disclosure of a new category of information to a nonaffiliated third party, so shortening a schedule triggers nothing. The nearest thing to review anywhere in the NAIC's records models is Model #910 § 9(B), which requires computer-based records to be maintained under "written procedures developed and adhered to by the insurer," available "to the commissioner during an examination." That is availability after the fact.

4. De-identification as an unregulated alternative. Section 5(A)(2) authorizes "de-identify" as an alternative to deletion. Section 4(J) defines de-identified data, and § 4(Q) excludes it from "nonpublic personal information" and therefore from the Act. Nothing constrains *how* de-identification is performed. A licensee that strips source identifiers, or partitions records so that outcome no longer joins to source, destroys the analytical value of the category without performing a "deletion." No deletion has occurred for anyone to challenge.

C. The current draft authorizes what the earlier drafts commanded

The Working Group has dropped the standalone data-minimization article that appeared in earlier drafts. That is an improvement. The change is from a command to a permission, and in this setting the two tend to produce the same records at the end: the decision belongs to a party whose interest runs one way, no minimum retention period constrains it, and the choice carries no consequence. Under this draft no one orders the file destroyed, and nothing requires that it be kept.

The Unum record supplies the reason to expect the permission to be used. Unum has opposed bias discovery in every decade covered by Addendum B. It had the *Boles* order restricted. It asked the Department of Labor to delete the federal selection rule because the rule invites discovery. Most of the actions in which discovery was ordered ended before the material was weighed, and where the material was produced, a protective order kept it from going further. A party that has

opposed the production of these records for three decades will not need to be commanded to destroy them once destruction is lawful.

D. California and this draft, compared

A legislature has examined provisions of this kind twice, and the two instruments diverge in opposite directions on the two questions that decide whether records survive.

The destruction command. California kept it; this draft dropped it. SB 354's findings state data minimization as a governing purpose, § 791.13(i)(1) requires that retention "be reasonably necessary and proportionate," and § 791.13(i)(3)(C) provides that once information "is no longer needed," a licensee "shall take reasonable steps to securely destroy, delete, or deidentify" it. This draft carries no counterpart.

The connection to existing retention law. California supplied it; this draft did not. The May 23, 2025 version of SB 354 made no reference to existing records-retention law, preempted inconsistent state law, and exempted its implementing regulations from the Administrative Procedure Act. The August 21, 2026 version differs in four respects:

(1) The Administrative Procedure Act exemption is **gone**.

(2) Section 791.39(d): *"This article shall not be construed to reduce or eliminate any existing records retention periods or supersede any legal requirements pertaining to records retention."*

(3) Section 791.39(e): *"This article shall not be construed to abridge or limit the rights of litigants, including parties to administrative proceedings, under the laws, or case law, of discovery of this state."*

(4) Section 791.13(i)(2) requires a licensee to "develop a written records retention policy and records retention schedule and shall make it available to the commissioner upon request," reviewed at least every three years.

The July 24 draft contains no counterpart to any of the four.

A savings clause is only as strong as the duty it saves. Section 791.39(d) preserves what exists and creates nothing. In California what exists is § 2695.3: a five-year period attached to a duty whose content is fixed by the chronology test at § 2695.3(a), and which enumerates no documents. See § V.C. **So in California that clause preserves a duration. It does not preserve a requirement that the report behind a denial or the claim investigation documentation be kept, because no located California claims regulation imposes one.**

Neither instrument produces the records. The lesson is therefore narrower than adopting California's language, and this letter does not propose that: **a legislature that examined provisions of this kind closely concluded that an article of this kind requires an express records-retention savings clause, an express discovery savings clause, and a written schedule the regulator can ask to see.** Addendum item 12 supplies the records-retention savings clause and item 13 the discovery protection, and item 8 requires compliance with the retention law those

clauses would preserve. Items 3 and 7 do what no savings clause can, by defining the category the retention law never defined.

As of the date of this letter, SB 354 awaits the Governor's action.

E. Three provisions that will supply the answering argument

Section 6(D)(1)(b)(i) excuses compliance where information "is not locatable or retrievable by the licensee," and its Drafting Note directs examiners to review a licensee's irretrievability justifications. There is no counterpart Drafting Note for deletion decisions. The review attaches to the licensee's claim that it *cannot* produce, and not to its decision that it *need not* preserve.

Section 28 deems a HIPAA-governed licensee that "maintains nonpublic personal information in the same manner as protected health information" to be "deemed to comply with the requirements of this Act." Health and disability claims are where independent medical examination, file review, and peer review practices concentrate, and every decision described in Part II arose in that setting. Without a conforming change, a health or disability insurer could assert blanket deemed compliance.

Section 29 provides that "[n]othing in this Article shall preempt or supersede existing state law related to medical records, consumer data privacy, health or insurance information privacy." It is limited to Article VII, while the provisions authorizing destruction sit in Articles II and III. The Working Group recently revised this clause to add "consumer data privacy," having therefore revisited what belongs in it, and records retention is still not among the subjects.

V. THE OTHER MODELS, AND WHAT THEY REQUIRE TO BE KEPT

A. The enforcement models require cross-claim proof: Models #900 and #880

Model #900 § 3 provides that it is an improper claims practice to commit an act defined in § 4 if "[i]t is committed **flagrantly and in conscious disregard** of this Act" or "[i]t has been committed with such **frequency to indicate a general business practice**." Liability requires either flagrancy or frequency.

Section 4(C) ("Failing to adopt and implement reasonable standards for the prompt investigation and settlement of claims") and § 4(F) ("Refusing to pay claims without conducting a reasonable investigation") are the provisions a systematically biased expert practice violates. They are also the provisions a single file will rarely establish, because on the face of any one file the licensee did investigate: it retained a credentialed professional and relied on the report. Model #880 is built the same way. **The NAIC's enforcement model requires the category of evidence its records models leave unpreserved.**

The Unum examinations show the same dependence from the regulators' side. The multistate report stated its findings in adverbs: "numerous instances," "many such instances," "certain instances," "a significant number of instances." It could not state them in counts, because its samples were drawn by company and line of business rather than by examiner, and the settlement did not require the companies to keep a record from which any examiner's history could be

assembled. A "general business practice" finding under Model #900 § 3 requires exactly the record the examiners did not have and the settlement did not require.

B. What Models #902 and #910 require a licensee to keep

1. The duty measures what the insurer did, and not what it relied upon. Model #902 § 4(B) states the whole documentation requirement in one sentence: "[d]etailed documentation shall be contained in each claim file in order to permit reconstruction of **the insurer's activities** relative to each claim." A claim file showing every step the adjuster took, in order, with dates, satisfies that sentence. Section 4(A) confirms it by enumerating the data an insurer must produce: "the claim number, line of coverage, date of loss and date of payment of the claim, date of denial or date closed without payment." Six items, recording that a claim was denied and when, with no field for why.

2. The one model that does better has largely not been adopted. Model #910 § 6(A) uses the same measure in its opening sentences, requiring claim files "sufficiently clear and specific so that pertinent events and dates of these events can be reconstructed." But it then provides that a claim file "shall, **at a minimum**, include the following items," and that list operates as a floor. Two listed items reach the substance of a decision in all three lines of business: "claim investigation documentation" and "correspondence used for determining and concluding claim payments or denials." A third, "any claim manuals or other information necessary for reviewing the claim," appears in the property and casualty list at § 6(A)(1) and in neither § 6(A)(2) nor § 6(A)(3). Model #910 therefore requires the denial correspondence to be kept.

The NAIC's own state page for that model, ST-910 (Fall 2022), records "NO CURRENT ACTIVITY" for thirty-nine of the fifty-one jurisdictions listed, and a citation for twelve. Among the thirty-nine are California, Texas, Florida, Illinois, Pennsylvania, Ohio, Georgia, New Jersey, and Michigan. The state page for Model #902 (Fall 2023) records no activity for sixteen. **The states adopted the model that measures the duty by the insurer's activities and declined the model that identifies the denial correspondence.** These are the NAIC's own compilations; the NAIC states that they are not formal legal opinions and that readers should consult state law, and they are cited here for the pattern rather than for the status of any particular state.

3. The expert record is never identified. The terms "expert," "consultant," "independent medical," "peer review," "engineer," and "appraiser" appear zero times in Models #900, #902, and #910. Model #910 § 6(A)(1) lists the property and casualty claim file down to police reports and salvage documentation, and omits the report on which a denial rests where the denial rests on a retained professional, along with what that professional was paid. The health list at § 6(A)(3) comes closest, with "health facility pre-admission certification or utilization review documentation," showing that the drafters identified a reviewer's work product where they intended to, in one line of business.

The Unum settlements repeat the omission. The Regulatory Settlement Agreement's claim-file provision defines what must be kept, "all documents relating to a claim history and/or decision," and not what must be created or how it must be indexed. The reassessment unit's tracking duties ran to notice dates, form dates, decision dates, and outcomes, never to the examiner used. The regulators who had just found the companies "selectively using independent medical

examinations" wrote a retention clause in which the examiner does not appear. (Addendum B, Parts IV.F and IV.G.)

4. The duty is defined by the examiner's needs, and confined to the single claim. Model #902 § 4 opens "To aid in such examination"; Model #910 § 2 states its purpose as retention "for market conduct purposes"; Model #910 § 4(A) requires records so the commissioner can ascertain compliance "during an examination." **A duty defined by its beneficiary will be read to end where that beneficiary's interest ends**, which is why a minimum retention period tends to be treated as the maximum. The same construction confines it to the individual claim: Model #902 § 4(B) reaches the insurer's activities "relative to each claim," which leaves out the reviewer's other assignments and the outcome distribution across them. Compensation sits further outside still. What a licensee pays a claim-evaluation source is ordinarily held in its accounting records, under the vendor, and not in any claim file, so no claim-file rule was ever going to reach it.

5. Duration. Model #902 § 4(A) requires data for "the current year and the two preceding years." Model #910 § 6(A) requires the claim file for "the calendar year in which the claim is closed plus three (3) years," with a Drafting Note contemplating five years for some states. Both are shorter than the period over which a pattern becomes visible. Dr. Swartz's nineteen engagements ran over five years. The compensation ordered in *Warner v. Unum Life Insurance Co. of America*, No. 12 C 2782, 2013 WL 3874060 (N.D. Ill. July 26, 2013), ran five years, and in *Wittmann v. Unum Life Insurance Co. of America*, No. 17-9501, 2018 WL 3374164 (E.D. La. July 11, 2018), four. The reports ordered in *Kelly* ran five years, and in *Small* nearly a decade.

The NAIC already knows how to write a records-integrity rule. Model #910 § 9(B) requires computer-based records to be "archival in nature, so as to preclude the alteration of the record after the initial transfer." Addendum A asks the NAIC to extend requirements it has already written.

C. California's claims regulations, and the conflict already in place

California's Fair Claims Settlement Practices Regulations, 10 Cal. Code Regs. § 2695.3, impose a documentation and retention duty in three parts. **Subsection (a)** requires claim files to "contain all documents, notes and work papers (including copies of all correspondence) which reasonably pertain to each claim **in such detail that** pertinent events and the dates of the events can be reconstructed **and** the licensee's actions pertaining to the claim can be determined." **Subsection (b)(1)** requires claim data "accessible, legible and retrievable for examination," available "for the current year and the four preceding years." **Subsection (b)(3)** requires that claim files "be maintained for the current year and the preceding four years."

First, the words that set the measure describe a chronology. Events, dates, and what the licensee did. A file permitting complete reconstruction of the sequence satisfies subsection (a), whether or not it records the facts and opinions relied upon, the policy language applied, or the reason given. Subsection (b)(1) confirms it: the required data is claim number, line of coverage, dates, and whether the claim was accepted, denied, or closed without payment. As in Model #902 § 4(A), there is no field for why.

Second, the regulation enumerates no documents, and no California analogue to Model #910 has been located. The NAIC's ST-902 state page records this subchapter as California's counterpart to Model #902. Its ST-910 state page lists California under "NO CURRENT ACTIVITY." So the one place in the NAIC's models where a claim file must contain "claim investigation documentation" and "correspondence used for determining and concluding claim payments or denials" appears to have no California counterpart. **No located California claims regulation requires a licensee to retain the claim investigation documentation or the report on which a denial rests.** This is a statement about what has been located, and about claims regulations. California may impose record-retention obligations elsewhere in its law; none bearing on claim handling has been found.

Third, the five-year duty this draft would override is real, and these regulations are not marginal. Section 6(C)(1) requires deletion within forty-five days, and the draft speaks to the conflict only at § 6(C)(2)(a), which says the licensee may keep the file. Section 29 does not reach it, for the reasons at § IV.E. These are also the regulations at issue in the one adjudicated enforcement action described at § V.E: the insurer there challenged §§ 2695.1(a), 2695.2(l), and 2695.2(y) as facially invalid, prevailed below, and was reversed on appeal, which upheld all three. Section 2695.3 was itself never litigated, but the subchapter containing it is the one an insurer contested for a decade.

D. *Campbell*, and the case for an affirmative duty

Two features of *State Farm Mutual Automobile Insurance Co. v. Campbell*, 538 U.S. 408 (2003), bear on what this draft would permit.

The nexus requirement. *Campbell* confirms that a defendant's other conduct is probative of reprehensibility while constraining which other conduct qualifies. Such conduct "must have a nexus to the specific harm suffered by the plaintiff." *Id.* at 422. "A defendant's dissimilar acts, independent from the acts upon which liability was premised, may not serve as the basis for punitive damages." *Id.* at 422–423. Read together, these direct the inquiry toward evidence of conduct **similar** to that which harmed the plaintiff: the same insurer, the same provision, the same stated reason, the same reviewer. That evidence resides principally in the licensee's own records, and is usable only where the licensee has kept them and can retrieve them by something other than claim number.

Why an anti-destruction rule alone would be insufficient. Justice Ginsburg's dissent, quoting the trial court, recites that State Farm made "systematic" efforts to destroy internal documents "that might reveal its scheme"; that an in-house attorney "instructed Utah claims management to search their offices and destroy a wide range of material of the sort that had proved damaging in bad-faith litigation in the past"; and that State Farm "admitted that it destroyed every single copy of claim-handling manuals ... on file in its historical department as of 1988." *Id.* at 434–435 (Ginsburg, J., dissenting) (quoting the trial court). The finding that bears most directly on this draft follows: the trial court found that "in recent years State Farm has gone to **extraordinary lengths to stop damaging documents from being created in the first place**," and that the company "kept no records at all on excess verdicts in third-party cases, or on bad-faith claims or attendant verdicts." *Id.* at 435.

This is the dissent's recitation of the trial court's findings, offered as illustration. It is no holding of the Court, and no conduct is attributed to any present licensee. The relevance is to drafting: **a rule prohibiting destruction answers the first set of findings and leaves the second untouched.** Where the aggregate record is never compiled, there is nothing to destroy and nothing to preserve, every individual claim file remains complete, and no litigant can point to a missing document. That is why Addendum item 7 asks for a duty to preserve **and to index**. A savings clause preserves a cause of action; an indexing requirement causes the underlying evidence to exist.

The Unum record supplies the disability-line version of the second finding. In *Kelly*, Unum's designee testified that the company kept no rating or evaluation system for its examiners. In *Clark v. Unum Group*, No. 4:20-CV-04013-KES, 2022 WL 17251352 (D.S.D. Nov. 28, 2022), a claims supervisor testified that recovery targets were passed on orally, and the court concluded that "even crediting Peter's testimony wholly, there would be no documents showing this practice." In *Hangarter*, company doctors were directed not to record disability opinions in the file, and roundtable decisions "were not documented in the claims files." A preservation duty that attaches only to documents already created does not reach a practice conducted without documents. An indexing duty does, because it requires the licensee to be able to retrieve, by source, what that source produced. (Addendum B, Parts II, IV.C, and VI.E.)

It is noted with appreciation that § 34 of the July 24 draft has been revised to add that the Act may not "be construed to curtail a private cause of action which would otherwise exist in the absence of this Act." Addendum item 13 is drafted to build on that clause rather than to strike it.

E. Enforcement

This section describes a result produced by the ordinary operation of the models' own design. It rests on two matters: the PacifiCare proceeding in California under the framework Model #900 carries, described from the filings, and the Unum settlements described in Part II. Each is the strongest available instance of its kind, and the two produce the same result from opposite directions.

1. The one adjudicated case under Model #900's framework. In its Decision imposing the largest penalty in the Department's history, the California Department of Insurance described the matter before it in its own words:

"[T]his is the first, and only, UIPA case ever litigated to either a proposed or final decision. All the other matters settled long before the litigation and penalty phase."

The Unfair Insurance Practices Act, Insurance Code § 790 et seq., is California's enactment of the framework Model #900 carries, added by Stats. 1959, ch. 1737. The statement appears in the Commissioner's Decision and Order of June 9, 2014, which was later set aside on judicial review; the sentence quoted is the Department's account of its own enforcement history, and nothing in the subsequent proceedings has disturbed it. Matters were initiated, and settlement disposed of all of them before any adjudication. **The finding is bounded, and correction of it is invited.** It says nothing about consent orders, complaint mediation, or market conduct examinations, none of

which adjudicates. If the NAIC holds data showing a materially different picture, that data would change the analysis and would be welcome.

In May 2007 the Department opened a targeted market conduct examination of a health insurer's claims handling, concluding that the insurer had violated the Insurance Code nearly one million times and recommending penalties of approximately $325 million. The Order to Show Cause issued January 25, 2008. The evidentiary hearing ran from December 7, 2009 to June 27, 2013: more than 230 hearing days, more than 60 witnesses, some 2,000 exhibits, and a record exceeding 50,000 pages. On August 5, 2013 the administrative law judge found 883,735 violations and proposed a penalty of $11,518,350. On June 9, 2014 the Commissioner rejected that proposed decision, found 908,547 violations, imposed a penalty of $173,603,750, and designated the decision a precedent decision.

Nothing in that decision has taken effect. On judicial review the trial court invalidated three of the claims-handling regulations and then, in September 2017, set aside all nineteen penalty categories. The Court of Appeal reversed the regulatory ruling and upheld all three regulations, *PacifiCare Life & Health Ins. Co. v. Lara*, 27 Cal. App. 5th 391 (2018), then reversed the penalty judgment as well and remanded for what it called a do-over, No. G056160, 2022 WL 1315467 (Cal. Ct. App. May 3, 2022). On remand the matter was retried. In August 2023 judgment was again entered for the insurer, and a writ issued directing the Commissioner to vacate the administrative decision.

In April 2024 the trial court awarded the insurer $66,153.13 in costs. The largest component, $49,827.50, was the insurer's attorney fees for preparing the administrative record of the Department's own enforcement action, awarded on a finding that the Commissioner had not produced an adequate record in the twelve months after the insurer requested it, and that the insurer's work assembling a complete one was "not just reasonable, but essential." A records regime built to serve the examiner failed to produce a usable evidentiary record even for the examiner, in the one case where everything depended on it.

Two appeals remained pending as of the most recent filing reviewed here, the Commissioner's reply brief of January 9, 2026. Eighteen years after the Order to Show Cause there has been no final adjudication of the underlying conduct. *This account is drawn from the filings and ends at January 9, 2026. The costs award is itself on appeal and is not final.*

Why California is the model's most favorable test. The natural inference is that California's statute is weak or its Department under-resourced. California in fact adopted a liability threshold lower than Model #900's. Where § 3 of the model reaches an act "committed flagrantly and in conscious disregard of this Act," California's § 790.03(h) reaches acts "[k]nowingly committing or performing with such frequency as to indicate a general business practice." Knowledge is the lower bar, and it is lower by a wide margin for a practice conducted through credentialed intermediaries, which is built to look measured. A jurisdiction took the model, made liability easier to establish, and applied the result to an insurer against which its own examiners had found nearly a million violations. The result was one adjudicated case in sixty-seven years and no final determination in eighteen.

The two statutes also differ in the penalties they authorize, and this letter leaves that difference out deliberately. The size of an authorized penalty explains what an action recovers and says nothing about whether one is brought. The constraint lies in the procedural and economic reality of contested adjudication conducted by a sole public enforcer, and Model #900 § 1, Model #910 § 1, and § 34 of this draft each bar a private right of action, making the enforcer sole.

2. The one examination that reached the practice. The PacifiCare matter shows what happens when a regulator adjudicates. The Unum settlements show what happens when a regulator settles, which the Department's own decision says is what happened in every other matter. The multistate examination closed by settlement. The regulators' summary acknowledged that "no specific 'findings' were reached," and the examination report itself stated that the settlement "obviated the need for additional investigation, review of a larger claim sample, specific claim findings or reaching a formal conclusion concerning the examination objective." The 2008 re-examination was confined to "the issues addressed by the Multistate Examination." During the agreement, each participating state agreed not to conduct its own Model Act market conduct examination or impose remedies for the matters it covered. (Addendum B, Part IV.F and note 107.)

The two instances together describe the range of public enforcement. Where the regulator adjudicated, eighteen years produced no final determination. Where the regulator settled, the settlement created no record of the practice it settled, and the participating states agreed not to examine the matters it covered while the agreement was in force. Neither instance produced a final adjudication of a general business practice. The Unum instance produced no fact about any examiner's compensation, engagement history, or outcome record. Every such fact in the public domain came from a private litigant. Model #900 § 1, Model #910 § 1, and § 34 of this draft bar a private right of action. What the private litigant has, and what this draft would permit a licensee to destroy, is the closed claim file of another insured.

3. Model #670. A search of California's counterpart to the model this draft would replace has located no enforcement action in approximately forty-five years. California enacted Model #670 as the Insurance Information and Privacy Protection Act, Insurance Code § 791 et seq., in 1980; the Senate Judiciary Committee's analysis of SB 354 records that "[t]he IIPPA was enacted in 1980, well before the digital revolution transformed how data is collected, stored, and shared." This finding rests on a search of reported decisions and publicly available administrative records. It does not capture consent orders, unappealed administrative actions, or informally resolved matters, and it concerns one state. If the framework being replaced has not operated, then what this draft adds is a set of deletion provisions layered onto a protection with no demonstrated enforcement history. The Working Group is in a position to establish or refute that premise.

F. The questions posed in May, which remain open, and four more

The inquiry letter of May 18, 2026 posed twenty-one requests for information. The May 21 response confirmed that the chairs had reviewed the letter and directed that comments be filed in the present window. **It did not address any of the twenty-one questions.** The August 6 letter renewed five of them. An NAIC staff email of August 17, 2026 stated that the Working Group does not

provide point-by-point responses to individual comment letters, and did not answer them. They are renewed again, and four are added on the Unum record.

Each asks for identification of specific matters and materials. Where the NAIC holds no responsive information, a statement to that effect would be equally useful, and is requested in the alternative.

(A) **Adjudicated enforcement under Models #900 and #880.** Please identify each matter under Model #900, Model #880, or a state counterpart that has been litigated to a proposed or final decision determining that an insurer engaged in an unfair claims settlement practice, giving for each the jurisdiction, the case or docket name and number, the date of decision, and the disposition. Consent orders, informal resolutions, and examinations closed without adjudication are outside the request. Please also identify any database, compilation, or examination-tracking record from which the NAIC or its members draw such matters, and any guidance, analysis, or survey addressing what a state must show to establish the "general business practice" element of Model #900 § 3.

(B) **Model #670 enforcement.** Please identify each enforcement action brought under Model #670 or a state counterpart in any jurisdiction, giving the jurisdiction, the respondent, the citation or docket number, the date, and the disposition. The search described at § V.E located none under California's counterpart in approximately forty-five years, and it reaches one state and does not capture consent orders or informally resolved matters, so any list the NAIC holds would materially change the analysis in this letter.

(C) **The retention of financially dependent experts.** Please identify each enforcement action, investigation, market conduct examination finding, regulation, bulletin, or written guidance, in any jurisdiction, addressing an insurer's retention, selection, supervision, or compensation of a person whose opinion is relied upon in evaluating a claim. Citations or docket numbers, jurisdictions, and dates are requested for each.

(D) **The conflict with Model Regulation #902 and with state claims regulations.** Please identify any analysis, memorandum, drafting note, staff assessment, or comment received by the Working Group addressing the interaction between this draft's deletion provisions and Model Regulation #902's claim-file retention and documentation requirements, or the corresponding state regulations. Please also state which instrument the NAIC understands to control where this draft permits destruction of a record that #902, or a state regulation adopted from it, requires an insurer to retain. Section V.C sets out California's, which requires five years and which this draft would override on forty-five days' notice.

(E) **What remains.** Please identify any assessment the NAIC has made of what enforcement mechanism for Models #900 and #880 remains available if the cross-claim record on which both regulators and private litigants depend may lawfully be destroyed on the licensee's own schedule, together with any document in which that assessment is recorded.

(F) **The Unum selection rule.** Section B.3.d of the 2004 Regulatory Settlement Agreement requires the Unum companies to select examiners "without regard to results of previous IMEs or FCEs conducted by such individuals," and survives the agreement's termination. Please

identify any examination, report, data request, or finding by the lead regulators, by any participating state, or by the NAIC, at any time since the 2008 re-examination, addressing the selection, compensation, engagement volume, or outcome history of the examiners and reviewers used by those companies. Please also identify any record from which compliance with § B.3.d has been or could be assessed.

(G) **Examiner compensation and volume, generally.** Please identify any record held by the NAIC or, to the NAIC's knowledge, by any member department, in any jurisdiction and for any year, showing the compensation paid by a licensee to an independent medical examiner, file reviewer, peer reviewer, or the vendor supplying one, or the number of engagements any such person received from a licensee. If no such record exists, please state so.

(H) **Reports indexed by examiner.** Please identify any state law, regulation, bulletin, examination standard, or settlement provision, in any jurisdiction, that requires a licensee to retain the reports of its claim-evaluation sources in a form retrievable by the identity of the source.

(I) **Sections 5(A)(2) and 6(C) and the vendor layer.** Please identify any assessment the Working Group has made of the effect of §§ 5(A)(2) and 6(C) on records held by third-party service providers that supply medical, engineering, or other expert opinions to licensees, including the compensation and engagement records of the individual professionals those vendors engage, together with any comment received on that subject.

These are questions the amendments are designed to make unnecessary. If the answers show an active enforcement record, the amendments cost the NAIC very little, since on that assumption they constrain conduct that is already absent. If the answers are unavailable, the amendments are the least expensive protection against a consequence no one intends.

VI. THE PROPOSED AMENDMENTS

Addendum A sets out fourteen items. Nine are redlines against the July 24 draft, reproducing the baseline text verbatim; four propose new sections; and one supplies definitions keyed to alphabetical insertion points. Each states why the amendment is asked for, so this section states only what is needed to weigh them, and what the Unum record adds.

A. The duty: item 7

Item 7, new § 5A: preservation and repository of claim-evaluation records. This is the records-retention duty this letter asks for. It requires a licensee to preserve claim-evaluation records, to retain them in a repository retrievable by the identity of the claim-evaluation source, by each policy provision cited or applied, and by the individual who made or approved the claim decision, and to keep them for five years after claim closure, with ten years for the source's assignment list and compensation record, neither of which contains any consumer's identity.

Section 5A supplies what the Unum settlements omitted. Part II.A identified three requirements that were available to the regulators in 2004 and 2005 and that neither settlement imposed. Section 5A supplies two of them. Subparagraphs (A) and (B) of the *claim-evaluation record* definition at item 3 cover "the list of all claims for which the source provided facts or opinions" and

"all compensation paid to the source," and § 5A(C)(2) retains them for ten years. That is the compensation and engagement record from which financial dependence is assessed, and which *Demer* found sufficient, from amount and frequency taken together, to shift the burden to the administrator. Subparagraph (C) covers the licensee claim reports themselves, and § 5A(A) requires that they be retrievable by the identity of the source. That is the report set from which the *Chacko* court verified that the reviewer had found fifty of sixty-one claimants not disabled, with no compensation discovery, no admission, and no trial of any other claim. Both requirements reach the vendor, because § 5A(A) requires the licensee to "require each third-party service provider to preserve," and item 6 carves claim-evaluation records out of the vendor destruction clause at § 5(A)(2). The per-physician compensation that Unum told the *De Mello* court it did not have would, under § 5A, be a record the licensee is required to preserve.

Section 5A requires a repository, and not a larger claim file. That distinction matters for one category in particular. What a licensee pays a claim-evaluation source is ordinarily held in the accounting system, under the vendor, rather than in any claim file, and § 5A(A) is drafted accordingly: it requires that the records be retained and retrievable together, and leaves the licensee to decide where they physically reside. Nothing in it enlarges the claim file or requires an insurer to move accounting data into one.

The indexing requirement is what the settlements lacked. The Regulatory Settlement Agreement required the companies to keep "all documents relating to a claim history and/or decision." Nothing suggests the companies failed to keep them. What no one could do was retrieve them by examiner, because nothing required the examiner to be an index field. The claimant in *Mercer v. Unum Life Insurance Co. of America*, No. 3:22-CV-00337, 2023 WL 3131989 (M.D. Tenn. Apr. 27, 2023), asked for one physician's evaluative files, and Unum answered with a paralegal's estimate that reviewing them would take more than 300 hours; the court denied production. The claimant in *Clark* narrowed the request to one condition and three years, and the court ordered it. The difference between the two outcomes is the cost of retrieval, and § 5A(A) removes that cost by requiring the records to be retrievable by source in the first place. An insurer that keeps its records that way also gains something. It can do what the *Demer* administrator could not, and produce "records of its reviewers' findings on claims to show their neutrality in practice." A repository indexed by source is the only form in which an insurer's assertion that its reviewers are neutral can be tested, in either direction.

Two further features answer the objections it will draw. The duty reaches the basis and manner of a licensee's claim decisions **whether or not a professional was retained**, for the reason at § III.B: at least five of the eleven purposes for which courts order this discovery involve no expert. And the indexing requirement, not the retention period, is what makes the records usable, because a practice becomes visible along those three axes and rarely on the face of one file. Section 5A is drafted to supply what Model #900 § 3's "general business practice" standard requires and what §§ V.B and V.C show the records models leave unpreserved. It reaches no record outside the defined category, and it excludes the litigation file and settlement communications.

Items 1, 2, 3, 5, 6, and 14 are conforming. Item 3 carries the definitions, of which *claim-evaluation record* is the substantive one: its subparagraph (D) covers every written communication to a

consumer that states or explains a claim decision **or any reason given for it**, which is the category defined by the reason given that the retention models never identified. Item 14 supplies the transition rule, without which a purely prospective reading would leave records already in existence outside the duty.

B. The amendments that limit what this Act permits

Seven items explained in Addendum A. In the order they arise in the Act: **item 4** requires that de-identification under § 4(J) preserve cross-claim linkage, which is the least visible route to destruction in the draft and the amendment most worth the Working Group's attention; **item 8** makes § 6(C)(2)(a) mandatory so that compliance with other retention law is a duty rather than an option, confirms that § 6(C)(2)(d) is not limited to a proceeding involving the requesting consumer, and adds a carve-out at (e) that protects the requesting consumer more thoroughly than the current draft does; **item 9** bars solicitation of deletion requests, and describes no conduct attributed to anyone; **item 10** extends § 24(A)(7) to party-served discovery, arbitration, and appraisal, none of which the operative text presently names; **item 11** carves § 5A out of the § 28 HIPAA deeming clause and leaves that clause otherwise intact; **item 12** preserves stronger state retention law, which Articles II and III presently lack any savings clause for; and **item 13** supplies a right of action confined to the record-retention obligations, a rebuttable presumption from non-preservation, and a provision that compliance with this Act is no defense to a preservation duty arising elsewhere.

Part II bears on two of these. Item 11 matters because every decision described in Part II arose on a health or disability claim, and § 28 as drafted would let a HIPAA-governed disability insurer assert deemed compliance with the entire Act. Item 13 matters because a claimant cannot show what a destroyed file contained. Where a licensee has destroyed the records that § 5A requires it to keep, § 34(C) supplies the inference that a court would otherwise have no basis to draw.

C. Four conforming amendments to Models #902 and #910

This draft would authorize the destruction of records those regulations require a licensee to keep, and each was written without reference to the other. The amendments below would resolve that conflict from the other side. They are offered for whatever use the Working Group finds for them.

(A) **Identify the record.** Add to #910 § 6(A) a category for the reports, opinions, and evaluations of any retained professional or vendor relied upon or referenced in a claim decision, with the identity of the source and the compensation paid.

(B) **Extend the duty past the individual claim.** Amend #902 § 4(B) and #910 § 4(A) so that a licensee's use of a given claim-evaluation source can be reconstructed **across claims**, indexed by source identity. **This asks for indexing and adds no retention period. It is the most consequential of the four.**

(C) **State the beneficiary.** Amend the purpose clauses at #902 § 4 and #910 § 2 so the retention duty is not defined solely by examination convenience.

(D) **Require the source to disclose in the file.** Add to #910 § 6(A) a requirement that any claim-evaluation source whose facts or opinions are relied upon in a claim decision state, with the opinion and in the claim file, the number of engagements accepted from the licensee and its affiliates and vendors over a defined preceding period, the compensation received for them, any other financial interest or business relationship with the licensee likely to affect impartiality, and the disposition of the prior engagements. This is the first of the three requirements identified at § II.A. It is modeled on the disclosure California requires of every neutral arbitrator under Cal. Code Civ. Proc. § 1281.9, and on the disclosure the California Department of Insurance required of its own Independent Review Director in the 2005 Unum settlement. The duty attaches to the source rather than to the licensee, which makes it self-executing, and it carries none of the arbitration statute's apparatus of objection and waiver, which belongs to a party who may decline the neutral and has no application to a claimant who may not. It asks the source to write down what the source already knows. It belongs in a claims-handling regulation rather than in a privacy act, which is why it is offered here and not as an item in Addendum A. (Addendum B, Part IV.G.)

Redlined language for these amendments will be provided on request, or when Models #902 and #910 are taken up.

VII. CONCLUSION

This draft would permit closed claim files, and the vendor files behind them, to be destroyed on a schedule the licensee writes and no one reviews. Those files hold the cross-claim evidence that Model #900's "general business practice" standard requires and that Models #902 and #910 leave unpreserved. The Unum record shows what that evidence has been worth. In 2004 the NAIC's own members examined the largest disability insurer in the country, found the practice this letter concerns, and prohibited selecting examiners by their results without requiring any record of those results. Twenty-one years later, the only facts in the public domain about any examiner's compensation, volume, or outcome history have come from private litigants who obtained them through discovery, over the insurer's objection. The records can be preserved in an act whose stated purpose is privacy at no cost to that purpose, because the consumer's identity can be removed from them without loss to the evidence, as courts have done by redaction and protective order for twenty-seven years.

The Working Group is respectfully requested to:

(A) Adopt Addendum item 7, the preservation and indexing duty, together with its transition rule at item 14. This is the substantial request. It supplies what Model #900's "general business practice" standard requires, what Models #902 and #910 leave unpreserved, and what the 2004 and 2005 Unum settlements omitted;

(B) Adopt the remaining items at Addendum A, which limit what this Act permits or clarify what it already permits, and which are severable from item 7 and from each other;

(C) Consider the four conforming amendments to Model Regulations #902 and #910 at § VI.C;

(D) Consider Addendum B as part of the record of this proceeding, and, if any member department holds information that would correct or supplement it, provide that information; and

(E) Provide the information requested at § V.F, or state that the NAIC holds none responsive.

I would be glad to walk through the redlined language, the questions at § V.F, or the record in Addendum B by telephone at the Working Group's convenience. I am available on short notice at 805.298.1152 or cdion@exposingexpertbias.com.

Thank you for the Working Group's consideration.

Respectfully submitted,

/s/ Christopher L. Dion

Consulting Attorney

Addendum A, Proposed Amendments to Model #672, redlined from the July 24, 2026 Full Exposure Draft, is submitted concurrently with this letter.

Addendum B, *Designed to Deny: The Unum Scandal, Biased Medical Experts, and the Failure of the Regulatory Settlements*, is submitted concurrently with this letter as a separate document.

ADDENDUM A

Proposed Amendments to Model #672

Redlined from the July 24, 2026 Full Exposure Draft

Submitted with the comment letter of Christopher L. Dion dated September 22, 2026

ARTICLE I. GENERAL PROVISIONS

Item 1. § 1 (Purpose):

Redline.

Purpose. This Act governs the treatment of nonpublic personal health information and nonpublic personal information about individuals by all licensees of the state insurance department. This Act:

A. Requires a licensee to provide notice to individuals about its privacy policies and practices;

B. Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal information about individuals to affiliates and nonaffiliated third parties; and

C. Provides methods for individuals to prevent a licensee from disclosing that information.

Why. Absent a purpose hook, § 5A is exposed to a "beyond the stated purpose of the Act" objection. The purpose is stated in two facets, source neutrality and the basis for and manner of claim evaluation, because a purpose clause limited to the first would narrow § 5A by implication. *Conforming to item 7.*

Item 2. § 2(A) (Scope): confirm the Act reaches these records after de-identification

Redline.

A. Scope. This Act applies to:

(1) Nonpublic personal information about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. This Act does not apply to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes; and

(2) All nonpublic personal health information

Why. Because § 4(Q) excludes de-identified data from "nonpublic personal information," a de-identified claim-evaluation record could be argued out of the Act's scope entirely, taking § 5A's duties with it. This places the records within the Act's coverage for the limited purpose of § 5A, without making them nonpublic personal information. *Conforming to item 7*.

Item 3. § 4 (Definitions): eight insertions

Drafting instruction to the Working Group. Insert each definition at its alphabetical position and re-letter subsequent subsections accordingly. Anchor points below are keyed to the July 24, 2026 lettering, which runs A through V and then X through AA: twenty-six definitions, **with no subsection W**. Two of these eight are fundamental definitions: ***claim-evaluation record*** and ***claim-evaluation source***. The remaining six are supporting definitions used within them.

Insert before § 4(A) ("Affiliate"):

Insert after § 4(B) ("Biometric data"), before § 4(C) ("Clear and conspicuous"), in this order:

Insert after § 4(G) ("Consumer"), before § 4(H) ("Consumer reporting agency"):

Insert after § 4(L) ("Financial product or service"), before § 4(M) ("Insurance product or service"):

Insert after § 4(N) ("Licensee"), before § 4(O) ("Nonaffiliated third party"):

Why. Eight insertions, two of which do the substantive work. *Claim-evaluation record* defines the category by function. Its subparagraph (D) supplies what Models #902 and #910 do not: it covers every written communication to a consumer that states or explains a claim decision **or any reason given for it**, whether or not any source is referenced. That category, defined by the reason given, is the one the retention models never named. *Claim-evaluation source* covers any person whose facts or opinions are relied upon in a claim decision, regardless of any exclusion that would otherwise apply under another definition in the Act. Subparagraphs (A)–(C) and (F)–(G) of the record definition are source-keyed by their nature; (D) and (E) are not. The litigation and settlement carve-out in *claim decision* is confirmatory, and is deliberately **not** phrased in terms of privilege or work product, for the reason given at item 7. The remaining six definitions support these two, and each is tied to an alphabetical insertion point in the July 24 lettering.

Item 4. § 4(J) ("De-identified data"): de-identification must preserve cross-claim linkage

Redline.

J. "De-identified data" means information that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual.

Why. Section 5(A)(2) authorizes de-identification as an alternative to deletion, and § 4(Q) places the result outside the Act. Nothing constrains *how* the removal is performed. A licensee that removes the consumer's identity without retaining a stable claim-level identifier, or that partitions the reports, the correspondence, and the consumer's objections into stores that cannot be joined, has complied with every word of § 4(J) and destroyed the usefulness of the records, leaving no deletion to challenge and no missing document for anyone to notice. **This is the least visible route to destruction in the draft.** Two operations both remove the consumer's identity: one leaves the record analyzable across claims, the other does not. This amendment asks only that the permitted operation be the first. The operative text is at § 5A(D), which requires that de-identification preserve the cross-claim linkages, the integrity of each claim as a single reviewable transaction, and a persistent claim identifier. It is **privacy-enhancing on its face**: it removes the consumer's identity from the analytical record while leaving the accountability data intact. It seeks a better de-identification standard, not a weaker one, and § 4(Q) is deliberately left untouched, because that exclusion is what makes the compromise work in both directions.

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Item 5. Article II heading: conforming

Redline.

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Why. Proposed § 5A sits most naturally after § 5, because § 5 is the provision that mandates vendor-side destruction. The current Article heading does not accommodate a preservation duty. Retitling is the minimal-ripple fix. *Conforming to item 7.*

Item 6. § 5(A)(2): conforming carve-out from vendor-side destruction

Redline.

(2) Requires the third-party service provider to delete, destroy, de-identify or return all nonpublic personal information to the licensee when requested by the licensee; or to delete nonpublic personal information after it is no longer necessary to fulfill a legal requirement or to meet the record retention requirements of the licensee or third-party service provider and to notify the licensee of the action taken;

Why. The trigger for mandatory downstream destruction is "the record retention requirements of the licensee", which is a schedule this Act nowhere regulates. Because expert reports, referral instructions, compensation records, and often the claim correspondence itself are held by vendors rather than by the licensee, this is the provision that reaches the records at issue.

Item 7. new § 5A: Preservation and Repository of Claim-Evaluation Records

Proposed text.

rafting Note (proposed, to follow Section 5A).

This Section establishes an affirmative, continuing duty to preserve records bearing on the reliability and neutrality of the sources on whose facts and opinions claim decisions rest, and on the basis for and manner of the licensee's own evaluation and decision of claims. The second category is not conditioned on the involvement of any retained professional. The duty is independent of, and additional to, any preservation obligation arising from pending or anticipated litigation; it is not a litigation hold and does not depend on one. Subsection A requires that the records be retrievable by source identity, by policy provision applied, and by the individual who

made or approved the decision, because each is an axis along which a practice becomes visible that no single claim file discloses. Subsection D permits removal of the consumer's identity from the retained record. That identity remains recoverable only by the licensee, only through the segregated association at Section 6(C)(2)(e), and only for notice and consent under judicial supervision; it is not recoverable by any other person from the retained records. Subsection E confirms that neither this Section nor any other provision of this Act creates a confidentiality, privilege, or privacy objection to production in an adjudicative process. The consequence of non-preservation is addressed at Section 34(C).

Why. This is the records-retention duty the accompanying letter asks for.

The gap it closes. No provision of this Act requires preservation of any record bearing on a source's reliability or neutrality, or on the basis for a claim decision; across thirty-five sections the sole affirmative record-maintenance obligation is § 6(D)(3)(b), covering the consumer's written statement of disagreement. Nor do the NAIC's records models supply it. Model #902 § 4(B) measures an insurer's documentation duty by whether "the insurer's activities" can be reconstructed, and its § 4(A) data set records that a claim was denied and when, with no field for why. California's 10 Cal. Code Regs. § 2695.3(a) uses the same measure: pertinent events, dates, and the licensee's actions. Model #910 § 6(A) does require "claim investigation documentation" and "correspondence used for determining and concluding claim payments or denials," and the NAIC's own state page, ST-910 (Fall 2022), records "NO CURRENT ACTIVITY" for thirty-nine of fifty-one jurisdictions, California, Texas, Florida, Illinois, Pennsylvania, Ohio, Georgia, New Jersey, and Michigan among them. So in most states nothing located requires a licensee to keep the report on which a denial rests. Compensation sits further outside still: what a licensee pays a claim-evaluation source is ordinarily held in its accounting records, under the vendor, and not in any claim file, so no claim-file rule was ever going to reach it.

What it supports. Model #900 § 3 conditions liability on conduct "committed with such frequency to indicate a general business practice," which is a cross-claim standard. Section 5A is drafted to supply what that standard requires and to reach no record outside the defined category.

The duty rests on two facets, not one. It reaches source neutrality **and** the basis and manner of claim evaluation, because most of the purposes for which courts order this discovery do not involve a retained professional. Subsection (B) states the scope accordingly, and Subsection (D)(5) states the permitted uses; a use limitation confined to expert neutrality would preserve the records and forbid the analysis for which the rest of them are probative.

A repository, not a larger claim file. Subsection (A) requires that these records be retained together and retrievable together. It does not require that any of them be placed in a claim file, and it does not enlarge the claim file. This matters for the compensation record in particular, which ordinarily sits in the licensee's accounting system under the vendor. The Section leaves the licensee to decide where a record physically resides, and requires only that it survive and be retrievable.

Indexing is the working requirement. Subsection (A) requires retention in a repository retrievable by the identity of the claim-evaluation source, by each policy provision cited or applied, and by the individual who made or approved the claim decision. Each is a line along which a practice may become visible that a single claim file will rarely disclose: the reviewer who always finds the same way, the exclusion construed one way for one insured and the opposite way for the next, the adjuster whose files follow a common pattern. No existing NAIC model requires retrieval along any of them, and that absence is why a retention period by itself would accomplish little.

The remaining subsections. Subsection (C) sets retention at five years after claim closure for the claim-level records, and ten years for the source's assignment list and compensation record, neither of which contains any consumer's identity. Subsection (D) permits removal of consumer identity while preserving analytical linkage, and states permitted uses without limiting any person's use, production, or admissibility of the records. Subsection (E) confirms that nothing in this Act creates a confidentiality or privilege objection to production in an adjudicative process. Subsection (F) confirms that this Act does not displace preservation duties arising elsewhere.

What § 5A leaves out. The litigation file is excluded, as are settlement communications. That carve-out, drafted at item 3, avoids the language of privilege and work product deliberately, because a privilege recital in a preservation section would operate as a grant of protection in jurisdictions whose law presumes the claims file open in first-party bad faith.

Placement. Section 5A is proposed for Article II, immediately after § 5, because Article II contains the vendor-side destruction provision. Final placement and numbering are the Working Group's.

ARTICLE III. CONSUMER REQUESTS

Item 8. § 6(C)(2): mandatory compliance with other retention law, deletion carve-out, and consumer-protection production gate

Redline.

(2) The licensee is not required to delete nonpublic personal information if:

(a) The licensee is required by law or regulation to retain the nonpublic personal information;

(b) The nonpublic personal information may be necessary to perform the contract or service requested by or benefiting the consumer;

(c) The information is necessary to comply with a legal obligation; or

(d) The information is maintained in reasonable anticipation of a claim or civil or criminal proceeding

Drafting note. The amendment to subparagraph (a) is drafted as an insertion within the existing subparagraph so that the lettering of (b) through (e) is undisturbed and no cross-reference elsewhere in the Act requires conforming. The Working Group may prefer to lift the duty out into a separate paragraph; the substance is the same either way.

Why. Section 6(C)(2) opens "The licensee **is not required to delete** … if," and that opening governs all four conditions. Every one supplies an option. Subparagraph (a) applies wherever another law requires retention, which for a closed claim file in California is 10 Cal. Code Regs. § 2695.3(b)(3). So the Act addresses the conflict between its own deletion command and a state retention rule, and resolves it by telling the licensee that it may obey the state rule. **The amendment to subparagraph (a) changes that permission to a duty. It imposes no retention period and creates no new obligation. It requires compliance with retention obligations that already exist elsewhere.**

The remaining amendments address the closed claim file directly. Subparagraph (d) as it stands leaves the decision whether to preserve one insured's file for another insured's benefit with the party that benefits from destruction; the amendment to (d) confirms that it is not limited to a proceeding involving the requesting consumer, and new subparagraph (e) converts the permission into a rule for this category. It also protects the requesting consumer **more thoroughly than the current draft does**: the record is retained, the consumer's identity is de-identified out of it, and that identity is produced only on court order after notice and an opportunity to object. The retained association is what makes that notice possible. *The accompanying letter discusses this conflict at §§ IV.B.2 and V.C.*

Item 9. new § 6(D)(4): no solicitation of deletion requests

Proposed text.

Why. Section 31 bars penalizing a consumer for exercising these rights and is silent on *inducing* their exercise, and the Act contains no dark-patterns provision. Section 6(D)(2) affirmatively removes any cap on the number of requests. A licensee that placed a deletion control in a policyholder portal or claim-closing letter would reduce its own closed claim files one authenticated request at a time, while occupying the posture of a party complying with a mandatory statutory duty. **This item describes no conduct attributed to anyone and is offered as no accusation.** It protects the consumer's right from the one direction the draft leaves open.

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES

Item 10. § 24(A)(7): reach party-served discovery, arbitration, and appraisal

Redline.

(7) (a) To comply with federal, state or local laws, rules and other applicable legal requirements;

(b) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities; or

(c) To respond to judicial process or government regulatory authorities having jurisdiction over a licensee for examination, compliance or other purposes as authorized by law;

or

Why. Subparagraph (b) reaches subpoenas "by federal, state or local authorities"; (c) pairs "judicial process" with "government regulatory authorities" in a series whose other members are governmental. The strings "arbitrat-" and "apprais-" appear nowhere in the operative text of the July 24 draft. A licensee served with a party's document demand, an arbitrator's subpoena, or an appraisal demand has no clear permission under this Act to produce, and a colorable argument that it may not. Given how many insurance disputes resolve in appraisal and arbitration rather than in court, this gap is likely to be encountered often.

ARTICLE VII. RULES FOR HEALTH INFORMATION

Item 11. § 28: narrow carve-out from the HIPAA deeming clause

Redline.

A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

Why. Health claims are where independent medical examination, file review, peer review, and utilization review practices concentrate. Section 28 deems a HIPAA-governed licensee that "maintains nonpublic personal information in the same manner as protected health information" to be "deemed to comply with the requirements of this Act," so without a conforming change a

health insurer could assert blanket deemed compliance and escape § 5A entirely. **The carve-out is narrowed to § 5A alone and leaves the deeming clause otherwise intact.** Retaining these records is consistent with the uses § 25(B) already permits without authorization; combined with § 5A(D)'s removal of consumer identity, the health-privacy concern is addressed by the Act's own text.

ARTICLE VIII. ADDITIONAL PROVISIONS

Item 12. new § 30A: preserve stronger state retention and preservation law

Proposed text.

Why. Section 29 is limited to Article VII and directed at privacy subject matter; Articles II and III, which contain the destruction provisions, are covered by no savings clause at all. The clause above is confined to one direction: it preserves greater state *retention, preservation, and accessibility* law. A generic privacy floor would preserve stronger *deletion* law and, by negative implication, suggest stronger retention law is not preserved. **Section 29 is left untouched.** This item corresponds to Cal. Ins. Code § 791.39(d), which the accompanying letter discusses at § IV.D. Note the limit of what any savings clause accomplishes: § 791.39(d) preserves "existing records retention periods" and other "legal requirements pertaining to records retention," so it preserves what exists and creates nothing. Where a state's existing claim-file rule fixes content by a chronology test, as California's 10 Cal. Code Regs. § 2695.3(a) does, this clause preserves a duration and not a requirement that the report behind a denial be kept. That is why item 7 is asked for alongside it. Placement and final numbering are the Working Group's.

Item 13. § 34 (Individual Remedies): a narrow private right, a presumption, and the completion of the Working Group's own clause

Redline.

Section 34. Individual Remedies

This Act may not be construed to create or imply a private cause of action for violation of its provisions, nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Why. The new non-curtailment clause is a real improvement and should be credited. But a savings clause preserves the *cause of action*; it does not preserve the *record*, and it does not stop this Act from supplying the defense. A licensee that deletes under § 6(C)(1) answers a spoliation claim by saying it destroyed nothing it was entitled to keep. Section 34 does not reach that answer, and its own words confine it to actions "which would otherwise exist **in the absence of this Act**," while the

destruction is what the Act *supplies*. Subsection (E) closes that gap in one sentence, creating no remedy and imposing no duty. Subsections (A) through (D) are the more substantial request: a right of action confined to the record-retention, preservation, and anti-destruction obligations, with damages deliberately omitted, leaving injunctive relief, fees, and the rebuttable presumption at (C) that records not preserved would have been unfavorable.

Item 14. new § 35(D): transition and anti-destruction

Proposed text.

Why. Section 35 says nothing about records already in existence or claims already closed. A purely prospective reading would leave those records outside the duty, and § 35(A)'s compliance extension would operate as a period in which they could lawfully be destroyed before the duty attached. Paragraph (3) therefore attaches the duty not to destroy on the date of enactment, and confines the compliance extension to the building of the repository. *Conforming to item 7.*

End of Addendum A.

ADDENDUM B

DESIGNED TO DENY: THE UNUM SCANDAL, BIASED MEDICAL EXPERTS, AND THE FAILURE OF THE REGULATORY SETTLEMENTS[1]

In November 2004, the chief insurance regulators of forty-eight states, the District of Columbia, and the United States Department of Labor finalized a joint market conduct settlement with UnumProvident, then the nation's largest disability insurer. California concluded a separate settlement the following year. Regulators had documented a systematic pattern of claim denials: UnumProvident relied excessively on internal staff, interpreted ambiguous medical records against claimants, evaluated multi-systemic conditions in isolation, and demanded objective proof far beyond policy terms. California further revealed that the insurer deployed independent medical examinations (IMEs) selectively, overrode internal doctors who supported disability findings, and made substantive claim determinations in unrecorded "roundtable" sessions. Widely praised at the time, the settlements imposed monetary penalties, required claim reassessments, and established new claim-handling standards.

Yet the judiciary had already uncovered the same machinery years earlier. In 2002, a California jury learned that one UnumProvident examiner had rejected total disability in thirteen out of thirteen consecutive reviews, that retainer letters explicitly signaled the desired conclusion, and that a former medical director candidly described the strategy as searching for "the 'right physician to do the IME because we want to get the answer we want.'"[2] Other courts had similarly forced the insurer to disclose examiner payment histories and selection frequencies, establishing a clear evidentiary principle: bias is revealed through an examiner's financial ties and longitudinal record of insurer-favorable opinions.

The 2004–2005 regulatory settlements, however, largely ignored these structural incentives. While prohibiting UnumProvident from choosing examiners based on past outcomes and mandating

---

[1] This article is a working draft submitted for consideration to the Privacy Protections (H) Working Group of the NAIC. It has not yet undergone peer review; it has been prepared without editorial assistance or independent proofreading; errors in grammar, citation format, and cross-references are anticipated and will be corrected in later versions. Readers who identify one are invited to bring it to the author's attention. The analysis rests on primary sources: reported and unreported judicial decisions and discovery orders, the 2004 multistate Regulatory Settlement Agreement and the 2005 California Settlement Agreement together with their examination reports and follow-up examinations, comment letters filed in the Department of Labor's rulemaking on RIN 1210-AB39, and the parties' filings in the dockets cited. These were obtained from commercial legal databases, from federal and state court dockets, and from the publishing agencies. The characterizations of what a decision holds, what an examination found, and what a settlement required are the author's own reading of those documents. They are opinions, not findings, and nothing in this article should be taken as a statement of fact about any insurer's present practices. The author practices law on the policyholder side of insurance disputes, and the argument here is advanced in that light; the record on which it rests is public and is cited so that it can be checked independently.

[2] See note 32 and accompanying text.

objective selection criteria, the agreements required no tracking of examiner compensation, assignment volume, outcome ratios, or selection rationales. Compliance was measured instead through error rates in random file audits—a metric easily satisfied even if an insurer consistently routed claims to physicians who never found a claimant disabled. Unsurprisingly, in the two decades since, courts have continued to confront these identical practices. Every public record detailing examiner compensation, volume, or outcome bias has come not from regulatory oversight, but from individual claimants fighting to discover third-party claim files over the insurer's fierce objections.

This article traces that persistent divide between regulatory reform and judicial discovery. Part I details the governing legal framework—specifically ERISA's trust-law roots, the weight courts accord to insurer conflicts of interest, the federal 2016 reviewer-selection rule, and the four categories of evidence courts evaluate to determine whether a medical opinion was genuine or procured (referred to herein as Factors 1 through 4). Parts II and III examine pre-settlement judicial and regulatory findings, while Part IV analyzes the structural blind spots of the settlements themselves. Parts V and VI document post-settlement litigation, illustrating the heavy procedural burden claimants must bear to uncover examiner bias. Finally, Part VII scrutinizes the insurer's primary defenses against conflict-of-interest claims, concluding with an analysis of why non-party closed claim files remain the sole reliable repository of this evidence.

PART I. ERISA OVERVIEW

A. Trust law and ERISA's fiduciary frame

Although a claim for benefits under an employee benefit plan superficially resembles a standard breach-of-contract action, it is governed by the principles of trust law.[3] Within this framework, the plan administrator acts as a fiduciary bound by fundamental duties of loyalty and prudence. Pursuant to ERISA's statutory command, the fiduciary must execute its obligations "solely in the interest of the participants and beneficiaries" and for the "exclusive purpose of . . . providing benefits to participants and their beneficiaries."[4]

Congress did not adopt trust law to accommodate plan sponsors. As Langbein puts it, the normal private trust "is essentially a gift," and trust law therefore "exhibits great deference to the wishes of the transferor"; in ERISA, by contrast, "Congress imposed trust law concepts for regulatory purposes, to restrict rather than to promote the autonomy of the employer over its employee benefit plans."[5] The distinction matters because the contrary intuition, that a plan is a bargain between counterparties who may each pursue their own interest, has influenced the case law. It

---

[3] Employee Retirement Income Security Act of 1974, Pub. L. 93–406, 88 Stat. 829 (codified as amended at 29 U.S.C. §§ 1001–1461).

[4] 29 U.S.C. § 1104(a)(1)(A). See also John H. Langbein, *Trust Law as Regulatory Law: The Unum/Provident Scandal and Judicial Review of Benefit Denials Under ERISA*, 101 Nw. U. L. Rev. 1315, 1325-1327 (2007).

[5] Langbein, *supra*, at 1316–17 (Introduction).

confuses "a contract counterparty, who is allowed to act selfishly, with an ERISA fiduciary, who is forbidden to."[6]

Trust law presupposes a disinterested trustee. ERISA does not. The statute authorizes the employer to use "an officer, employee, agent or other representative" as a fiduciary, and section 408(c)(3) negates the prohibited-transaction rule that would otherwise forbid the arrangement, "thereby inviting the conflicts of interest that so trouble the law of benefit denials."[7]

A fiduciary who selects, pays, instructs, or evaluates the person whose opinion will decide the claim, and who stands to gain, directly or indirectly, from the outcome, is conflicted well before the claim is decided. The gain need not be the benefit dollars. *Metropolitan Life Ins. Co. v. Glenn* holds that the dual role of deciding and paying "creates a conflict of interest," and that is the paradigm case rather than the limit of the category.[8]

An insurer that renews a vendor whose reviews have produced savings, and declines to renew one whose reviews have not, has created an incentive without writing a contingent term. The reviewer's fee is the same for every opinion; the reviewer's income depends on the opinions.

Such an agreement is outcome-neutral on its face: the reviewer is paid the same whether the claim is approved or denied. The neutrality sits in the instrument and not in the arrangement behind it, so an insurer's answer that its reviewers are paid a flat fee regardless of outcome establishes nothing. Contingent terms supply the same interest more visibly. A contract that pays for savings, a fee or renewal that moves with loss experience, an internal metric that rewards closure, and a reviewer whose future assignments depend on how past ones came out are each a version of it, and none of them requires the decider ever to pay a claim. *Saldi v. Paul Revere Life Ins. Co.* treated an intermediary's interest of that kind as a proper subject of discovery, permitting inquiry into the criteria for referring files, the tracking of those referrals, the relationship between the vendor and the insurers, and "Genex's interest in saving money for its clients."[9]

Fiduciary status turns on function. *Firestone Tire & Rubber Co. v. Bruch* says that "one is a fiduciary to the extent he exercises any discretionary authority or control," and the statutory definition reaches anyone who "exercises any discretionary authority or discretionary control respecting management of [a] plan."[10] A plan document naming someone else does not answer it. The insurer, its affiliated vendor, and the examining physician each perform one step, and each has argued in litigation that the duty rests with another. Section E below sets out what the 2016 amendments did about that distribution.

---

[6] *Id.,* at 1329-1330 (responding to the contract-counterparty framing).

[7] ERISA § 408(c)(3), 29 U.S.C. § 1108(c)(3); Langbein, *supra*, at 1325–27. Trust law "presupposes that the trustee who administers a trust will be disinterested, in the sense of having no personal stake in the trust assets."

[8] 554 U.S. 105, 108 (2008).

[9] 224 F.R.D. 169, 191 (E.D. Pa. 2004); see *id.* at 173 (Genex alleged to be a wholly owned subsidiary of Provident and UnumProvident).

[10] 489 U.S. 101, 113 (1989) (quoting 29 U.S.C. § 1002(21)(A)(i)).

The conflict reaches the claim through choices the fiduciary makes: who renders the opinion, what question is put to that person, what the person is paid, and how the answer is judged. Trust law has a vocabulary for each of those choices in the rules governing the selection, instruction, and monitoring of a delegate. ERISA practice has not applied it. The procurement of the medical opinion, therefore, falls outside the terms in which fiduciary duty is discussed and outside the record the plan compiles.

B. ERISA's standard of review

Firestone set the default: "Consistent with established principles of trust law, we hold that a denial of benefits challenged under § 1132(a)(1)(B) is to be reviewed under a de novo standard unless the benefit plan gives the administrator or fiduciary discretionary authority to determine eligibility for benefits or to construe the terms of the plan."[11] Plans drafted the discretionary clause into their documents, and deferential review became the norm.

Glenn then held that the dual role of deciding and paying is a factor to be weighed in the mix, its significance varying with the circumstances.[12] The Court then stated how the weight is set:

> "The conflict of interest at issue here, for example, should prove more important (perhaps of great importance) where circumstances suggest a higher likelihood that it affected the benefits decision, including, but not limited to, cases where an insurance company administrator has a history of biased claims administration. See Langbein, supra, at 1317–1321 (detailing such a history for one large insurer). It should prove less important (perhaps to the vanishing point) where the administrator has taken active steps to reduce potential bias and to promote accuracy, for example, by walling off claims administrators from those interested in firm finances, or by imposing management checks that penalize inaccurate decisionmaking irrespective of whom the inaccuracy benefits."[13]

The "one large insurer" whose "history of biased claims administration" the Court cited is the subject of Langbein's essay and of this article.[14]

The Court also described what reduces the conflict's weight: the administrator's "active steps to reduce potential bias and to promote accuracy."[15] The two examples it gave both act on the incentive. The first removes the decision-maker from the financial interest. The second attaches a consequence to being wrong. Both also leave a record: an organizational separation can be described and tested, and a check that penalizes inaccuracy must first measure it. The second example sets a further condition. The check must penalize error "irrespective of whom the inaccuracy benefits," so it must reach the claim wrongly paid and the claim wrongly denied on the

---

[11] *Firestone, supra,* 489 U.S. at 115 (1989).

[12] *Glenn, supra,* 554 U.S. at 108, 115–17 (2008).

[13] *Glenn, supra,* 554 U.S. at 117 (2008).

[14] *Glenn, supra,* 554 U.S. at 117, citing Langbein, *supra*, at 1317–21.

[15] *Id*.

same terms. A review function that looks only for overpayment expresses the conflict rather than curing it.

An insurer's reasonable measures fall to be assessed against that standard, and it is the standard Unum's three answers are offered to satisfy: a regulator's statements that it complied with the settlement, a record of judgments in its favor, and the quality assurance function established under the Regulatory Settlement Agreement.[16] None of the three measures accuracy in either direction.[17] Part VII takes each in turn.

Glenn also made procedural irregularity matter without making it obtainable. Procedural irregularity is Factor 3, defined in Section C below: departure, in the handling of a particular claim, from the plan's own procedures or from the ordinary requirements of a fair investigation. After *Glenn*, a claimant who can show such a departure increases the weight the conflict carries. The rules governing what a claimant may discover did not change in 2008 and have not changed since. Part VI, Section A sets out what they require.

The deferential default has narrowed over the period this article covers, because several states have banned discretionary clauses. Nothing here turns on a trend over time, and the orders described in Part VI were not selected to show one.

C. ERISA's Requirement of A Fair Investigation

ERISA's substantive investigative standard is far from toothless. Section 503 of the statute (29 U.S.C. § 1133) and its implementing regulation (29 C.F.R. § 2560.503-1) mandate a "full and fair review." This requirement imposes affirmative duties to investigate claims thoroughly, address contradictory medical evidence, and articulate reasoned decisions. Fairness is a statutory imperative; every procedural defect cataloged in Part V represents a direct breach of this core obligation.

The Four Factors Governing Expert Bias

Courts assessing whether a retained or employed expert's opinion was tainted by financial or structural bias generally rely on four categories of evidence:

---

[16] Four substantially identical Regulatory Settlement Agreements were executed on November 18, 2004, among Provident Life and Accident Insurance Company and Provident Life and Casualty Insurance Company, The Paul Revere Life Insurance Company, Unum Life Insurance Company of America, and First Unum Life Insurance Company (collectively, the "Unum Companies"), and the domestic insurance regulators of each of the Unum Companies, and the United States Department of Labor; the agreement was subscribed to by forty-eight states and the District of Columbia (collectively, the "Regulatory Settlement Agreement"). 2008 Examination Report, at 6. All fifty states, the District of Columbia and American Samoa had participated in the multistate examination; California did not subscribe to the settlement and settled separately. 2004 Examination Report, at 4; California Settlement Agreement § III.A.

[17] Regulatory Settlement Agreement, Ex. 3; *Kelly v. Provident Life & Accident Ins. Co.*, No. 1:09-cv-00070-jgm, 2010 WL 5300807, at *3 (D. Vt. Dec. 20, 2010); see Parts IV.E and VII.D.

- **Factor 1: Relational Metrics.** The financial and contractual relationship between the insurer and the expert, including total compensation, annual engagement volume, duration of the relationship, and the proportion of income derived from other payors.[18]
- **Factor 2: Reputational Metrics.** The statistical distribution of an expert's findings across claims, specifically measuring the frequency with which the expert's reports support benefit denials.[19]
- **Factor 3: Procedural Irregularities.** Demonstrable flaws, omissions, or conduct in the investigation, handling, and evaluation of a specific claim.[20]
- **Factor 4: Reasonable Safeguards.** The affirmative measures implemented by the insurer to ensure structural neutrality, objective claims handling, and expert reliability.[21]

The four are not interchangeable. Factor 1 is the only direct measure of financial dependence; the other three show whether it has operated and whether it has been checked. Factors 1 and 2 require information the insurer holds, and the claimant must extract; Part VI shows what happens when a claimant tries. Factor 3 can often be proved from the reviewer's own report and testimony, at no cost, which is why Part V treats it as the proof mode that survives.

Factor 4 is the insurer's conduct and oversight. *Glenn* does not address expert neutrality directly, but its two examples of steps that reduce a conflict's weight — separating the decision-maker from the financial interest, and attaching a consequence to being wrong — supply the standard against which an insurer's measures fall to be assessed.

---

[18] See e.g., *Demer v. IBM Corp. LTD Plan*, 835 F.3d 893, 901–02 (9th Cir. 2016) (200–300 reviews a year at $125,000–$175,000; "[t]he magnitudes of these numbers, particularly when combined, raise a fair inference that there is a financial conflict"); *Hangarter v. Provident Life & Accident Ins. Co.*, 373 F.3d 998, 1011 (9th Cir. 2004) (nineteen retentions over five years); *Velikanov v. Union Sec. Ins. Co.*, 626 F. Supp. 2d 1039, 1047, 1051 (C.D. Cal. 2009). Cf. *Cardiner v. Provident Life & Acc. Ins. Co.*, 158 F. Supp. 2d 1088, 1101 (C.D. Cal. 2001) (relational facts held insufficient standing alone; the court required evidence that the reviewers "routinely find for the insurer when faced with contrary evidence" and did not say what would supply it).

[19] See e.g., *Demer, supra,* 835 F.3d at 906 (outcome rates across claims are a crucial input; adverse inference from the insurer's failure to produce them); *Hangarter, supra,* 373 F.3d at 1011 (thirteen of thirteen total-disability claims rejected); *Chacko v. AT&T Umbrella Benefit Plan No. 3*, 690 F. Supp. 3d 1123 (E.D. Cal. 2023) (82% of 61 reviewed claimants found not disabled, at an average $353 per review, together with prior judicial criticism in three circuits).

[20] See e.g., *Demer*, 835 F.3d at 905 (paper-only review, credibility rejected without explanation, reliance on a superseded functional assessment, an unexplained substitution of reviewers on appeal); *Moody v. Liberty Life Assur. Co. of Boston*, 595 F. Supp. 2d 1090, 1096–97 (N.D. Cal. 2009) (insurer that answered one Social Security document and ignored six others acted "as an adversary, not a fiduciary"); *Montour v. Hartford Life & Accident Ins. Co.*, 588 F.3d 623, 634 (9th Cir. 2009).

[21] See e.g., *Glenn, supra*, 554 U.S. at 117 (2008); *Demer*, 835 F.3d at 903 (the insurer "could have maintained records of its reviewers' findings on claims to show their neutrality in practice, but it did not," and thereby "missed an opportunity to negate any inference of a financial conflict of interest"); *Moody*, *supra,* 595 F. Supp. 2d at 1098 (structural conflict given relatively heavy weight where no safeguard evidence was offered).

D. ERISA's Limitations on Insurance Litigation

Under ERISA there is no bad faith cause of action. State common-law tort and contract claims for improper processing of a claim under an insured plan are pre-empted.[22] There are no extracontractual compensatory or punitive damages for improper or untimely processing of benefit claims.[23] The remedy is generally the benefit due, with fees discretionary.

The expected cost of an erroneous denial is therefore constrained to the benefit. In first-party insurance, an insurer that wrongfully denies can be made to pay more than it withheld, which is the function of tort law. Under ERISA, it cannot. The worst outcome of an unsuccessful denial is that the insurer pays the benefit it owed, later, with interest and perhaps fees.

That asymmetry is the condition that makes the conduct described in this article rational. An insurer choosing how much to spend on the accuracy of a denial faces, on one side, the cost of a thorough investigation in every case, and on the other, a downside capped at the benefit in the fraction of cases where the claimant litigates and wins. Nothing in that calculation requires anyone to act in bad faith. It requires only that the calculation be made.

E. The 2016 ERISA Amendments

In 2016, the Department of Labor amended the claims regulation, and the amendments did three things that bear directly on the bias issues.

The amendments reached the selection stage for the first time. New paragraph (b)(7) requires that decisions regarding hiring, compensation, termination, promotion, or other similar matters with respect to an individual involved in making a benefit determination (a claims adjudicator or, as codified, a medical "or vocational" expert) not be made based upon the likelihood that the individual will support the denial of benefits. The preamble states that a plan cannot contract with a medical expert based on the expert's "reputation for outcomes in contested cases" rather than on the expert's professional qualifications.[24] After four decades of ERISA practice, the regulation reached the question of how the opinion-giver is chosen.

They also confirmed that the duty follows the work through the vendor. The preamble extends coverage to individuals hired or compensated by third parties engaged by the plan and requires the plan to take steps ("in the terms of its service contract and ongoing monitoring") to ensure that the service provider's practices are not based on the likelihood that the individual will support a denial.[25] The vendor layer is where per-physician dependence currently disappears.

---

[22] *Pilot Life Ins. Co. v. Dedeaux*, 481 U.S. 41 (1987).

[23] *Massachusetts Mutual Life Ins. Co. v. Russell*, 473 U.S. 134 (1985).

[24] 29 C.F.R. § 2560.503-1(b)(7); Claims Procedure for Plans Providing Disability Benefits, 81 Fed. Reg. 92,316, 92,319 (Dec. 19, 2016).

[25] 81 Fed. Reg. at 92,320. Part VI.C shows what the vendor layer does to this duty in practice. In *Leung v. Unum Life Ins. Co. of Am.*, No. 22-cv-00767-W-JLB, 2023 WL 4056041 (S.D. Cal. June 15, 2023), the discovery that succeeded addressed Unum's own payments to the vendor and stopped there: what the vendor paid the physician who wrote the

And they preserved, per claim, the material from which a reputational metric is built. The regulation requires identification of the medical and vocational experts whose advice was obtained on behalf of the plan "without regard to whether the advice was relied upon," and requires the denial notice to explain the basis for disagreeing with those views.[26] The claimant is therefore entitled, in each claim, to the name of every expert consulted, including those whose views were discarded, and to a reason for discarding them. Reputational statistics are compiled from names that recur across claims. What the Department declined to do was make the aggregate a mandatory disclosure. It did not, and could not without amending these provisions, deny the claimant the per-claim identification from which the aggregate is built.

The Department also observed that an expert's reputation for outcomes bears on whether the expert was impartially selected, and was asked by this insurer to delete that proposition. Part VII, Section F takes up that history, and what Unum said about the provision to the regulator who wrote it.

ERISA supplies a duty of full and fair review, a fiduciary duty of loyalty, a conflict weighed according to the insurer's history and its own measures, and a federal rule addressed to selection. None of those duties requires the record from which compliance could be tested. That is the condition that the remainder of this article documents, first in the regulatory settlements and then in the litigation that followed.

PART II. WHAT THE COURTS HAD FOUND BEFORE 2004

The Unum companies had institutionalized the use of biased experts. Their model was cost-efficient because it relied heavily on in-house medical professionals, and almost entirely on medical opinion (staff reviewers and independent medical examiners) rather than on the wider range of experts other insurers retain. Those reviewers relied on experiential, subjective analysis and discounted disabling conditions that the companies characterized as self-reported, such as pain, limited range of motion, and weakness.[27] The conduct was a business method. It was adopted because it worked, and the settlements did not end it.

---

report is not in Unum's records at all, and no order in the corpus reaches it. More problematic for the claimant was Unum's retention of additional experts after the administrative appeals process, without the claimant sufficiently inquiring into their potential bias. See *Leung v. Unum Life Ins. Co. of Am.*, No. 22-cv-00767-W-JLB, 2023 WL 7351581 (S.D. Cal. Nov. 6, 2023).

[26] 29 C.F.R. § 2560.503-1(h)(3)(iv); *id.* §§ (g)(1)(vii)(A)(ii), (j)(6)(i)(B).

[27] Order of the Commissioner, at 3 (finding that the companies were "[c]haracterizing certain disabling conditions as 'self-reported' (e.g., pain, limited range of motion, weakness), then accepting only objective test results to support disability resulting from these conditions even though no policy provision requires objective test results"); Cal. Dep't of Ins., Public Report of the Market Conduct Examination of the Claims Practices of the Unum Life Ins. Co. of Am., Provident Life & Accident Ins. Co., and Paul Revere Life Ins. Co., at 17 (as of June 30, 2003) (Sept. 23, 2005) [hereinafter 2005 CDI Public Report] (claims with "multiple Independent Medical Examinations or Vocational assessments

In the files the examiners reviewed, the defect was not a facial irregularity. The reviewers were credentialed, the reports were in order, and the files contained what the procedure required. The defect lay inside the opinions: they rested on subjective judgments that cannot be tested, and they were applied to conditions chosen because no objective test can disprove them. Part V describes what the litigated record later showed about the reviewers' qualifications, the accuracy of their reports, and the completeness of the files they were given.

Hangarter v. Provident Life & Accident Insurance Co. was among the first cases to directly address the industry's use of biased experts in the claims process. The claimant, a chiropractor with an own-occupation policy, suffered shoulder, elbow, and wrist injuries and could no longer treat patients. After about a year and a half of paying benefits, the insurer sent the claimant to an independent medical examination, recharacterized the occupation as business owner rather than chiropractor, and took the position that the claimant was not totally disabled because the claimant could keep books, teach a class, or see two patients an hour. The jury returned a unanimous verdict of $7,670,849, including $5 million in punitive damages. The district court denied judgment as a matter of law in November 2002, and the Ninth Circuit affirmed the verdict on June 25, 2004, five months before the multistate settlement.[28]

The evidence of the examiner's bias was specific. Paul Revere had used Dr. Aubrey Swartz nineteen times between 1995 and 2000, and "in thirteen out of thirteen cases involving claims for total disability, Dr. Swartz rejected the insured's claim that he or she was totally disabled." The letter retaining Dr. Swartz, "written by an in-house medical consultant who had never examined Hangarter, claimed that there were no objective findings for a disabling injury," and the plaintiff's claims-handling expert testified that the letter "bias[ed]" and "predispos[ed] the doctor" by "telling him [Defendants'] opinion."[29] The district court found that the defendants "chose an examiner, Dr. Swartz, with a record of finding claimants not disabled and instructed him through Dr. Bianchi in how he should find that Plaintiff's condition with conservative treatment would improve over time," and that the examiner evaluated the claimant without the claimant's own description of the work.[30] The plaintiff contended that the referral letter had been sent by GenEx, a wholly owned subsidiary of UnumProvident.[31]

The record also showed how examiners were chosen and where decisions were made. Dr. William Feist, Provident's vice-president and director of its medical department through 1996, testified to

---

indicating claimants were disabled were denied additional benefits when the Company determined that the results of its own investigations were based on the 'self-report' of the claimant").

[28] *Hangarter v. Paul Revere Life Ins. Co.*, 236 F. Supp. 2d 1069, 1082 (N.D. Cal. 2002), aff'd in part, rev'd in part sub nom. *Hangarter, supra,* 373 F.3d at 1004–05. The Ninth Circuit's summary refers to "an eleven-month period" of payments, 373 F.3d at 1003, but its own chronology runs from payments beginning in October 1997 to termination on May 21, 1999, *id.* at 1004–05, consistent with the district court's "one and one-half years," 236 F. Supp. 2d at 1082. The Ninth Circuit reversed only the injunction under the Unfair Competition Act. 373 F.3d at 1003.

[29] 373 F.3d at 1011.

[30] 236 F. Supp. 2d at 1086.

[31] *Id.* at 1104.

tactics introduced by the claims executive Ralph Mohney, among them "searching for the 'right physician to do the IME because we want to get the answer we want; we don't want to get the answer that's detrimental to our cause.'" Feist also testified that Mohney told him that, once Mohney took over the claims area, doctors "were no longer permitted to express their opinions regarding disability in the claims file." Mohney introduced round table claims reviews and a "net termination ratio" goal that rose to 104 percent by 1997, and the plaintiff's claims-handling expert testified that the round table proceedings "were not documented in the claims files." The claimant's own file went to a round table on September 9, 1997, four weeks after the claim form arrived.[32]

On the law, the Ninth Circuit held that a jury's finding that an insurer's investigation was biased "may preclude a finding that the insurer was engaged in a genuine dispute, even if the insurer advances expert opinions concerning its conduct." It then listed five "factors" through which "[a]n insurer's bias may be shown": the insurer misrepresented the nature of the investigatory proceedings; its employees lied in depositions or to the insured; it dishonestly selected its experts; its experts were unreasonable; or it failed to conduct a thorough investigation.[33] The list came from *Chateau Chamberay Homeowners Ass'n v. Associated International Insurance Co.*, which had drawn it from *Guebara v. Allstate* as "circumstances where a biased investigation claim should go to jury," added that the list was "not intended to be exhaustive," and warned that an insurer may not "insulate itself from liability for bad faith conduct by the simple expedient of hiring an expert for the purpose of manufacturing a 'genuine dispute.'"[34] Each circumstance describes the insurer's conduct. None is a test of expert bias, and none is a factor evidencing it.

Despite exposing the examiner's pattern of findings for the insurer, neither opinion addressed the business relationship among Dr. Swartz, the insurer, its representatives, and the industry. Neither addressed the role of an affiliated vendor in making the referral nor the insurer's failure to disclose the examiner's conflict, which alone may be unreasonable and give rise to a bad-faith claim. Neither addressed how Dr. Swartz was selected. By focusing on the insurer's bias and its bad-faith conduct, the courts failed to fully explore the underlying issue: the expert's bias and the measures the insurer takes to address it.

Hangarter was one of several decisions available to the regulators before the multistate report issued on November 18, 2004.[35] They did not all point the same way.

---

[32] *Id.* at 1084–86; 373 F.3d at 1011, 1018. The district court described Mohney's goal as raising the ratio to 84 percent, then 90 percent by 1996 and 104 percent by 1997. 236 F. Supp. 2d at 1085.

[33] 373 F.3d at 1010.

[34] *Chateau Chamberay Homeowners Ass'n v. Associated Int'l Ins. Co.*, 90 Cal. App. 4th 335, 348–49 & n.8 (2001) (citing *Guebara v. Allstate Ins. Co.*, 237 F.3d 987, 996 (9th Cir. 2001)).

[35] Earlier decisions pointed the same way. In *Shapiro v. Paul Revere Life Ins. Co.*, No. C-96-1758-FMS (JL), 1997 WL 601430, at *4 (N.D. Cal. Sept. 18, 1997), the court held discoverable the allegation that the insurer "routinely removes or does not include any information in the claims file which is negative to Defendant's position," evidenced by documents marked "Not For File," and observed that the practice, if proven, would circumvent the claim-file requirements of Cal. Code Regs. tit. 10, § 2695.3. Ten days before the Ninth Circuit decided *Hangarter*, the court in

- *Cardiner v. Provident Life & Accident Insurance Co.* (C.D. Cal. 2001). The insured showed that one evaluator had testified 20 to 25 times since 1990, always for an insurance company or its lawyer, and never for an insured, and that the other had been paid by Provident eighteen times in 1997 through 1999 to examine Provident insureds. The court held the showing insufficient: "The mere fact that these doctors have been hired by insurers rather than insureds does not support bias. . . . Significantly, Plaintiff offers no evidence that these doctors routinely find for the insurer when faced with contrary evidence."[36]
- *Waggener v. Unum Life Insurance Co. of America* (S.D. Cal. 2002). Over Unum's motion for a protective order, the court ordered answers to an interrogatory asking, for each independent contractor who evaluated the claim, "the number of times [Unum has] employed that person to participate in evaluating or handling a claim . . . [and] the total amount of compensation paid on each occasion." It also ordered the production of the requested documents on the "general selection of physicians for Independent Medical Examinations," without the limits it imposed on three of the plaintiff's other document requests.[37]
- *Saldi v. Paul Revere Life Insurance Co.* (E.D. Pa., August 13, 2004). Compelling discovery into the insurers' claims policies, the court summarized the *Hangarter* trial record: "Paul Revere exhibited bias by selecting a biased independent medical examiner, by not providing the examiner with the plaintiff's description of her work, by discussing the plaintiff's claim in roundtable groups with the purpose of brainstorming how to terminate the claim, and by not including notes of the roundtable discussions in the plaintiff's claim file." The termination in *Saldi* rested on an investigation by Genex Services, Inc., which the plaintiff alleged was "a wholly owned subsidiary of Provident and UnumProvident."[38]

The 2004 examination report cites none of these decisions. California's settlement, by contrast, recites that the Department "surveyed recent court cases, interviewed certain individuals, [and] reviewed evidence and testimony in civil cases."[39]

Radford Trust v. First Unum Life Ins. Co. of Am., 321 F. Supp. 2d 226, 247–48 (D. Mass. 2004), wrote that "an examination of cases involving First Unum and Unum Life Insurance Company of America . . . reveals a disturbing pattern of erroneous and arbitrary benefits denials, bad faith contract misinterpretations, and other unscrupulous tactics."

[36] *Cardiner, supra,* 158 F. Supp. 2d at 1101. The court did not say what evidence would have satisfied it.

[37] *Waggener v. Unum Life Ins. Co. of Am.*, 238 F. Supp. 2d 1179, 1181, 1187–88 (S.D. Cal. 2002). The court described the interrogatory as "identifying the extent to which physicians or other independent contractors who participated in evaluating Waggener's claim have previously participated in claim handling for Unum," and ordered production on Request No. 4 "regarding selection of Independent Medical Examiners," while limiting Request Nos. 3, 5, and 8. *Id.* at 1187–88.

[38] *Saldi, supra,* 224 F.R.D. at 173, 179 (E.D. Pa. 2004).

[39] California Settlement Agreement § I.B (Oct. 3, 2005).

PART III. THE EXAMINATIONS AND THE SETTLEMENTS

A. The Examination Findings

The multistate examiners reviewed 299 randomly selected claim files, then 75 more after the companies represented that their practices had changed. They reported four "general areas of concern," applicable to individual and group business alike, with "no material differences in claim handling among the individual companies or among their claim offices": excessive reliance upon in-house medical professionals; unfair construction of attending physician or IME reports; failure to evaluate the totality of the claimant's medical condition; and an inappropriate burden placed on claimants to justify eligibility for benefits.[40] The examination closed by settlement, and the regulators' summary acknowledged that "no specific 'findings' were reached."[41]

The first two areas concern medical opinion. The examiners identified "numerous instances" in which the companies relied heavily on in-house professionals who "do not examine or otherwise interact with claimants directly" and "refrained from securing an IME," and "many such instances" in which the companies "discounted or disputed the opinions of claimants' attending physicians, but chose not to invoke the requirement that the claimant attend an IME." They inferred that the companies' "excessive reliance upon in-house medical professionals also suggests the Companies' employment of such professionals often resulted in a Company bias and the inappropriate interpretation or construction of medical reports, to the detriment of claimants," including IME reports that were "narrowly or even incorrectly construed."[42] The other two areas address the handling of co-morbid conditions and denials for want of "objective evidence" when "[t]he Companies' policy forms do not require the claimant to provide such evidence."[43]

---

[40] 2004 Examination Report, at 4–7. The Report offered the following on Unum's use of biased experts: "The Companies' excessive reliance upon inhouse medical professionals also suggests the Companies' employment of such professionals often resulted in a Company bias and the inappropriate interpretation or construction of medical reports, to the detriment of claimants. In certain instances, this bias was reflected in the interpretation of attending physicians' statements or medical records supplied by attending physicians. In other instances in which the Companies had obtained an [independent medical examination (IME)], the reports supplied by the IME providers were narrowly or even incorrectly construed. The bias of the in-house medical professionals was also reflected in attempts to focus upon any apparent inconsistencies in the medical records or other information supplied by claimants, rather than attempt to derive a thorough understanding of the claimant's medical condition." See Conduct Report, "Areas of Concern", item 2. As a remedial measure, Unum was required to select third-party professionals solely on the basis of objective, professional criteria. Unum and the third-party professional must also execute a "Statement of Professional Conduct", whereby Unum commits to "[m]ake appropriate decisions by providing a thorough, fair and objective evaluation of all claims", and the third-party professional commits to "provide fair and reasonable evaluations." See Exhibit 5 to Regulatory Settlement Agreements. Unum was also required to change their Guidelines on IMEs. See Exhibit 6 to Regulatory Settlement Agreements.

[41] Settlement FAQ, at 1; see 2004 Examination Report, at 8.

[42] 2004 Examination Report, at 6.

[43] *Id.* at 6–7.

California's proceeding was different in kind. The Department issued an Accusation. The companies denied its allegations but acknowledged that certain of them, "if heard and proved, could constitute grounds for the Insurance Commissioner to suspend Respondents' certificates of authority and licenses," and waived hearing.[44] The Commissioner then found, "without Respondents having had the opportunity to defend at a hearing," that the companies had "in certain instances" engaged in twenty-eight enumerated acts or practices in violation of sections 700 and 704 of the Insurance Code, and ordered that they are "prohibited from engaging in the conduct set forth in the Findings enumerated above."[45] The investigation behind the Order reached beyond claim files. The Department also "surveyed recent court cases, interviewed certain individuals, reviewed evidence and testimony in civil cases," and requested a list of claims in which an independent medical examination had been obtained, which ran to 803 claim files.[46]

Six of the findings concern the production and use of medical opinion:[47]

1. Selectively using independent medical examinations (IMEs) to Respondents' own advantage;
2. Selectively using portions of medical records and IME findings to Respondents' own advantage;
3. Overruling the opinion of the attending physician after Respondents' in-house medical personnel have conducted a "paper review" of the medical file;
4. Overruling the opinion of in-house medical personnel who supported a finding of disability or the need for specific objective testing;
5. Failing to request that the IME perform objective testing that could support a finding of disability resulting from a "self-reported condition," or ignoring objective test results from the IME that do support a finding of disability;
6. Discounting objective test results by imputing the physiologically disabling condition to a "psychological component," thus triggering the "mental or nervous condition" limitation.

Two more concerns were where and why decisions were made. The companies failed "to document claim files adequately regarding the so-called 'roundtable' sessions at which substantive claims decisions were made," and they targeted claims "for 'resolution' (i.e., denial or termination of benefits) in the interest of improving 'net termination ratios' . . . for reasons other than the merits of individual claims or fair, thorough, objective investigations into those claims," chiefly claims under high-benefit, noncancellable disability income policies.[48] The companies told the Department that they began recording the participants in and outcome of roundtable reviews in 2003, and the

[44] California Settlement Agreement §§ I.C, I.F–I.I.

[45] Order of the Commissioner, at 2–5.

[46] California Settlement Agreement § I.B; 2005 CDI Public Report, at 4, 6–7.

[47] Order of the Commissioner, at 2–3.

[48] *Id.* at 3–4.

rationale for roundtable decisions in 2004.[49] The remaining findings concern the definition of disability, occupational analysis, policy provisions, and communications with claimants.[50]

The remedies tracked the diagnoses. The multistate Plan of Corrective Action provided for the reassessment program, changes in corporate governance, quarterly meetings with the lead regulators and the Department of Labor, the $15 million penalty with a contingent $145 million fine tied to the 7 percent error-rate tolerance, a full re-examination within twenty-four months, and changes in claim procedures that included "[i]ncreased utilization of IME's."[51] California's settlement added an Independent Review process for reassessed claims, discontinued the self-reported-conditions limitation in California contracts, and imposed the $8 million penalty and the Order.[52] Part IV addresses what those instruments required.

B. What the Findings Omitted

The multistate report uses the term "bias" to refer to one group: the companies' in-house medical professionals. The examiners knew that a second group existed. The passage diagnosing excessive reliance on in-house staff notes that "[t]he Companies also use the services of medical professionals who are independent contractors," and that the policies allow the companies to require an examination "conducted by a physician of the Companies' choice."[53] Outside examiners then appear in the report only as the corrective measures the companies failed to use, or as authors of reports that in-house staff misread. The report emphasized the companies' use of biased in-house professionals and failed to address their equally troubling use of biased third-party medical examiners.

---

[49] 2005 CDI Public Report, at 20.

[50] Order of the Commissioner, at 2–5. The findings include knowingly applying a definition of disability inconsistent with California case law; mischaracterizing the claimant's occupation or its duties; treating nonsedentary nursing occupations as sedentary during the own-occupation period; determining "predominantly through an analysis of billing records" that medical specialists could perform their own occupations; misapplying partial and residual disability provisions; inappropriate surveillance; using the twenty-four-month mental and nervous limitation to curtail physiologically based disabilities; pre-existing-condition language and its misapplication; offsetting estimated Social Security benefits; misstating a duty to apply for Social Security benefits; failing to refer claimants to the Department; "[c]ontinuing to seek additional information where claimants have provided adequate proof of disability, thus unfairly shifting the burden of investigation to the claimant"; communications suggesting that ERISA governed non-ERISA policies; extended payment under a reservation of rights followed by termination and a demand for repayment; failing to disclose additional benefits; and "[c]ompelling a claimant to accept an unreasonably low settlement offer through the above means and others, or resort to litigation." *Id.* On the ERISA finding, the Department reviewed documents "indicating that the Company was aware that claims believed to be covered under ERISA (Employee Retirement Income Security Act) may not be subject to 'bad faith' claims in excess of the actual benefits provided in the policy," and identified eight non-ERISA claims whose denial letters referred to ERISA. 2005 CDI Public Report, at 20. The termination letter in *Hangarter* made the same misstatement. 373 F.3d at 1011.

[51] 2004 Examination Report, at 8–10; Settlement FAQ, at 3–4.

[52] California Settlement Agreement §§ III.C, IV.C; Order of the Commissioner, at 5.

[53] 2004 Examination Report, at 6.

The litigated record pointed the other way. The examiners whose conduct the courts had described were outside retainers rather than employees: Dr. Swartz in *Hangarter*, whose conduct the court described; the evaluators in *Cardiner*, whose engagement histories the insured put in evidence; and the contractors in *Waggener*, whose engagement counts and compensation the court had ordered Unum to state. The report mentions none of it. For excessive reliance on in-house opinion, the Plan of Corrective Action prescribed more outside opinion, "[i]ncreased utilization of IME's," with the examiners still chosen by the companies.[54] Dr. Swartz was not an employee.

Measured against the four factors set out in Part I, the findings addressed only one. Factor 3, procedural irregularity, is where both examinations did their work: attending physicians discounted without an examination, reports construed against claimants, co-morbid conditions assessed one at a time, objective evidence demanded that the policies did not require, and, in California, examinations used selectively and favorable opinions overruled. Factor 1, the relational metrics, was not examined. No finding addresses what any examiner was paid, how many engagements any examiner received, how long any relationship had run, or the use of an affiliated vendor to arrange examinations. Factor 2, the reputational metrics, was not examined. No finding reports how any examiner's opinions came out across engagements, although that pattern was the evidence *Hangarter* accepted. Factor 4, the insurer's measures to ensure the neutrality of the experts it retained, was not examined either. No finding describes how the companies selected examiners, whether they evaluated examiners at all, or on what criteria.

The multistate examination was not designed to produce those findings. Its samples were drawn by company, line of business, claim category (litigated, pending, closed, and appealed), and the claimant's state of residence, and none was drawn by reviewer or examiner.[55] A claim-by-claim review of randomly selected files does not assemble any examiner's engagement history. The report names no examiner, physician, or claim office, gives no count for any finding, and states its findings in adverbs: "numerous instances," "many such instances," "certain instances," "a significant number of instances," "some instances."[56] The 2008 re-examination drew its samples the same way, by reassessment unit, operations unit, and line of business.[57]

California came closer. The Department asked for the list of claims in which an independent medical examination had been obtained and found that the companies were "[s]electively using independent medical examinations (IMEs) to Respondents' own advantage."[58] The Department had also told itself what was in the litigated record. Its settlement recites that it "surveyed recent court cases, interviewed certain individuals, [and] reviewed evidence and testimony in civil cases." The Ninth Circuit affirmed *Hangarter* on June 25, 2004; the Order issued in October 2005. The record

---

[54] *Id.* at 9; 236 F. Supp. 2d at 1085; 373 F.3d at 1011, 1018; *Cardiner*, 158 F. Supp. 2d at 1101; *Waggener*, 238 F. Supp. 2d at 1181, 1187–88.

[55] 2004 Examination Report, at 5, Exs. A–C.

[56] *Id.* at 6–7.

[57] 2008 Examination Report, at 8–9.

[58] Order of the Commissioner, at 2; 2005 CDI Public Report, at 6–7.

the Department says it reviewed contained the thirteen-of-thirteen finding, the referral letter that supplied the conclusion, and the testimony about searching for the right physician.

The selective-use finding does not say which selection it means: the decision whether to order an examination, the choice of examiner, or the use made of the report. The public report behind the Order describes the companies' consultants as "medical consultants paid by the insurer" and faults the companies for disregarding the advice of "their own medical consultants or physicians paid to perform Independent Medical Examinations" in seven claims.[59] That report never uses the word "bias." It identifies no examiner, reports nothing about how often any examiner was used or how any examiner's opinions came out, and makes no finding about referral letters, compensation, or the vendors through which examinations were arranged.

The overruling finding shows what medical opinion was doing in these decisions. The companies overruled in-house personnel "who supported a finding of disability or the need for specific objective testing," overruled attending physicians after in-house "paper review[s]," and ignored objective test results from their own examiners "that do support a finding of disability."[60] If the medical opinion were driving the decision, adverse in-house opinions would have driven it too. They did not. The opinion was retained where it supported denial and set aside where it did not. A remedy that reduces reliance on in-house opinion or adds an outside one does not address a decision-making process that selects among available opinions after the fact.

The roundtable and targeting findings place the operative decision outside the claim file. California found that substantive decisions were made in roundtable sessions the files did not adequately document, and the *Hangarter* record added a termination-ratio goal and a policy barring company doctors from recording disability opinions in the file.[61] Each practice kept the decisive reasoning out of the files the examiners reviewed. The multistate report mentions neither roundtables nor termination targets.

The later examinations kept the same frame. California's 2008 follow-up, discussing "the appropriate use of Independent Medical Examinations, Functional Capacity Examinations, and Medical Records Reviews," reported the companies' statement that their combined number of independent medical examinations, functional capacity examinations, and medical record reviews "has increased significantly from 2003 to 2006."[62] The report records the count. It does not address who performed the examinations, how those examiners were chosen, what they were paid, or what their opinions were.

---

[59] 2005 CDI Public Report, at 17.

[60] Order of the Commissioner, at 2–3; see 2005 CDI Public Report, at 17 (files in which "the medical consultants indicated disabling conditions but the Companies denied the claims," and files in which the consultants "indicated the need for specific objective testing . . . but the tests were not performed prior to discontinuing benefits").

[61] Order of the Commissioner, at 4; 236 F. Supp. 2d at 1085.

[62] 2008 CDI Follow-Up Report, at 6–7.

C. The Reassessment Figures

In the early 2000s, the then-largest American provider of disability insurance was exposed for institutional bad faith claims practices and the unlawful denial of long-term disability claims reaching back to at least the mid-1990s.[63] Court decisions exposed the practices, two nationally broadcast investigative programs and a run of newspaper stories followed, and the United States Department of Labor joined state insurance regulators in the action that resolved them.[64]

The resolution is usually summarized in a handful of figures. A Regulatory Settlement Agreement subscribed to by forty-eight states and the District of Columbia. A $15 million penalty under that agreement and an $8 million penalty under California's separate settlement. A reassessment program offered to approximately 200,000 claimants. A reversal rate of 41.7 percent. And approximately $676.2 million in additional benefits "either paid immediately or reserved for future payments."[65] Commentary has carried those figures forward as proof that the regulatory response worked. One article described strict oversight by state insurance departments as the approach "which has proved to be most successful in the Unum Provident case," reported, on the strength of the 2008 examination, that the companies were "in complete compliance with the [Regulatory Settlement Agreement]," and estimated that "it appears the companies paid more than a billion dollars in benefits due to the reassessed claims."[66]

---

[63] See Langbein, supra, at 1317–21; Report of the Targeted Multistate Market Conduct Examination of Unum Life Ins. Co. of Am., The Paul Revere Life Ins. Co., and Provident Life & Accident Ins. Co., at 5 (Nov. 18, 2004) [hereinafter 2004 Examination Report] (reporting that the companies and their New York affiliate ranked first in market share in both individual and group long-term disability insurance).

[64] *Radford Trust, supra,* 321 F. Supp. 2d at 247–49 (referring to the "60 Minutes" and "Dateline" segments and to press coverage); 2004 Examination Report, at 8 (settlement to be entered into with the lead state regulators "and the United States Department of Labor").

[65] Report of the Multistate Market Conduct Examination of Unum Life Ins. Co. of Am. et al., at 4, 6–7 (as of Dec. 31, 2007) (Apr. 14, 2008) [hereinafter 2008 Examination Report]; 2004 Examination Report, at 8 ($15,000,000 penalty; notice to eligible claimants "representing approximately 200,000 claims"); Decision and Order of Insurance Commissioner upon Settlement, at 5, Cal. Settlement Agreement Ex. A (Oct. 2005) [hereinafter Order of the Commissioner] ($8,000,000 civil penalty). The regulators' settlement summary put the notice population at "[a]pproximately 215,000 claimants." Information About the UnumProvident Settlement Concerning Disability Income Claim Handling Practices, at 2 [hereinafter Settlement FAQ].

[66] Jillian Redding, ERISA: Remedies, Preemption and the Need for More State Regulatory Oversight, 18 Conn. Ins. L.J. 169, 169, 215 (2011).

The 41.7 percent is a share of the claims that were reassessed. The regulators' 2008 report gives the sequence that produced the reassessed population:[67]

Table 1. The reassessment program, from notice to reversal

Multistate reassessment population, as reported by the regulators in 2008

STAGE	CLAIMANTS	SHARE OF PRIOR STAGE	SHARE OF THOSE NOTICED
Notices mailed to eligible claimants	290,903	—	100.0%
Elected to participate	78,422	27.0%	27.0%
Requested participation without a notice	974	—	—
Total requesting reassessment	79,396	—	27.3%
Filed the Reassessment Information Form and were reassessed	**23,190**	**29.2%**	**8.0%**
Reversed in whole or in part	**9,672**	**41.7%**	**3.3%**

Note. The 41.7 percent reversal rate is a share of the 23,190 claims reassessed, not of the 290,903 claimants noticed. Of those noticed, fewer than 8 percent were reviewed and about 3 percent had a denial reversed in whole or in part. Of the 79,396 claimants who asked for reassessment, 56,206 — 71 percent — were never reassessed. The 974 claimants who requested participation without a notice fall outside the noticed population, and are excluded from the percentages in the final column.

Of the 290,903 claimants informed that their claims might be reviewed, 23,190 were reviewed, fewer than 8 percent. Of those 290,903, 9,672, about 3 percent, had a denial reversed in whole or in part. The reports say nothing about the other 267,713. The figure of 200,000 usually attached to the settlement was the regulators' 2004 estimate of the number of people who would receive notice. It was never a count of claims reopened.[68]

The largest attrition occurred after claimants requested a review. Of the 79,396 who asked, 56,206, or 71 percent, were never reassessed. The 2008 report records the drop without explanation, and one commentator observed that "[i]t is unclear why only 29% of the claimants correctly filed the Reassessment Forms."[69] The procedure the settlement prescribed supplies part of the answer. A claimant had sixty days to elect to participate and, once the Claim Reassessment Unit scheduled the review, another sixty days to return a Reassessment Information Form "in order to be considered by the CRU."[70] Claimants whose claims had been closed on a return to work received a

[67] 2008 Examination Report, at 6–7. The report states the opt-in rates by line of business (29 percent of noticed group claimants and 21.7 percent of noticed individual claimants) and the completion rate for all requesting claimants (29.2 percent). The other aggregate shares in the table are computed from the reported counts.

[68] Compare 2004 Examination Report, at 8, and Settlement FAQ, at 2, with 2008 Examination Report, at 6.

[69] 2008 Examination Report, at 6; Redding, supra, at 214 n.278.

[70] Regulatory Settlement Agreement, Ex. 1, §§ II.2, II.4 (Nov. 18, 2004) [hereinafter Regulatory Settlement Agreement]. Exhibit 1 permits an extension only where the claimant "requests in writing an extension and explains why such an extension is needed." *Id.* § II.4.

separate notice, and Unum told its shareholders that almost half of the eligible pool was "subject to a preliminary determination as to whether the claimant seeking reassessment 'returned to work' under the policy, in which case the claim is not eligible for further reassessment."[71] A claimant who elected to participate also "conditionally agree[d] to forego the pursuit of a legal action."[72] In 2004, the same examiners had identified an "[i]nappropriate burden placed on claimants to justify eligibility for benefits," a practice "particularly of concern for claimants whose medical conditions may be interfering with their ability to interact with the Companies' staff in the handling of their claims."[73] The remedy required that population to meet two paperwork deadlines.

The data needed to explain the attrition existed. The settlement required the companies to record, for each claimant, the date the Reassessment Information Form was sent and the date a completed form was received, together with the outcome of each reassessment, and to keep records from which the results "may be tracked on a state-by-state basis as well as on a group basis."[74] Neither examination report uses those records to account for the claimants who dropped out.

California's reassessment followed the same course. Unum mailed 33,566 notices to California claimants; 11,098 asked for reassessment; 2,654 returned the form and were reassessed; and 1,155 received additional benefits. Fewer than 8 percent of the claimants noticed were reviewed, about 3 percent were paid, and 8,444 claimants who asked for review did not receive one. Of the 298 reassessed claimants who used the Independent Review process that California added, the reviewer agreed with Unum in 278.[75]

Stated as a share of reassessed claims, the reversal rate suggests that nearly half of Unum's decisions were corrected. Stated against the population the program was built to address, it describes a review for eight claimants in every hundred and a reversal for three. The report does not separate full reversals from partial ones, and the $676.2 million combines benefits paid with *reserves set aside for future payments*.[76] The headline figure states what was paid or reserved for the 23,190 claims that were reassessed. It says nothing about the 267,713 claims that were not.

---

[71] Regulatory Settlement Agreement § B.2.b & Ex. 1, Attach. A-2; UnumProvident Corp., Annual Report (Form 10-K), at 27 (Mar. 14, 2005). Unum put the eligible pool at "approximately 215,000 claims." *Id.*

[72] Regulatory Settlement Agreement § B.2.b; see Settlement FAQ, at 3.

[73] 2004 Examination Report, at 7.

[74] Regulatory Settlement Agreement § B.2.b & Ex. 1, § III.6.

[75] Cal. Dep't of Ins., Report of the Market Conduct Examination of the Claims Practices of Unum Life Ins. Co. of Am., Provident Life & Accident Ins. Co., and The Paul Revere Life Ins. Co., at 7 (as of July 31, 2007) (adopted Mar. 28, 2008) [hereinafter 2008 CDI Follow-Up Report]. Of the 2,654 reassessed claims, 1,376 denials were upheld, 123 were left unchanged because the form was incomplete, 611 were reopened with an additional payment, and 544 were reopened with continuing payments. *Id.* The Department reported $112,046,062 paid or reserved for California claimants. *Id.*

[76] 2008 Examination Report, at 6–7 (reporting reversals "in whole or in part" and benefits "either paid immediately or reserved for future payments").

PART IV. THE REGULATORY REMEDY THAT CONCEALED THE BIASED EXPERT PRACTICE

The settlement prohibited the selection of examiners by reference to their results, and designated compliance with that prohibition as a subject for examination. It then adopted a compliance test that could not reach it, required no record from which it could be reached, and made the untestable prohibition permanent. The regulators retained access to every claim file and every internal communication in it, at all times, and never compiled a single examiner's history. This Part sets out what the remedy required, what it required to be recorded, and what those two things together made it possible to see.

A. The Regulators Recognized the Foundational Problem

The regulators saw bias. The multistate examiners wrote that the companies' reliance on in-house professionals "suggests the Companies' employment of such professionals often resulted in a Company bias and the inappropriate interpretation or construction of medical reports."[77] California found that the companies were "[s]electively using independent medical examinations (IMEs) to Respondents' own advantage."[78] The Regulatory Settlement Agreement directs examiners to look in claim files for "[a]ctions suggesting a pre-disposition or bias against the claimant," forbids "any attempt to influence the impairment determinations of professionals conducting the IME," and requires the companies to select examiners "without regard to results of previous IMEs or FCEs conducted by such individuals."[79] California required that the reviewers in its own Independent Review process be people who, to the Director's knowledge, "have no bias toward either claimants or insurers."[80]

By 2004, the courts had also identified the evidence from which an examiner's bias is shown. Those are the four factors set out in Part I: the financial relationship between insurer and examiner, the examiner's record of outcomes, procedural irregularities in the evaluation, and the insurer's measures to keep its examiners neutral. The decisions described in Part II applied them to these companies.

California also knew what a disclosure remedy addressed to a decision-maker's neutrality looks like, because it wrote one into its own settlement for the one reviewer the Department appointed itself; Section G sets it out. Neither instrument required a record of any of the four from the examiners the companies hired.

B. Factor 1: Relational Metrics (Compensation and Claim Assignments)

The courts had the relationship in front of them. Paul Revere used Dr. Swartz nineteen times between 1995 and 2000, and the plaintiff contended that the referral came through

---

[77] 2004 Examination Report, at 6.

[78] Order of the Commissioner, at 2.

[79] Regulatory Settlement Agreement §§ B.3.c(i), B.3.d, B.3.i; see id. Ex. 6, §§ C.1, C.2.

[80] California Settlement Agreement Ex. B, ¶ 2.c.

UnumProvident's subsidiary GenEx.[81] In *Cardiner*, one of the evaluators had been paid by Provident eighteen times in 1997 through 1999 to examine Provident insureds.[82] In *Waggener*, the court ordered Unum to answer an interrogatory asking how many times it had used each contractor who evaluated the claim and "the total amount of compensation paid on each occasion."[83]

In *Saldi*, the court allowed discovery of Paul Revere's relationship with Genex Services, which the insured alleged was a wholly owned subsidiary of Provident and UnumProvident. The order reached the companies' agreements with Genex, their standards and expectations for it, the claim savings attributed to its work, every investigation performed for the companies by the Genex personnel who handled the claim, and those personnel's payroll records.[84] The insured contended that those investigations "almost always resulted in the termination of claims."

Neither settlement mentions compensation, volume, duration, exclusivity, or the vendors through which examinations are arranged. Nothing in either requires the companies to record what an examiner was paid or how often the examiner was used, and no examination report gives either figure.[85] California required anyone considered to direct its Independent Review process to "disclose any financial interests or business relationships likely to affect impartiality or that might create an appearance of partiality."[86] It asked nothing comparable about the examiners the companies hired.

C. Factor 2: Reputational Metrics (Patterns and Practices)

Dr. Swartz had rejected total disability in thirteen of thirteen claims, and the district court found that the defendants "chose an examiner, Dr. Swartz, with a record of finding claimants not disabled."[87]

Courts had also begun ordering the records from which an examiner's history is built. In *Small*, decided in 1999, the insured alleged that Provident obtained an unreliable examination report from a physician reputed to be a "medical mercenary," and subpoenaed the examiner's records of forensic examinations. The court held that "the existence of a pro-insurance bias on the part of Dr. Bromberg is germane" to the bad faith claim. It found that reports prepared to determine eligibility for insurance benefits carry "a somewhat reduced expectation of privacy." It limited the subpoena, which sought the examiner's medical records, billing records, reports, and scheduling books, to examinations performed for insurance companies since 1990, and ordered the medical records

---

[81] *Hangarter, supra*, 373 F.3d at 1011; *Hangarter, supra,* 236 F. Supp. 2d at 1104.

[82] *Cardiner, supra*, 158 F. Supp. 2d at 1101.

[83] *Waggener, supra,* 238 F. Supp. 2d at 1181, 1187–88.

[84] *Saldi, supra,* 224 F.R.D. at 173, 190–92 (E.D. Pa. 2004).

[85] The claim-file provision defines what must be kept ("all documents relating to a claim history and/or decision"), not what must be created, and the reassessment unit's tracking duties run to notice dates, form dates, decision dates, and outcomes, not to the examiner used. Regulatory Settlement Agreement § B.3.l & Ex. 1, § III.6.

[86] California Settlement Agreement Ex. B, ¶ 2.a.

[87] *Hangarter, supra,* 236 F. Supp. 2d at 1084, 1086; *Hangarter, supra,* 373 F.3d at 1011.

redacted so that they "contain only the name of the insurance company for whom the record was prepared, Dr. Bromberg's analysis, and the recommendation made."[88]

The settlement addresses the examiner's record in one clause: examiners are to be selected "without regard to results of previous IMEs or FCEs."[89] The drafters thought the clause important enough to outlive the agreement: section B.3.d is one of the provisions that survives termination. No finding supports the rule, because neither examination examined how examiners were chosen nor drew its sample by examiner.[90] Nor does the settlement require anyone to record an examiner's results. A claim file shows one examination. Whether that examiner was chosen with regard to earlier results depends on all of the examiner's results, and the thirteen-of-thirteen record in *Hangarter* came from litigation, not from a file. In 2010, Unum's designee in *Kelly* testified that the companies had "no formal rating or evaluation system" for examiners, and the court left the claimant to "decipher the 'outcomes'" from the examiners' prior reports.[91] A company that keeps no record of its examiners' conclusions cannot be shown to have considered them when choosing examiners.

California wrote a rule allowing removal of an independent reviewer who "engaged in a pattern or practice" of unfair review.[92] It wrote no such rule for the companies' examiners.

D. Factor 3: Procedural Irregularities in the Expert's Investigation and Opinions

Procedural irregularity is the factor the examinations reached. The regulators found reports construed against claimants, attending physicians discounted without an examination, examinations used selectively, and favorable opinions overruled. The settlements addressed several of those findings with rules that have triggers and leave a mark in the file, and courts have enforced them.[93]

---

[88] *Small v. Provident Life & Accident Ins. Co.*, No. 2:98-cv-02934, 1999 WL 1128945, at *1–4 (E.D. Pa. Dec. 8, 1999) (bad faith claim under 42 Pa. Cons. Stat. § 8371).

[89] Regulatory Settlement Agreement § B.3.d; see id. Ex. 6, § C.1 ("without regard to results of previous IME's conducted by such individuals"). *Id*. § C.10(i) (listing § B.3.d among the provisions that survive termination).

[90] See Part III.B; 2004 Examination Report, at 5, Exs. A–C; 2008 Examination Report, at 9.

[91] *Kelly v. Provident Life & Accident Ins. Co.*, No. 1:09-CV-70, 2010 WL 3259997, at *2–3 (D. Vt. Aug. 17, 2010).

[92] California Settlement Agreement Ex. B, ¶ 2.k.

[93] See Part III.A–B. The trigger rules include the attending-physician and IME-request provisions added nationally in October 2005, Amendment to Regulatory Settlement Agreement ¶¶ 4, 5 (Oct. 3, 2005), and the Social Security and co-morbidity provisions, Regulatory Settlement Agreement §§ B.2.b, B.3.g. For enforcement, see *Chronister v. Unum Life Ins. Co. of Am.*, 563 F.3d 773, 776–77 & n.3 (8th Cir. 2009) (Social Security award; procedures "put in place pursuant to settlement agreements and consent decrees"); *Freeland v. Unum Life Ins. Co. of Am.*, No. 11-cv-053-wmc, 2013 WL 4482995, at *12 (W.D. Wis. Aug. 19, 2013) (separate review of physical and psychological conditions "violated the Regulatory Settlement Agreement," though harmless); *Moseley v. Unum Life Ins. Co. of Am.*, 659 F. Supp. 3d 89, 90–92 (D. Mass. 2023) (refusal of a requested IME; Regulatory Settlement Agreement Ex. 6, § B.4). None of the decisions examined here enforces Regulatory Settlement Agreement § B.3.d.

The irregularities that run through the examiner were treated differently. In *Hangarter*, the referral letter, written by an in-house consultant who had never examined the claimant, asserted that there were no objective findings for a disabling injury, and the examiner worked without the claimant's own description of the work.[94] The settlement forbids attempts to influence an examiner and requires that evaluators receive all available evidence.[95] It does not require anyone to review the contents of a referral, and no examination report mentions referral letters.

The central guideline also lets the examination be skipped. Where in-house opinion is the primary basis for a denial, an examination "should be sought," unless the Chief Medical Officer or a designee reviews the file and finds "reasonable medical certainty supporting the position of the Company's medical professionals involved in the claim file and in disagreement with the AP."[96] A senior in-house paper review may take the place of the examination. California's Order prohibits "[o]verruling the opinion of the attending physician after Respondents' in-house medical personnel have conducted a 'paper review' of the medical file."[97]

E. Factor 4: The Insurer's Reasonable Measures to Ensure a Fair Claims Process

Provident's former medical director testified to "searching for the 'right physician to do the IME because we want to get the answer we want.'" *Waggener* ordered production of Unum's documents on the general selection of physicians for examinations (Part II).[98]

The settlement requires selection "solely on the basis of objective, professional criteria." It never states the criteria or requires that they be written down.[99] Its other measures are directed at employees: a conduct statement that only employed professionals must sign, and a Quality Compliance Consultant responsible for "appropriate file documentation and decision rationale."[100] In *Kelly*, the employee responsible for "locating and hiring IMEs" testified that no formal evaluation system existed, and the court accepted that answer.[101] The claims reassessed under the settlement were reconsidered with examinations obtained under the same selection rule.[102]

---

[94] *Hangarter, supra,* 373 F.3d at 1011; *Hangarter, supra,* 236 F. Supp. 2d at 1084.

[95] Regulatory Settlement Agreement §§ B.3.c(i), B.3.f, B.3.h.

[96] Id. Ex. 6, § A.2. The October 2005 amendment's attending-physician rule contains an exception in substantially the same words, so a paper review that makes the Exhibit 6 finding satisfies both. Amendment to Regulatory Settlement Agreement ¶ 5.

[97] Order of the Commissioner, at 2.

[98] *Hangarter, supra,* 236 F. Supp. 2d at 1085; *Waggener, supra,* 238 F. Supp. 2d at 1181, 1188.

[99] Regulatory Settlement Agreement § B.3.d; id. Ex. 6, § C.1.

[100] Id. §§ B.3.a(iv), B.3.e & Exs. 3, 5.

[101] *Kelly, supra,* 2010 WL 3259997, at *2–3.

[102] The Claim Reassessment Unit operated "as a unit of the Benefit Center," reported "to the most senior executive in charge of claim operations," and used "internal and external resources as appropriate, including peer calls and independent medical examinations." Regulatory Settlement Agreement § B.2.a & Ex. 1, §§ III.1, III.4.

The settlement named the selection rule as a subject for examination. Section B.3.i directs examiners to review claim files for the failure to "[s]elect individuals to conduct IMEs and FCEs solely on the basis of objective, professional criteria, and without regard to results of previous IMEs or FCEs," and, separately, for "[a]ctions suggesting a pre-disposition or bias against the claimant" and "[e]vidence of any incentives provided to deny or terminate benefits."[103] The next paragraph defines compliance as an error rate of no more than 7 percent, determined by "random samples of the total files," with a $145 million fine at stake.[104]

The two cannot be made to work together. Whether an examiner was chosen with regard to earlier results is not a fact about a claim file. It is a fact about a pattern across files, and it is held by the company and recorded nowhere. The same is true of an incentive to deny. A random sample of individual files cannot reach either, however large the sample or the penalty. The drafters placed three subjects on the monitoring list and, one paragraph later, selected the one method of monitoring that could not observe them.

The 2008 re-examination reported error rates of 4, 4, 0, and 3 percent and said nothing about how examiners were selected.[105] Under that test, an insurer that sent every examination to a physician who had never found a claimant disabled would show a credentialed examination, a documented rationale, and an error rate of zero. California's later examinations contain no findings regarding any examiner (Part III.B).[106]

F. What the Remedy Required

The regulators recognized the bias, designated it as a subject for monitoring, and prohibited the selection of examiners based on their results. They then wrote a remedy that required no record of what examiners were paid, how often they were used, how their opinions came out, or how they were chosen, and measured compliance with a test that could not see any of it. They did not, however, lack access to the underlying material. Section B.3.l defines a claim file to include "all documents relating to a claim history and/or decision, including but not limited to correspondence, medical records, vocational records, forms, internal memoranda and internal communications (including e-mail communications)," and provides that "[t]he Lead Regulators and the DOL shall have access to all such paper or electronic files at all times." Compiling any examiner's engagement history required no new obligation on the companies. It required someone to ask. The

[103] Regulatory Settlement Agreement § B.3.i.

[104] Id. §§ B.3.j, D.6, D.7.

[105] 2008 Examination Report, at 8–11.

[106] 2008 CDI Follow-Up Report, at 6–7; Cal. Dep't of Ins., Report of the Market Conduct Examination of the Claims Practices of Unum Life Ins. Co. of Am., Provident Life & Accident Ins. Co., and Paul Revere Life Ins. Co., at 4–6 (as of Feb. 15, 2013) (adopted Dec. 17, 2014). The 2008 California follow-up reviewed 191 reassessed files and found seven violations, below the settlement's tolerance. 2008 CDI Follow-Up Report, at 3.

multistate inquiry closed without deciding whether the companies' practices were systemic, and the re-examination was confined to the issues already examined.[107]

The regulators identified the mechanism, prohibited it, and designated compliance with the prohibition as a subject for examination. They then measured compliance by a test that could not reach it, required no record from which it could be reached, and made the untestable prohibition permanent. They reserved access to every claim file and every internal communication in it, at all times, and in twenty-one years and four examinations named no examiner, counted no engagement, and stated no payment.

The reassessment program shows that these regulators were not indifferent to claimants. Two hundred ninety thousand notices went out, and $676.2 million was paid or reserved. That is the difficulty. The multistate examiners had found the bias themselves and had the litigated record available to them, and they wrote a prohibition they made untestable. California went further and then stopped short: in the same instrument in which it required its own appointed reviewers to disclose any interest "likely to affect impartiality or that might create an appearance of partiality," to be free of bias toward either side, and to be removable for a pattern or practice, it required nothing of the examiners the companies hired. Whatever was intended, both instruments were built so that the practice they addressed could not be seen, and it has not been seen since.

G. What the Remedy Disregarded

California law already contained the instrument the regulators needed, and the California Settlement Agreement applied it, to the one reviewer the Department appointed itself. Where California law requires a decisionmaker to be neutral, it requires that decisionmaker to disclose, affirmatively, in writing, and before the decision is taken, the facts on which a party can assess it. The Department wrote that requirement into its own Independent Review process and wrote nothing comparable for the examiners the companies hired.

Candidates to serve as Independent Review Director "must disclose any financial interests or business relationships likely to affect impartiality or that might create an appearance of partiality."[108] The reviewers on the Independent Review panel were to be individuals who, to the Director's knowledge, "have no bias toward either claimants or insurers in determining disability claims,"[109] and either the Department or the company could seek the removal of any reviewer who "has engaged in a pattern or practice that suggests he or she is not qualified for the task of an

---

[107] 2004 Examination Report, at 8 (the settlement "obviated the need for additional investigation, review of a larger claim sample, specific claim findings or reaching a formal conclusion concerning the examination objective"); Settlement FAQ, at 1 ("no specific 'findings' were reached"); Regulatory Settlement Agreement §§ C.2 (re-examination "of the issues addressed by the Multistate Examination"), C.11, C.12 (no admission). During the agreement, each participating state agreed not to conduct its own Model Act market conduct examination or impose remedies for the matters it covered, subject to the reservations in §§ D.10 and D.13. Id. § C.15. California did not join the multistate settlement. California Settlement Agreement § III.A.

[108] California Settlement Agreement, Ex. B; see Part IV.A.

[109] California Settlement Agreement, Ex. B.

informed review of a disability claim file, or that he or she is not performing in a fair, thorough and objective manner."[110] The Department wrote a disclosure rule, an appearance standard, and a pattern-and-practice removal mechanism into the same instrument, and left Unum's own examiners subject to nothing beyond an unwritten instruction to select on "objective, professional criteria" and "without regard to results of previous IME's."[111]

The model was neither new nor untested. California had imposed the same architecture on private adjudication a decade before the settlements. A proposed neutral arbitrator "shall disclose all matters that could cause a person aware of the facts to reasonably entertain a doubt that the proposed neutral arbitrator would be able to be impartial."[112] The statute enumerates what that includes: any ground that would disqualify a judge, among them a current arrangement, or discussions within the last two years, concerning prospective paid service as a neutral for a party;[113] any attorney-client relationship, and any professional or significant personal relationship, with a party or a party's lawyer; and the names of the parties to every prior or pending case in which the arbitrator has served for any party or lawyer in the proceeding, together with the result of each case arbitrated to conclusion, the date of the award, the prevailing party, and the amount of any damages.[114] The disclosure reaches back five years, and it must be made to all parties in writing within ten calendar days of notice of the proposed nomination or appointment.[115]

Section 1281.9 forbids no relationship. An arbitrator who derives a year's income from a single party may serve, and the award is not impeached by that fact. What the statute requires is that the

---

[110] California Settlement Agreement, Ex. B.

[111] Regulatory Settlement Agreement § B.3.d; id. Ex. 6, § C.1; see Parts IV.B and IV.E.

[112] Cal. Code Civ. Proc. § 1281.9(a).

[113] The grounds that disqualify a judge are set out at Cal. Code Civ. Proc. § 170.1. They include a financial interest in the subject matter of the proceeding or in a party, id. § 170.1(a)(3)(A), together with "a duty to make reasonable efforts to inform himself or herself about his or her personal and fiduciary interests," id. § 170.1(a)(3)(C); the circumstance that "[a] person aware of the facts might reasonably entertain a doubt that the judge would be able to be impartial," id. § 170.1(a)(6)(A)(iii); and "a current arrangement concerning prospective employment or other compensated service as a dispute resolution neutral," or discussions regarding such employment within the last two years with a party, id. § 170.1(a)(8)(A), "party" being defined to include "the parent, subsidiary, or other legal affiliate of any entity that is a party," id. § 170.1(a)(8)(B)(ii). The last of these is the closest analog in California law to the position of a retained medical examiner: for a judge the Legislature treated the prospect of future paid work from a party as disqualifying in itself, without inquiry into whether it in fact influenced anything, while for a neutral arbitrator the same fact is disclosable rather than disqualifying. The judicial provisions also separate what must be disclosed from what requires recusal. A judge must disclose a reportable campaign contribution from a party or lawyer "even if the amount would not require disqualification," id. § 170.1(a)(9)(C), and the party who did not make the contribution may waive the disqualification it creates, id. § 170.1(a)(9)(D). Disclosure is the broader duty because its function is to enable the parties to evaluate the risk rather than to resolve it.

[114] *Id.* § 1281.9(a)(1) (grounds that would disqualify a judge, including the prospective-service ground at Cal. Code Civ. Proc. § 170.1(a)(8)(A)); id. § 1281.9(a)(5), (a)(6) (attorney-client relationships and professional or significant personal relationships); id. § 1281.9(a)(4) (prior and pending cases and their results); see id. § 1281.9(a)(3) (imposing the same disclosure as to service as a party arbitrator).

[115] *Id.* § 1281.9(b), (d).

relationship be stated and that the parties be given a defined opportunity to act on it: a proposed neutral who fails to disclose is disqualified on the demand of any party entitled to the disclosure, a proposed neutral who does disclose is disqualified only if a party then serves a notice of disqualification, each within fifteen days, and the objection is waived if no notice is served.[116]

That architecture presupposes a party who can act on what he is told. A party to an arbitration participates in selecting the neutral, pays the neutral, and may reject the neutral on the strength of the disclosure. An insured does none of these things. He has no part in selecting the examiner, which the settlements left to the company alone;[117] he cannot decline the examiner the company selects; and that examiner's opinion will be the factual predicate of the decision on his claim whether he objects to it or not. A disclosure regime borrowed whole from the arbitration statute would hand him a set of facts, no power to act on them, and a waiver that could only ever operate against him.

Where the affected party does not choose the decisionmaker, the law protects him by a prohibition addressed to the decisionmaker rather than by asking his consent, and it does not treat his silence as acceptance. Insurance law has such prohibitions already. California requires the insurer to conduct a "thorough, fair, and objective investigation" of every claim, and the duty is the insurer's own; it is not discharged by referring the question to a consultant.[118] For disability plans governed by ERISA, the Department of Labor has since made the point explicit: claims must be "adjudicated in a manner designed to ensure the independence and impartiality of the persons involved in making the decision," and decisions regarding "hiring, compensation, termination, promotion, or other similar matters" with respect to a medical or vocational expert "must not be made based upon the likelihood that the individual will support the denial of benefits."[119] An insurer may not select a biased examiner, and no disclosure to the claimant cures a breach of that rule.

Disclosure serves a different purpose here than it serves in arbitration. The claimant approves nothing. Disclosure places in the claim file, at the time the opinion is given, the facts on which the claimant can afterward dispute the denial: in the administrative appeal, before the regulator, and in the action that follows. Today no claimant can obtain those facts without filing suit, propounding discovery, and winning an order that survives objection. The arbitration statute is addressed to concealment; here the selection itself is the wrong, and concealment is what keeps it from being examined.

---

[116] Cal. Code Civ. Proc. § 1281.91(a) (disqualification on demand within fifteen days where the proposed neutral fails to comply with section 1281.9); id. § 1281.91(b)(1) (disqualification on a party's notice within the same period where the proposed neutral does comply); id. § 1281.91(c) (waiver where no notice is served, except where the neutral "makes a material omission or material misrepresentation in his or her disclosure"). Subdivision (d) separately preserves a party's right to demand disqualification at any time before the conclusion of the proceeding on any ground specified in section 170.1.

[117] Regulatory Settlement Agreement § B.3.d; id. Ex. 6, § C.1; see Parts IV.B and IV.E.

[118] Cal. Code Regs. tit. 10, § 2695.7(d).

[119] 29 C.F.R. § 2560.503-1(b)(7); see Part VII.F.

California has required, since section 1281.9 took effect on January 1, 1995, that a private neutral hand the parties an outcome record identifying, case by case, who won. That is Factor 2, compiled by the neutral, furnished before the engagement begins, and obtained without any discovery at all. Eleven years after the settlements, and twenty-one years after the arbitration statute took effect, Unum told the United States Department of Labor that a medical expert's reputation for outcomes could not be measured: "In practice and in theory, there is no way to measure 'reputation' in this context."[120] Every neutral arbitrator in California had been measuring it, and disclosing it, for more than a decade.

Two objections are commonly made to treating an examiner's relationship with the insurer as evidence of bias, and each has an answer. The first is compensation. A judge is paid by neither party, so any benefit a party confers on him is anomalous on its face. An insurer must retain medical experts and must pay them, and retention and payment therefore cannot themselves establish bias. *Cardiner* held that "the mere fact that these doctors have been hired by insurers rather than insureds does not support bias," and required something further.[121] Nothing proposed here would disturb that. A disclosure requirement does not make a relationship disqualifying; it makes the relationship known and leaves what follows from it to be argued on the facts of the claim. The necessity of payment is not the necessity of dependence. Nothing about engaging an examiner requires that one physician accept hundreds of referrals from a single company, derive the bulk of his professional income from it, or be engaged again after producing favorable opinions. Those are choices about how to procure, and a record of engagements and compensation would expose them.

The second objection is that dependence must be expressed as a share of the reviewer's income before it can matter. No decision examined for this article makes a proportion the test. *Demer* drew its inference from "evidence of not only the frequency of reviews for MetLife but also the significant dollar amounts earned by the reviewers," reasoning from amount and frequency taken together rather than from any share of the reviewers' practice, and, having found the inference warranted, held that "the burden shifted to MetLife to counter that evidence."[122] *Wittmann* ordered a comparison between a reviewer's compensation from Unum and his compensation from all medical work, but it did so because the claimant had identified that comparison as the purpose of the request, not because a proportion is the measure the law demands.[123] What the decisions treat as significant is material compensation, taken together with whatever else the record shows about how the opinion was produced. A proportion, where it can be obtained, demonstrates materiality. It is not the threshold, and treating it as the threshold concedes more than the cases require.

---

[120] Comment of Unum Group on RIN 1210-AB39, at 10 (Jan. 19, 2016); see Part VII.F.

[121] *Cardiner, supra,* 158 F. Supp. 2d at 1101; see Part II.

[122] *Demer, supra,* 835 F.3d at 902–03.

[123] *Wittmann v. Unum Life Ins. Co. of Am.*, No. 17-9501, 2018 WL 3374164, at *2–4 (E.D. La. July 11, 2018).

Three Requirements the Settlements Could Have Imposed

Each of the three was available on the face of the settlements.

First, disclosure of the indicia of bias by the examiner in each claim. An examiner or reviewer furnishing an opinion on a claim could have been required to state, with the opinion and in the claim file, the matters section 1281.9 requires of a neutral arbitrator: the number of engagements accepted from the company and its affiliates and vendors over a defined preceding period; the compensation received for them; any other financial interest or business relationship with the company likely to affect impartiality or to create an appearance of partiality; and the disposition of the prior engagements.

The duty would attach to the examiner rather than to the insurer, so that it would be discharged at the moment the opinion is given rather than on a regulator's request. It would carry none of section 1281.91's apparatus of objection and waiver, which belongs to a party who may decline the neutral and has no application to a claimant who may not. What it would carry instead is a consequence in the claim: an opinion furnished without the disclosure is not a document on which a denial may rest, and a file containing one is incomplete. Section 1281.9 is enforceable because section 1281.91 attaches disqualification to silence; a disclosure rule for examiners needs its own equivalent, and the completeness of the claim file is the natural one. Its office is evidentiary. It would leave a record in the file of the very facts a court is now told cannot be assembled without a mini-trial in another claimant's case.

Second, retention of the records from which financial dependence can be assessed. What matters is what the insurer paid the reviewer and how often it engaged the reviewer, which are facts the insurer holds and already records for its own purposes. A settlement could have required the companies to maintain, for each examiner and reviewer engaged, the compensation paid, the number of engagements, and the identity of any vendor through which the engagement ran. Where the reviewer's own share of professional income from insurance work can also be obtained, as *Wittmann* shows it sometimes can, it adds to the picture. Where it cannot, the amount and the frequency are the evidence *Demer* found sufficient to shift the burden to the administrator. Neither figure was recorded under either settlement, and the vendor layer removes even the first, because the insurer's records show only what the insurer paid the vendor, not what the vendor paid the physician.[124]

Third, retention of the expert reports themselves. *Chacko* shows that an examiner's pattern can be established from the reports alone: the plan produced the conclusion pages of eighty-eight reviews, counsel tabulated them, and the court verified the tabulation against the pages.[125] A settlement that required the companies to retain the medical opinions prepared for them, indexed by examiner, would have made that demonstration available in every case rather than in the rare one where a court ordered production and the order survived.

---

[124] *Wittmann, supra,* 2018 WL 3374164, at *2–4; see Part VI.C.

[125] *Chacko, supra,* 690 F. Supp. 3d at 1150–51; see Part VII.F.

The retention requirement is the one the companies could least plausibly have resisted, because they already bore the obligation to keep the files. What the Regulatory Settlement Agreement defined was what must be kept, "all documents relating to a claim history and/or decision," and not what must be created or how it must be indexed, and the reassessment unit's tracking duties ran to notice dates, form dates, decision dates and outcomes, never to the examiner used.[126] Adding the examiner to the index would have cost the companies a field.

Demer states the value of the absence of such a record in litigation. The administrator there "could have maintained records of its reviewers' findings on claims to show their neutrality in practice, but it did not," and so "missed an opportunity to negate any inference of a financial conflict of interest."[127] The observation cuts both ways, and the companies have taken advantage of it. Unum's designee in *Kelly* later confirmed that the companies kept no such record.[128] The settlements left the companies in that position, unable to show that they had not selected on outcomes, and left the claimant to prove the negative.

None of the three requirements asks the companies to disclose anything they do not know. Each asks them to write down what they already do, in a form that someone other than the company can inspect. A rule of that kind does not depend on an examination cycle, a penalty tolerance or a regulator's continuing attention, which is what distinguishes it from everything the settlements did impose. It would have left the companies free to engage whichever qualified reviewer they chose, and would have added nothing to the duty to investigate fairly, which they already owed. It would have made it possible, for the first time, to tell whether that duty had been observed.

PART V. UNUM'S PRACTICES CONTINUED AFTER SETTLEMENTS

Unum's procurement of medical opinions that could be relied on to support denial survived the settlements intact. The decisions since 2004 show the practice in two ways. The first is the reviewer's own reasoning: courts have repeatedly found that Unum's reviewers reached conclusions based on their own experience rather than the claimant's record, and treated disabling conditions as self-reported, so that the absence of objective proof could be held against the claimant. The second is the relationship behind the reviewer: where a claimant has been able to show what a particular reviewer was paid, how often Unum used that reviewer, or how that reviewer's opinions came out, courts have ordered the material produced.

The two are not equally available. The first can usually be proved from the reviewer's own report; the second requires discovery, and Part VI describes what happens when a claimant seeks it. The sections that follow take the reviewers first, then the pattern in their reasoning, then what the

---

[126] Regulatory Settlement Agreement § B.3.l & Ex. 1, § III.6.

[127] *Demer, supra,* 835 F.3d at 903.

[128] *Kelly, supra,* 2010 WL 3259997, at *2–3. See also Part VII.D.

settlements require of any of it, and then the one route by which an experiential opinion has actually been tested.

A. The Cases after the Regulatory Settlement Agreement and California Settlement Agreement

The settlements did not end the wrongful practices described in Parts II and III. Courts have continued to find them in claims decided since 2004, and claimants have shown that a particular reviewer's opinions follow a pattern across many claims.[129] Three named reviewers, and one unnamed group, can be identified from the following decisions. Dr. Scott Norris and Dr. James H. Bress are employed physicians, and what is known about them comes from orders compelling their compensation, their performance records, and their opinions in other claims. A third physician, identified in the *Boles* order only as Dr. Bress, reviewed claims under an arrangement that order described in figures before it was sealed; the conditions at issue fall within rheumatology, which is the specialty of Dr. Norman Bress, but no available source supplies the forename.[130] The consultants in *Zagante* are outside physicians, and what is alleged about them is a rate of recommended denial.

In *Braun*, the claimant's appeal was reviewed by Dr. Scott Norris, a physician employed by Unum.[131] To obtain discovery, the claimant cited a line of decisions rejecting Dr. Norris's opinions: opinions based only on file reviews and not supported by the record, opinions that discounted or ignored contrary evidence, opinions on conditions outside the reviewer's expertise, and an opinion that "merely restat[ed] unfavorable evidence" rather than reconciling it.[132] Unum answered that the claimant "simply disparages Dr. Norris, professes that he is wrong on the medical merits, and demands a deposition." The court disagreed. Taken together, the decisions "raise[ ] the possibility

---

[129] See *Chronister, supra,* 563 F.3d at 776 (treating Unum's "history of biased claims administration" as a factor in reviewing a denial, and quoting *Radford Trust, supra,* 321 F. Supp. 2d at 247, on the "disturbing pattern of erroneous and arbitrary benefit denials, bad faith contract misinterpretations, and other unscrupulous tactics"). For the practices identified in the post-settlement decisions, see Section C below.

[130]

[131] *Braun v. Unum Life Ins. Co. of Am.*, No. 22 CV 1223, 2022 WL 17740459, at *1 (N.D. Ill. Dec. 16, 2022). Dr. Norris is board-certified in family, occupational, and aerospace medicine, has worked at Unum since 2010, and has not treated patients since then. *Dwyer v. Unum Life Ins. Co. of Am.*, 548 F. Supp. 3d 468, 483 (E.D. Pa. 2021); see *Mundrati v. Unum Life Ins. Co. of Am.*, 772 F. Supp. 3d 567, 578 n.9 (W.D. Pa. 2025). Courts have given Dr. Norris's opinions "little weight," *Boykin v. Unum Life Ins. Co. of Am.*, No. 2:19-cv-00137-TLN-DB, 2022 WL 458213, at *16 (E.D. Cal. Feb. 15, 2022); held that restating unfavorable evidence does not reconcile it, *Clark v. Unum Life Ins. Co. of Am.*, No. 3:17-cv-01119, 2018 WL 4931935, at *15 (M.D. Tenn. Oct. 10, 2018); see also *Mundrati*, 772 F. Supp. 3d at 587; declined to credit the opinion over those of physicians who examined the claimant, *Fleming v. Unum Life Ins. Co. of Am.*, No. SACV 17-01576-CJC (JDEx), 2018 WL 6133859, at *10 (C.D. Cal. Nov. 20, 2018); see *Boersma v. Unum Life Ins. Co. of Am.*, 546 F. Supp. 3d 703, 713 (M.D. Tenn. 2021); and, after the claimant deposed Dr. Norris, found the claimant disabled on de novo review, *Dwyer*, 548 F. Supp. 3d at 483–84.

[132] *Braun*, 2022 WL 17740459, at *2–3 (discussing, among others, *Carney*, *Dwyer*, *Boykin*, *Boersma*, *Tam*, *Mistick*, *Rikimaru*, *Brown*, *Fleming*, and *Clark* (M.D. Tenn.), as well as *Chicco v. First Unum Life Ins. Co.*, No. 20 CV 10593, 2022 WL 621985, at *4 (S.D.N.Y. Mar. 3, 2022), and *Dewsnup v. Unum Life Ins. Co.*, No. 17 CV 126, 2018 WL 6478886, at *10 n.3 (D. Utah Dec. 10, 2018)).

that [Unum's] decision[-]making process … was structurally tainted in a material way."[133] The court allowed the claimant to depose Dr. Norris on the reviewer's training and expertise and whether Unum considers them in assigning claims, the reviewer's compensation and any "financial incentive to deny" claims, the reviewer's knowledge of Unum's "general approval and termination rates," and the "steps [Unum] has taken to reduce bias and promote accuracy."[134]

The deposition was to be completed by January 31, 2023.[135] The court then decided the claim on the administrative record and ruled for Unum, in an opinion that does not mention the deposition. It found that the structural conflict did not influence the decision because Unum "has been acting pursuant to the [Regulatory Settlement Agreement] for almost twenty years" and "[n]othing in the [Regulatory Settlement Agreement] or any case law prevents defendant from relying on medical examiners that it employs." It also treated Unum's offer of an examination, which the claimant declined, as a safeguard "to minimize the conflict."[136] The claimant had assembled a judicial record of the reviewer's errors, and the settlement was accepted as evidence that the conflict had been addressed.

In *Boles*, the court granted a motion to compel answers to interrogatories on Unum's conflict of interest.[137] The order recited the answers. The reviewing physician, identified in the order only as Dr. Bress, had reviewed an average of some 250 Unum claims a year, about eleven a year within the condition class at issue, and had received an average of $237,500 a year in 2008 and 2009 for work on Unum files.[138] Two days later, on Unum's emergency motion, the court prohibited publication of the order. The claimant moved to make it public; Unum, which had by then answered the interrogatories, moved for reconsideration, and the court declined to "reconsider, rewrite, or redact" the order.[139] One hundred and eight days after the order was entered, the court denied the

---

[133] *Id.* at *3 (quoting *Mohammed v. Prudential Ins. Co.*, No. 19 CV 3258, 2020 WL 4569696, at *7 (N.D. Ill. Aug. 7, 2020)). The court made no finding that Dr. Norris had engaged in misconduct or shown bias. *Id.*

[134] *Id.* at *3 (drawing the subjects from *Klein v. Northwestern Mut. Life Ins. Co.*, 806 F. Supp. 2d 1120, 1127 (S.D. Cal. 2011)).

[135] Minute Entry, *Braun*, No. 1:22-cv-01223 (N.D. Ill. Dec. 16, 2022), ECF No. 31.

[136] *Braun v. Unum Life Ins. Co. of Am.*, No. 22 C 1223, 2023 WL 4205536, at *5, 7 (N.D. Ill. June 27, 2023).

[137] Memorandum and Order, *Boles v. Unum Life Ins. Co. of Am.*, No. 4:11-cv-03031 (D. Neb. Jan. 22, 2013), ECF No. 69 (restricted access).

[138] *Boles, supra,* 2013 WL 1079016, at *1–2 & n.1 (order denying reconsideration, reciting the figures). The January 22 order is sealed, and the reconsideration order does not name the reviewer; the figures are attributed to "Dr. Bress" without a forename. The conditions recited with those figures fall within rheumatology, the specialty of Dr. Norman Bress, but no available source states the forename.

[139] Order, *Boles, supra,* No. 4:11-cv-03031 (D. Neb. Jan. 24, 2013), ECF No. 71 (restricting access); *Boles, supra,* 2013 WL 1079016, at *1–2. Unum asked the court to remove "factual conclusions about [Unum's] handling of [Boles'] claim . . . and broad accusatory statements about [Unum's] culture and claims practices that have no support in the limited record before the court."

motion to make the order public as moot and directed that the order "shall remain a restricted access document." Judgment of dismissal followed on June 5, 2013.[140]

Clark shows a court ordering production of a staff reviewer's other opinions. The claim, under an individual disability policy issued by Paul Revere, was denied based on the opinions of physicians who work for Unum, including Dr. James H. Bress.[141] The court described the claimant's allegation as a denial "based upon the statistical average recovery time for pulmonary embolisms instead of reviewing the claim based on the symptoms and recovery Dr. Clark specifically experienced."[142] The court ordered production of the personnel files of those physicians and of the claim staff, including "salary or bonuses," together with their compensation for 2015 through 2019 and their scorecards.[143] Unum objected that evaluating Dr. Bress's other opinions would require "a series of mini-trials." The court found the request "clearly relevant" and ordered production of the opinions Dr. Bress and two other staff physicians gave on individual disability claims involving pulmonary embolism from 2015 through 2017.[144]

Claimants have also documented a pattern in figures. In *Zagante*, decided in May 2026, the claimant alleged that the outside consultant physicians who reviewed the claim had no expertise relevant to the claimed disability, and that at least one "has a track record of recommending denial of LTD benefits in 82% of the matters considered." The court held those allegations sufficient. It

---

[140] Text Order, *Boles, supra,* No. 4:11-cv-03031 (D. Neb. May 10, 2013), ECF No. 89; Judgment, *id.* (June 5, 2013), ECF No. 91 (dismissal with prejudice on joint motion).

[141] *Clark v. Unum Grp.*, No. 4:20-CV-04013-KES, 2022 WL 17251352, at *1, 6, 18 (D.S.D. Nov. 28, 2022). *Clark* asserted state-law bad faith and contract claims, with alternative claims under ERISA. *Id.* at *1. Two physicians named Bress appear in the decisions. Dr. James H. Bress is an internist: "Dr. James H. Bress, board-certified in internal medicine," *Vander-Leeuw v. First Unum Life Ins. Co.*, No. 11-5685, 2013 WL 3479433, at *5 (D.N.J. July 9, 2013); "Dr. J. Bress, a board-certified internist," *Price v. Unum Life Ins. Co. of Am.*, No. GJH-16-2037, 2018 WL 1352965, at *5 (D. Md. Mar. 14, 2018); "Dr. Bress, a Board Certified Internist," *Bellard v. Unum Life Ins. Co. of Am.*, No. 15-0428, 2016 WL 7108577, at *4 (W.D. La. Dec. 5, 2016). Dr. Norman Bress is a rheumatologist: "Dr. Norman Bress, a rheumatologist," *Weitzenkamp v. Unum Life Ins. Co. of Am.*, 661 F.3d 323, 328 (7th Cir. 2011); "Rheumatologist Norman Bress, M.D.," *Bilyeu v. Morgan Stanley Long-Term Disability Plan*, No. CV-08-02071-PHX-SRB, 2015 WL 4134447, at *7 (D. Ariz. June 2, 2015), *aff'd*, 711 F. App'x 380 (9th Cir. 2017). Where an opinion gives only "Dr. Bress," the stated specialty or the condition under review identifies which physician is meant. Dr. James Bress has also reviewed claims for another insurer as "a physician consultant at University Disability Consortium." *Campbell v. United of Omaha Life Ins. Co.*, No. 2:14-cv-00623-JEO, 2015 WL 5818040, at *7 (N.D. Ala. Oct. 6, 2015). In a second United of Omaha case, the insurer agreed to disclose "the number of files Dr. Bress and his employer have reviewed on behalf of United, and the amount of income Dr. Bress has received," and the court refused to order production of the reports Dr. Bress wrote immediately before and after the claimant's. *Weinberg v. United of Omaha Life Ins. Co.*, No. 13-11017-NMG, 2014 WL 250339, at *1–2 (D. Mass. Jan. 21, 2014).

[142] *Clark* (D.S.D.), *supra,* 2022 WL 17251352, at *18.

[143] *Id.* at *6–8, 21.

[144] *Id.* at *21–22. The court excluded opinions given to Provident, a nonparty, and limited production to pulmonary-embolism claims. *Id.* at *22. Compare *Small* and *Kelly*, discussed in Part IV.C, both of which ordered production of an examiner's other reports in bad faith actions, with *Warner* and *Dwyer*, discussed in Section E, which refused comparable discovery in ERISA actions.

ordered First Unum to produce each consultant's total compensation, the number of reports each prepared for it in 2023 and 2024, and the method by which each was paid. On the allegations made, it declined to order comparable discovery about the insurer's employees who reviewed the claim.[145]

B. How the Opinions Work

The reviewers are no longer only Unum's own staff. The regulators' concern was Unum's reliance on in-house professionals.[146] California's 2008 follow-up then reported a significant increase in the companies' use of examinations and record reviews between 2003 and 2006.[147] The decisions since the settlements involve two groups: physicians employed by Unum who review files, such as Dr. Norris and Dr. James Bress, and outside physicians retained to examine claimants or review their records. By 2010, Unum staff in its Independent Assessment Network were responsible for "locating and hiring IMEs."[148] In *Zagante*, the reviewers at issue were "independent consultant physicians" who prepared "IPC reports" for First Unum.[149] The opinions described below come from both groups, and neither settlement requires a record of the outcomes of either group.

Whichever group a reviewer belongs to, the bias at issue is the same. Financial dependence bias arises when a reviewer's income depends on continued work from an insurer, its vendors, or the industry as a whole, and the reviewer has reason to supply the opinions that keep the work coming. For an outside consultant, the work is the next referral. For an employed reviewer, it is continued employment, pay, and advancement. Courts have recognized both forms. Courts have also ordered production of employed reviewers' compensation and bonuses because the records may show "whether a particular employee was rewarded financially for denying a certain number or percentage of claims."[150]

Payment alone proves nothing, because an insurer must pay for every opinion it obtains. The question is the degree of dependence: how much of the reviewer's work and income comes from the payor, and for how long. The other three factors show whether that dependence has operated and whether anything has been done to check it. Factor 2 shows whether the reviewer's conclusions run consistently in one direction. Factor 3 shows the marks the dependence leaves on

---

[145] *Zagante v. First Unum Life Ins. Co.*, No. 25-CV-06680 (JGK) (RFT), 2026 WL 1413584, at *1–2 (S.D.N.Y. May 20, 2026). The 82 percent figure is the claimant's allegation; the court found it sufficient to support discovery and made no finding on its accuracy. The order is without prejudice to a later application for discovery into whether the insurer's employees "had any financial incentives to deny the claim." *Id.* at *1.

[146] 2004 Examination Report, at 6; see Part III.A.

[147] 2008 CDI Follow-Up Report, at 6–7.

[148] *Kelly, supra,* 2010 WL 3259997, at *2–3.

[149] *Zagante*, *supra,* 2026 WL 1413584, at *1.

[150] *Clark* (D.S.D.), *supra,* 2022 WL 17251352, at *7 (quoting *Anspach v. United of Omaha Life Ins. Co.*, No. 5:10-CV-05080-JLV, 2011 WL 3862267, at *9 (D.S.D. Aug. 31, 2011)); see *Warner v. Unum Life Ins. Co. of Am.,* No. 12 C 2782, 2013 WL 3874060, at *6 (N.D. Ill. July 26, 2013) (ordering compensation and bonus information for employed and outside reviewing physicians as "circumstantial evidence of structural bias").

the handling of individual claims. Factor 4 asks whether the insurer has safeguards that would detect or prevent it, of the kind *Glenn* describes: separating the reviewer from those with an interest in the company's finances, or "imposing management checks that penalize inaccurate decisionmaking irrespective of whom the inaccuracy benefits."[151]

Each factor looks past the form of an arrangement to its effect. A reviewer described as independent may depend on the insurer as heavily as an employee does. A compliance program that audits file documentation measures none of the four factors. The settlements and Unum's responses to bias discovery since have addressed form: the reviewer's credentials, the documentation of the decision, the existence of a quality function, and the settlement. None of these shows whether a reviewer depends on the insurer or whether that dependence has shaped the opinion.

Whatever their source, the opinions in these decisions share a pattern. Unum's reviewers reach conclusions based on their own judgment and experience rather than the claimant's records, and they treat disabling conditions such as pain, limited range of motion, and weakness as self-reported, so that the absence of objective proof can be held against the claimant. California's Order describes the practice in its own terms: "[f]ailing to request that the IME perform objective testing that could support a finding of disability resulting from a 'self-reported condition'" and "[d]iscounting objective test results by imputing the physiologically disabling condition to a 'psychological component.'"[152]

C. Key Practices Identified by the Courts

A review of court decisions and litigation records involving Unum and its affiliates has identified 87 distinct irregularities in the handling of disability claims.[153] Forty-three of them concern how an expert's opinion is obtained, framed, or used.[154] The decisions cited for them concern claims decided after the 2004 settlement.

---

[151] *Glenn, supra,* 554 U.S. at 117.

[152] Order of the Commissioner, at 3.

[153] For an earlier survey of the post-settlement decisions, see Philip W. Thomas, *Fifteen Years Later – Did the Unum Group Improve Its ERISA Claims Handling Practices?*, 39 Miss. C. L. Rev. 199, 209–25 (2021). Thomas groups the decisions under eight headings: improper cherry-picking from medical records; disregarding evidence favorable to claimants; mischaracterization and failure to analyze claimant's job duties; requesting independent physicians opine on mis-defined job description; disregarding attending physicians' opinions on disability; failing to adequately communicate with attending physicians; disregarding Social Security Administration's disability determination; and fabrication of evidence or misstating the administrative record. Id. Thomas concludes that "Unum repeatedly loses cases for the same underlying reasons," that "[t]here are too many cases for these to be honest mistakes," and that "[i]t is a playbook." Id. at 234. The eight headings correspond to roughly two dozen of the 87 practices. Reasoning from assumption, the first group identified here, has no heading of its own, and none of the headings addresses how the reviewer was selected or paid.

[154] The other practices concern the routing and scheduling of claims, the application of policy terms, the preservation and disclosure of records, the internal appeal, the insurer's internal targets and incentives, and litigation conduct. The

(1) Reasoning from Assumption. The first group concerns the reviewer's own reasoning. In *Proctor*, Unum relied on the premise that "most people's cognitive impairments from mild concussions resolve within 3 months," and the court found that "Unum relied on the typical progression, rather than Proctor's progress to deny Proctor's continuing claim."[155] In *Mistick*, "each of Unum's file reviewers made credibility determinations and dismissed the opinions of Mistick's treating physicians and the limitations they imposed as subjective exaggerations without examining Mistick."[156] Reviewers have inferred capacity from recreation, although "[s]wimming, walking, and biking have nothing to do with Kaminski's ability to perform full-time work that consists of 'mostly sitting,'" and have inferred that a condition was not disabling because treatment did not escalate.[157] The decisions record seven practices of this kind, and an eighth has been alleged.[158]

(2) Disregarding Contrary Evidence. The second group concerns what the reviewer leaves out. Courts have found that Unum's reviewers "cited only those portions of the medical record that supported its denial of the claim,"[159] that a reviewer "listed all of Clark's supplemental records with brief descriptions" without addressing them,[160] and that Unum "started

---

selection, qualifications and compensation of reviewers are counted within the forty-three, and Part IV addresses them under Factors 1, 2 and 4.

[155] *Proctor v. Unum Life Ins. Co. of Am.*, No. 20-2472 (JRT/DTS), 2022 WL 4585278, at *10, 15 (D. Minn. Sept. 29, 2022).

[156] *Mistick v. Unum Grp. Corp.*, No. 1:19-cv-190, 2020 WL 13442144, at *6 (E.D. Tenn. Mar. 30, 2020).

[157] *Kaminski v. Unum Life Ins. Co. of Am.*, 517 F. Supp. 3d 825, 863 (D. Minn. 2021); *Dwyer, supra,* 548 F. Supp. 3d at 490.

[158] The practices, with representative decisions, are: (1) credibility determinations by reviewers who never examined the claimant, *Mistick, supra,* 2020 WL 13442144, at *6; *Carney v. Unum Life Ins. Co. of Am.*, 596 F. Supp. 3d 845, 857–58 (E.D. Mich. 2022); *Mundrati, supra,* 772 F. Supp. 3d at 587; (2) reliance on how most patients fare rather than on the claimant's record, *Proctor, supra,* 2022 WL 4585278, at *15; *Dimopoulou v. First Unum Life Ins. Co.*, 162 F. Supp. 3d 250, 259 (S.D.N.Y. 2016); *Boersma, supra* 546 F. Supp. 3d at 713; (3) reasoning from the expected course of a condition, *Proctor, supra,* 2022 WL 4585278, at *15, 18; *Bencivenga v. Unum Life Ins. Co. of Am.*, No. 14-10118, 2015 WL 1439697, at *7, 11 (E.D. Mich. Mar. 27, 2015); (4) inferring capacity from daily activities, travel, or prescribed exercise, *Kaminski, supra,* 517 F. Supp. 3d at 863; *Schwartz v. Unum Life Ins. Co. of Am.*, No. 24-cv-02444-TSH, 2025 WL 1827904, at *15 (N.D. Cal. July 1, 2025); *Petrusich v. Unum Life Ins. Co. of Am.*, 984 F. Supp. 2d 1112, 1123 (D. Or. 2013); (5) finding capacity from the absence of stated restrictions, or only on conditions, *Logan v. Paul Revere Life Ins. Co.*, No. 1:24-cv-113, 2025 WL 2723542, at *19 (E.D. Tenn. Sept. 24, 2025); *Petrusich, supra,* 984 F. Supp. 2d at 1121; (6) treating a normal or negative test result as proof, *Radmilovich v. Unum Life Ins. Co. of Am.*, 701 F. Supp. 3d 984, 1000 (C.D. Cal. 2023); *Meyer v. Unum Life Ins. Co. of Am.*, 96 F. Supp. 3d 1234, 1250 (D. Kan. 2015) (causation under a pre-existing-condition exclusion); and (7) inferring severity from the intensity of treatment, *Dwyer, supra,* 548 F. Supp. 3d at 490; *Iravani v. Unum Life Ins. Co. of Am.*, 692 F. Supp. 3d 904, 918 (N.D. Cal. 2023); *Clark* (M.D. Tenn.)*, supra,* 2018 WL 4931935, at *16. The review also identified templated reasoning, in which a reviewer applies largely identical analysis across unrelated claims. That practice has been alleged but not found. See *Choi v. Unum Life Ins. Co. of Am.*, No. 24-06338-JKS-AME, 2025 WL 2234903, at *1, 5 (D.N.J. Aug. 6, 2025) (reciting the claimant's allegations in denying a discovery motion).

[159] *Mundrati, supra,* 772 F. Supp. 3d at 590.

[160] *Clark* (M.D. Tenn.)*, supra,* 2018 WL 4931935, at *15.

parsing off Plaintiff's symptoms and possible diagnosis for separate review by specialists," so that no one assessed the conditions together.[161] The group includes the treatment of Unum's own consultants. In *Kamerer*, "Unum's own consultants . . . concluded that Ms. Kamerer was not disabled from psychiatric symptoms," yet Unum "alleged that Ms. Kamerer's disability was due to psychological conditions."[162] The decisions record eight practices in this group.[163]

(3) Failure to Investigate and Restriction of the Evidence. A reviewer's opinion depends on the file they are given. Unum has relied on file reviews "despite the fact that Carney's complaints (pain and its ensuing effects) are highly subjective in nature."[164] It has refused an examination the claimant requested.[165] In *Bulas*, a reviewer found the record "indeterminate" and said further testing "would assist in this determination"; no testing was requested, and the same reviewer then agreed, "without the benefit of any additional testing," that the claimant could work.[166] Unum has asked physicians to assess a claimant's capacity against an occupational description that omitted "the cognitive requirements, which are undoubtedly relevant because Wessberg is claiming cognitive impairment,"[167] and has limited a records request so that its reviewer, lacking the record of a visit to the treating neurologist, reported "no follow-up with treating neurologist."[168] The decisions record four practices of failing to investigate and three of restricting the evidence.[169]

---

[161] *Lewis v. Unum Life Ins. Co. of Am.*, 569 F. Supp. 3d 983, 1013 (D. Ariz. 2021).

[162] *Kamerer v. Unum Life Ins. Co. of Am.*, 334 F. Supp. 3d 411, 428 (D. Mass. 2018).

[163] The practices, with representative decisions, are: (1) review of each condition in isolation, *Lewis, supra,* 569 F. Supp. 3d at 1013; *Freeland, supra,* 2013 WL 4482995, at *12; *Mistick, supra,* 2020 WL 13442144, at *6; (2) selective citation of the record, *Mundrati, supra,* 772 F. Supp. 3d at 590; *Kaminski, supra,* 517 F. Supp. 3d at 865; *Bencivenga, supra,* 2015 WL 1439697, at *13; *Schwartz, supra,* 2025 WL 1827904, at *13; (3) failure to address evidence favorable to the claimant, *Carney, supra,* 596 F. Supp. 3d at 859; *Wessberg v. Unum Life Ins. Co. of Am.*, No. 22-94 (JRT/DLM), 2024 WL 3444044, at *17 (D. Minn. July 15, 2024); *Doe v. Unum Life Ins. Co. of Am.*, 35 F. Supp. 3d 182, 192 (D. Mass. 2014); (4) listing the evidence in place of weighing it, *Clark* (M.D. Tenn.)*, supra,* 2018 WL 4931935, at *15; *Doe, supra,* 35 F. Supp. 3d at 192; (5) disregarding a Social Security disability award, including one the insurer helped the claimant pursue, *Iravani*, 692 F. Supp. 3d at 912, 914; *Chronister, supra,* 563 F.3d at 777; (6) excluding evidence as not "time relevant," *Mundrati, supra,* 772 F. Supp. 3d at 590, 592; *Dimopoulou, supra,* 162 F. Supp. 3d at 261; *Wessberg, supra,* 2024 WL 3444044, at *15; (7) rejecting attending physicians' opinions without stated reasons, *Kamerer, supra,* 334 F. Supp. 3d at 426; *Dwyer, supra,* 548 F. Supp. 3d at 492; *Carney, supra,* 596 F. Supp. 3d at 858; and (8) setting aside the opinions of the insurer's own consultants or reviewers, *Kamerer, supra,* 334 F. Supp. 3d at 428; *Proctor, supra,* 2022 WL 4585278, at *15; *Radmilovich, supra,* 701 F. Supp. 3d at 1000.

[164] *Carney, supra,* 596 F. Supp. 3d at 856.

[165] *Moseley, supra,* 659 F. Supp. 3d at 90–91.

[166] *Bulas v. Unum Life Ins. Co. of Am.*, No. 2:22-cv-112, 2023 WL 3951214, at *16 (S.D. Ohio June 12, 2023).

[167] *Wessberg*, 2024 WL 3444044, at *16; see id. at *4, 17.

[168] *Hertan v. Unum Life Ins. Co. of Am.*, 111 F. Supp. 3d 1075, 1080–81 (C.D. Cal. 2015).

[169] The practices of failing to investigate, with representative decisions, are: (1) reliance on file reviews where the condition or a question of credibility called for an examination, *Carney, supra,* 596 F. Supp. 3d at 856–57; *Tam v. First*

(4) Manufacturing Support. Unum has also drafted the opinion it needed and asked a physician to adopt it. In *Knuth*, Unum's on-site physician "twice wrote to Rogers on the issue of etiology asking him to agree that Knuth's condition resulted from an illness (a degenerative back condition) and not an accident."[170] In *Backman*, Unum "extracted a single sentence from Dr. Suchard's report, listing Backman's functional limitations but omitting Suchard's opinion that Backman could not return to work due to her disability."[171] In *Hart*, Unum's letter to a treating physician stated: "If you agree with the summary of our discussion as set forth above, there is no need to respond to this letter."[172] Other decisions record statements by a physician's office staff presented as the physician's own. The decisions record six practices in this group, and two more have been identified.[173]

(5) Other Practices. The remaining groups are smaller. The question put to the reviewer can fix the answer, as when an occupation is measured against generic demands, a physical standard is applied to cognitive work, or the question includes a condition the policy does not contain. California found that Unum handled own-occupation claims "as if they were

---

Unum Life Ins. Co., 491 F. Supp. 3d 698, 709, 711 (C.D. Cal. 2020); (2) failure to obtain an examination the circumstances called for, *Moseley, supra,* 659 F. Supp. 3d at 90–92; *Iravani, supra,* 692 F. Supp. 3d at 914; *Petrusich, supra,* 984 F. Supp. 2d at 1122; (3) failure to obtain testing identified as necessary, *Bulas, supra,* 2023 WL 3951214, at *16; *Petrusich, supra,* 984 F. Supp. 2d at 1122–23; and (4) failure to speak with the treating physician, *Warner v. Unum Life Ins. Co. of Am.*, No. 12 C 2782, 2014 WL 7497233, at *2 (N.D. Ill. Dec. 31, 2014); *Carney, supra,* 596 F. Supp. 3d at 857. The practices of restricting the evidence are: (1) omitting the relevant occupational demands from the description given to those asked to assess capacity, *Wessberg, supra,* 2024 WL 3444044, at *4, 16–17; *Doe v. Unum Life Ins. Co. of Am.*, No. 13-6900, 2014 WL 6454560, at *4 (E.D. Pa. Nov. 18, 2014); (2) limiting the records that reach the reviewer, *Hertan, supra,* 111 F. Supp. 3d at 1080–81; and (3) selective use or description of surveillance, *Doe, supra,* 35 F. Supp. 3d at 194–95; *Clarke v. Unum Life Ins. Co. of Am.*, 852 F. Supp. 2d 663, 673, 681 (D. Md. 2012); *Knuth v. Paul Revere Life Ins. Co.*, No. CV-14-02387-TUC-RCC (DTF), 2017 WL 8941237, at *8 (D. Ariz. Feb. 6, 2017) (finding a jury question on the point).

[170] *Knuth, supra,* 2017 WL 8941237, at *8; see *id.* at *10 (finding evidence from which a jury could conclude that Unum "attempted to create evidence unfavorable to its insured").

[171] *Backman v. Unum Life Ins. Co. of Am.*, 191 F. Supp. 3d 1053, 1069 (N.D. Cal. 2016).

[172] *Hart v. Unum Life Ins. Co. of Am.*, 253 F. Supp. 3d 1053, 1064 (N.D. Cal. 2017); see *id.* at 1072.

[173] The practices, with representative decisions, are: (1) asking a treating physician to agree to a conclusion the insurer drafted, *Knuth, supra,* 2017 WL 8941237, at *8, 10; *Rikimaru v. Unum Life Ins. Co. of Am.*, No. 19-cv-00186-LTB, 2020 WL 13505360, at *4, 8 (D. Colo. Mar. 27, 2020); (2) quoting an examiner selectively, or treating a physician's silence as agreement, *Backman, supra,* 191 F. Supp. 3d at 1069; *Hart, supra,* 253 F. Supp. 3d at 1064, 1072; (3) reliance on an unrecorded conversation between physicians, *Hart, supra,* 253 F. Supp. 3d at 1071–72; *Fleming, supra,* 2018 WL 6133859, at *5 n.2, 10; *Potthoff v. Unum Life Ins. Co. of Am.*, No. 1:24-cv-991, 2026 WL 177603, at *4–5 (W.D. Mich. Jan. 22, 2026); (4) attributing to a physician a statement made by office staff, *Logan, supra,* 2025 WL 2723542, at *5–6; Wessberg, 2024 WL 3444044, at *6–7, 17; *Fleming, supra,* 2018 WL 6133859, at *9; (5) asking a treating physician to retract an opinion, *Radmilovich, supra,* 701 F. Supp. 3d at 991; and (6) relying on a fact not in the record, *Petrusich, supra,* 984 F. Supp. 2d at 1120–21; *Carney*, 596 F. Supp. 3d at 858. The review also identified the adoption of unsourced text as a medical premise and the use of expert opinions obtained after the decision, or after suit, to support it.

covered under 'Any Occupation' coverage."[174] Unum's reviewers and claim staff have misstated the record; one court found that Unum's reading of the medical records "fabricated conflict and inconsistency where none existed."[175] Unum has terminated benefits on information it already had when it last approved them, and has withheld a reviewer's analysis until after the final decision, so that the claimant "was not able to rebut" it.[176]

D. What the Settlements Require about these Practices

Where a practice leaves a mark in the file, the settlements have a rule. Conditions must be considered together.[177] An attending physician's opinion may be rejected only for specific reasons stated in the file.[178] An independent examination should be sought when the claimant requests

---

[174] 2005 CDI Public Report, at 16. The practices of framing the question, with representative decisions, are: (1) routing a claim into a psychiatric review when disability was not claimed on that basis, *Tam, supra,* 491 F. Supp. 3d at 709; *Bencivenga, supra,* 2015 WL 1439697, at *10; *Kamerer, supra,* 334 F. Supp. 3d at 428; (2) measuring the occupation against generic demands, *Hardy v. Unum Life Ins. Co. of Am.*, No. 23-cv-563 (JRT/JFD), 2024 WL 4043540, at *12–13 (D. Minn. Sept. 4, 2024); *Logan, supra,* 2025 WL 2723542, at *15–16; *Hertan, supra,* 111 F. Supp. 3d at 1087; *Christoff v. Unum Life Ins. Co. of Am.*, No. 17-3512 (DWF/KMM), 2019 WL 4757884, at *8 (D. Minn. Sept. 30, 2019); (3) applying a physical standard to a cognitive occupation, *Brown v. Unum Life Ins. Co. of Am.*, 356 F. Supp. 3d 949, 966 (C.D. Cal. 2019); *Hardy, supra,* 2024 WL 4043540, at *15; *Doe, supra,* 35 F. Supp. 3d at 193; (4) writing into the question a condition the policy does not contain, *Jalali v. Unum Life Ins. Co. of Am.*, No. 2:20-cv-5071, 2022 WL 896785, at *9–11 (S.D. Ohio Mar. 28, 2022); *Meyer, supra,* 96 F. Supp. 3d at 1242, 1247; and (5) using forms that limit the answers a physician can give, *Jalali, supra,* 2022 WL 896785, at *9; *Dimopoulou, supra,* 162 F. Supp. 3d at 260; *Hines v. Unum Life Ins. Co. of Am.*, No. 1:18-cv-786, 2018 WL 6599404, at *4 (N.D. Ohio Dec. 17, 2018). The review also identified a vocational review that adopts the medical conclusion rather than testing it.

[175] *Christoff, supra,* 2019 WL 4757884, at *9. The practices of misrepresenting the record, with representative decisions, are: (1) treating a clearance from an unrelated specialty as evidence of capacity, *Akans v. Unum Life Ins. Co. of Am.*, No. 3:23-cv-79, 2024 WL 1200301, at *9 (E.D. Tenn. Mar. 20, 2024); *Fleming, supra,* 2018 WL 6133859, at *9; *Kaminski, supra,* 517 F. Supp. 3d at 865; and (2) mischaracterizing the claimant's evidence, *Christoff, supra,* 2019 WL 4757884, at *9; *Clarke, supra,* 852 F. Supp. 2d at 673, 681; *Hines, supra,* 2018 WL 6599404, at *6. The review also identified conduct a court has called deceptive.

[176] *MacNaughton v. Paul Revere Life Ins. Co.*, 589 F. Supp. 3d 129, 139 (D. Mass. 2022). The practices of reversing position and denying a genuine review, with representative decisions, are: (1) requiring a new finding on a measure that did not change while benefits were paid, *Lundberg v. Unum Life Ins. Co. of Am.*, No. 22-cv-2188 (ECT/DLM), 2024 WL 1461433, at *14–15 (D. Minn. Apr. 4, 2024); *Iravani, supra,* 692 F. Supp. 3d at 917, 920; (2) terminating benefits on information the insurer had when it last approved them, *Christoff, supra,* 2019 WL 4757884, at *8; *Hardy*, 2024 WL 4043540, at *16; *Iravani, supra,* 692 F. Supp. 3d at 916; and (3) withholding a reviewer's analysis until after the final decision, *MacNaughton, supra,* 589 F. Supp. 3d at 131, 139; *Johndrow v. Unum Life Ins. Co. of Am.*, No. 1:21-cv-296, 2026 WL 777232, at *14 (E.D. Tenn. Mar. 19, 2026). But see *Clarke, supra,* 852 F. Supp. 2d at 676–77 (declining to require disclosure of in-house reviews before the appeal decision).

[177] Regulatory Settlement Agreement § B.3.g.

[178] Amendment to Regulatory Settlement Agreement ¶ 5; California Settlement Agreement § III.D.

one.[179] California discontinued the self-reported-condition limitation and restricted the use of the mental and nervous limitation.[180]

Courts have found those rules broken after the settlements took effect. In *Freeland*, "[n]one of Unum's experts appeared to consider Freeland's physical and psychological co-morbidities together," and the court held: "This violated the Regulatory Settlement Agreement to which Unum is bound."[181] In *Dwyer*, the court noted that the settlement "requires that significant weight be given to opinions of attending physicians," and found that Unum's analysis "greatly discounted if not ignored outright" those opinions.[182] In *Moseley*, Unum refused an examination the claimant requested, although the settlement provides that one "should be sought whenever" the claimant asks.[183]

The practices of reasoning from assumption have no rule. Nothing in either settlement requires a reviewer to state the basis for relying on general expectations, on the intensity of treatment, or on personal experience, and nothing requires anyone to record it. The conduct statement asks employed professionals to "[p]rovide reasonable, clear, and accurate explanations of professional opinions," but it is a pledge; it binds only employees, and no one reviews compliance with it.[184] As Part IV shows, the settlements require no record of how an examiner was chosen, what the examiner was paid, or how the examiner's opinions came out.

E. An Opinion Based on Experience is Difficult to Test

An opinion based on the reviewer's experience rests on a premise the file does not contain. A reviewer who concludes that a claimant with a given condition would have sought more treatment, or would have recovered by now, is drawing on what the reviewer has seen in other patients. The claim file records the conclusion but not the experience, and nothing in the file allows the premise to be checked.

Courts have been able to test such opinions only at the edges. The claims regulation requires consultation with a professional who has "appropriate training and experience in the field of medicine involved in the medical judgment," and courts have measured reviewers against that requirement.[185] In *Boersma*, the court found "Dr. Norris's conclusory rejection of the possibility that fibromyalgia might be disabling is particularly striking, given that he is not a rheumatologist and does not have meaningful expertise in the condition."[186] In *Fleming*, the court found that "Unum has not explained how Dr. Norris had 'training and experience' in the fields of medicine" involved in

---

[179] Regulatory Settlement Agreement Ex. 6, § B.4.

[180] California Settlement Agreement §§ IV.B, IV.C.

[181] *Freeland, supra,* 2013 WL 4482995, at *12.

[182] *Dwyer, supra,* 548 F. Supp. 3d at 485, 492.

[183] *Moseley, supra,* 659 F. Supp. 3d at 90–91 (quoting Regulatory Settlement Agreement Ex. 6, § B.4).

[184] Regulatory Settlement Agreement § B.3.e & Ex. 5.

[185] 29 C.F.R. § 2560.503-1(h)(3)(iii); see *id.* § 2560.503-1(h)(3)(v).

[186] *Boersma, supra,* 546 F. Supp. 3d at 713.

the judgment.[187] Those decisions test the reviewer's credentials. They do not test whether the reviewer's experience supports the premise.

Testing the premise has required a deposition. *Dwyer* was reviewed de novo, and the court allowed the claimant to depose Dr. Norris because the reviewers' findings "go to the heart of the matter."[188] Dr. Norris's written review had treated the claimant's "infrequent fills of small amounts of antiemetic medication" and "declination to pursue additional advanced therapy" as inconsistent with the claimed symptoms.[189] Under examination, Dr. Norris testified to having treated about five patients with Meniere's disease, the last one likely in 2006 and none of them bilateral amputees; to having no doubt about the claimant's reporting of symptoms; and to having nothing to recommend "in addition to what [Plaintiff's] specialist had recommended." The court found the claimant disabled.[190]

The 2020 order that allowed the deposition also shows how narrow that route is. The court refused interrogatories on the reviewers' "approval and denial of other LTD claims in the last five years," their personnel files and performance assessments, and their compensation, holding that bias is not at issue on de novo review.[191] Most of these claims are reviewed under the deferential standard, where a deposition is the exception. In *Braun*, where the court allowed one, the merits decision was confined to the administrative record and does not mention it.[192] In *Warner*, the court ordered the reviewing physicians' compensation and performance evaluations, but refused both a count of the claims each had reviewed and denied and the five reports each wrote before and after the claimant's.[193]

Any such test also requires knowing who the reviewer is. In *Lundberg*, the denial letter did not name the reviewing physicians, and the court identified them from the administrative record: "Neither physician is identified by name in the letter."[194] In *Kaminski*, the claimant's counsel argued on appeal that the denial "conflate[d] notes and findings randomly plucked from Mr. Kaminski's 2016 medical records" without identifying their source, making it unclear whether the excerpts were "hand-picked by Unum's physicians."[195] A claimant cannot assess the qualifications or history of an unnamed reviewer, and the failure to identify the reviewer is itself a departure from the regulation's identification requirement (Part I.E).

---

[187] *Fleming, supra,* 2018 WL 6133859, at *10.

[188] *Dwyer v. Unum Life Ins. Co. of Am.*, 470 F. Supp. 3d 434, 439–40 (E.D. Pa. 2020).

[189] *Dwyer, supra,* 548 F. Supp. 3d at 484.

[190] *Id.* at 483, 490.

[191] *Dwyer, supra,* 470 F. Supp. 3d at 439–40.

[192] *Braun, supra,* 2023 WL 4205536, at *5.

[193] *Warner, supra,* 2013 WL 3874060, at *6–7.

[194] *Lundberg, supra,* 2024 WL 1461433, at *11 n.37.

[195] *Kaminski, supra,* 517 F. Supp. 3d at 848. The passage recites the claimant's appeal argument; it is not a finding.

The practices of reasoning from assumption described in Section C are therefore the hardest to examine. The file does not show the premise, and the settlements require no record of it. The evidence that could show whether a reviewer applies the premise evenly (how often the reviewer is used, what the reviewer is paid, and how the reviewer's opinions come out) is the evidence courts most often refuse. Part VI addresses those refusals.

PART VI. DISCOVERY AND UNUM'S SUPPRESSION OF EVIDENCE RELATED TO BIAS

Courts grant discovery into bias when a claimant asks about an identified reviewer and supports the request with facts already in hand. They most often refuse it when the request is put as a general inquiry into Unum's practices. Unum's objections are built to keep the request in the second category, and they work most reliably where the claimant has nothing to start from.

The orders below show both halves of that pattern, factor by factor. Courts have ordered Unum to produce a reviewer's compensation, the number of reports the reviewer prepared, the method by which the reviewer was paid, the reviewer's other opinions, the insurer's quality audits of the reviewer, and the internal targets against which claims are managed. Those orders show that the material exists and that it can be produced. Each of them was obtained by a claimant who could identify a reviewer and say something concrete about that reviewer's work, and what a claimant can say at the outset comes from other insureds' claims.[196]

A. The Administrative Record and the Threshold Showing

Judicial review of an ERISA benefit denial is confined to the administrative record. The term appears nowhere in the statute or the claims regulation. It denotes the evidence that was before the plan administrator when it decided the claim.[197] In practice, the record is a compilation the insurer assembles after the decision from a file the insurer created. Its contents depend on the insurer's choices: what was placed in the claim file, what was written down, and what was removed before production. Unum has described the last of those under oath. In *Taekman*, the declaration supporting the filing of the record stated that before a claim file is sent to a claimant, a benefit specialist reviews it and removes any documents concerning another claimant, and that settlement communications and "Alternative Resolution Team documentation" had been withheld from the record filed with the court.[198] The court thus reviews a body of evidence assembled by the party whose conduct is under review.

---

[196] The orders discussed here were entered in actions against Unum, Provident, Paul Revere and First Unum between 1997 and July 2026. They record what the parties contested and what the courts decided; requests Unum answered without a motion, and requests claimants abandoned, do not appear. No production rate is stated for that reason, and nothing here turns on a trend over time.

[197] See *Quesinberry v. Life Ins. Co. of N. Am.*, 987 F.2d 1017, 1025–27 (4th Cir. 1993) (en banc); *Tekmen v. Reliance Standard Life Ins. Co.*, 55 F.4th 951, 961 n.6 (4th Cir. 2022).

[198] On removal before production: the declaration supporting the filing of the record in *Taekman* states that before a claim file is sent to a claimant it "is reviewed by the Benefit Specialist to determine if any documents" concern another

A claimant who wants evidence outside that record must first show that the insurer's conflict of interest affected the decision.[199] The insurer's standard objection is that evaluating a reviewer's conclusions in other claimants' matters would require the court to relitigate those claims; the cases call this the mini-trial objection. Even accepted in full, the objection reaches one class of material: the reviewer's work product in other insureds' files and the outcome distribution built from it. It does not reach what the reviewer was paid and by whom, the criteria by which files were referred, the instructions sent with the referral, the insurer's own evaluations of the reviewer, or the recovery plans and reserve-based targets by which claims are managed in the aggregate. Those are facts about the insurer, and none requires inquiry into the merits of any other claim. The objection is nevertheless made to all of them.[200]

The threshold showing is where the doctrine closes. The structural conflict does not satisfy it. *Stallman* holds that "a structural conflict does not entitle a plaintiff automatically to conflict-of-interest discovery," and requires "a reasonable suspicion of misconduct."[201] The claimant's view of the merits does not satisfy it. *Jacob* holds that a termination "is not, by itself, evidence of bias," and that arguments about the weight of the medical evidence are "not appropriate to establish bias."[202]

---

claimant or are privileged, and that "[i]f such documents are located within the claim file, they are removed prior to sending the claim file to the claimant or attorney"; the same declaration states that Unum "has withheld all settlement communications and Alternative Resolution Team documentation from the Administrative Record filed with the Court," identifying the withheld material as pages UA-CL-LTD-000751 through UA-CL-LTD-000878. The claimant asked the court to strike the label "Administrative Record" from the docket entry as inaccurate. *Taekman v. Unum Life Ins. Co. of Am.,* No. 1:22cv605, 2023 WL 6460377, at *2–3 (M.D.N.C. Oct. 4, 2023) (motion to compel denied; the declaration was credited). On what enters the file and what is written down: *Shapiro, supra,* 1997 WL 601430, at *3 ("Not For File" written across a claims examiner's note and across two documents from an unrelated claim); *Hertan, supra,* 111 F. Supp. 3d 1088 n.3 ("The Administrative Record does not explain why Unum, when it was considering terminating Plaintiff's benefits and denying her appeal, did not refer the file back to Dr. Lezberg to reconsider his earlier conclusion that Plaintiff was disabled"); *Houston v. Unum Life Ins. Co. of Am.*, 246 Fed. App'x. 293, 296 (6th Cir. 2007) (summary forwarded to the reviewing physician "conspicuously omitted any reference to Unum's previous favorable conclusion"); *Bencivenga, supra,* 2015 WL 1439697, at *10 ("Unum has done its best to conceal it and indeed has not made any mention of it"); Order of the Commissioner, at 4 (substantive decisions made at roundtables the claim file did not capture). On a claimant's remedy for a suspected omission: *McCauley v. First Unum Life Ins. Co.*, 551 F.3d 126, 131 (2d Cir. 2008) (claimant identified a document missing from the record and a statement that his file had been reviewed by a physician when it had been reviewed by a nurse; the district court required a showing that the document was lost in bad faith).

[199] See *e.g.*, *Sandeen v. The Paul Revere Life Ins. Co.*, No. 1:18-cv-248, 2019 WL 13123409 (E.D. Tenn. Oct. 23, 2019).

[200] See *Jacob v. Unum Life Ins. Co. of Am.,* No. 1:19-cv-131-TRM-CHS, 2019 WL 13298916 (E.D. Tenn. Dec. 17, 2019) (conflict discovery denied in its entirety, the requests having sought recovery targets set against claim reserves and the distribution of recovery plans from vice presidents down to directors); *Gray v. Unum Life Ins. Co. of Am.,* No. EDCV 17-1778-JGB-KKx, 2018 WL 4566850, at *4 (C.D. Cal. Sept. 21, 2018).

[201] *Stallman v. First Unum Life Ins. Co.*, Civ. No. 23-20975 (JXN) (LDW), 2024 WL 4988603, at *5 (D.N.J. Dec. 5, 2024); see *id.* (quoting *Hocheiser v. Liberty Mut. Ins. Co.*, No. 17-CV-6096 (FLW)(DEA), 2018 WL 6026818, at *4 (D.N.J. Nov. 16, 2018) ("[A]bsent more, the singular fact that Liberty administers and pays claims is not by itself enough to open the door to discovery of extra-record materials.")).

[202] *Jacob v. Unum Life Ins. Co. of Am., supra*, at *4.

The disagreement between the treating physician and the file reviewer is therefore the merits, and cannot serve as the predicate, although that disagreement is present in nearly every terminated claim and is often the only thing the claimant has. What the claimant must produce is a fact from outside the file: a specific irregularity in the handling of the claim, or a fact about the reviewer, in hand before any discovery is had.[203]

Facts about reviewers reach a claimant in one way. They exist publicly where an earlier claimant compelled them. In *Boles*, an order compelling Unum to answer interrogatories on its conflict recited the reviewing physician's annual claim volume and his average annual compensation from Unum. Two days later, on Unum's emergency motion, the court restricted access to the order. One hundred and eight days after the order was entered, the motion to unrestrict was denied as moot; the case was dismissed six weeks later, and the order remains restricted.[204] Those figures are the kind of extrinsic fact the threshold requires. Sealing the order took nothing from *Boles*, who already had them. It took the predicate from every claimant who came after.

The predicate a claimant must supply in order to obtain conflict discovery is therefore the evidence that conflict discovery would produce. The rule applies to both sides, but they do not hold the same information. The insurer holds the selection records, compensation records, engagement counts, and outcome distribution. The claimant holds a denial letter.

B. The Unum bias Discovery Requests

Generally, requests regarding biased experts focus on the reviewer. Claimants ask who the reviewer is, how the reviewer was selected, what the reviewer was paid and by whom, how often the insurer has used the reviewer, how the reviewer's opinions have come out, and what the insurer does to check the reviewer's work. For employed claim staff and physicians, they ask about bonus programs, scorecards, recovery plans, and weekly reports tracking claim closures.[205]

Those requests map onto the four factors. Compensation and volume are Factor 1. The distribution of a reviewer's conclusions is Factor 2. The underlying reasons for the conclusions, the claim policies, procedures, and manuals, and the internal handling of the claim are Factor 3. Factor 4

---

[203] *Semien v. Life Ins. Co. of N. Am.*, 436 F.3d 805, 813–15 (7th Cir. 2006) (claimant must identify a specific conflict or instance of misconduct and make a prima facie showing of good cause to believe limited discovery will reveal a procedural defect), softened but not rejected in light of *Glenn* by *Dennison v. MONY Life Ret. Income Sec. Plan for Retirees*, 710 F.3d 741, 747 (7th Cir. 2013); see *Warner, supra,* 2013 WL 3874060 (threshold met on identified handling defects; five years of compensation and bonus data and the reviewing physicians' performance evaluations ordered).

[204] *Boles v. Unum Life Ins. Co. of Am.*, 4:11-cv-03031 (D. Neb.), docket entries 69–72, 88–89; *Boles*, 2013 WL 1079016 (D. Neb. Mar. 14, 2013) (denying reconsideration). The figures are set out at Part V.A, and survive publicly only because they were quoted to the Department of Labor in a comment letter on RIN 1210-AB39 three years later.

[205] See, e.g., *Gray*, *supra*, 2018 WL 4566850, at *4–6 (recovery plans and weekly tracking reports); *Clark* (D.S.D.), *supra*, 2022 WL 17251352, at *6–10, 18–21 (personnel files, compensation, goals and targets, recovery methodology, scorecards); *Chamlee v. Unum Grp. Corp.*, No. 4:21-cv-21-CLM, 2022 WL 22895707, at *3 (N.D. Ala. Aug. 22, 2022) (evaluation, compensation and incentive plans for the employees who reviewed the claim).

covers the selection criteria, the quality audits, the monitoring reports, and the insurer's periodic evaluation of its reviewers.

C. Factor 1: Compensation and Volume

Courts have ordered compensation discovery in a substantial number of these cases. *Waggener* ordered Unum to state, for each independent contractor, the number of engagements and the compensation paid.[206] *Warner* ordered five years of compensation and bonus information for three reviewing physicians, together with their performance evaluations.[207] *Smith* ordered Unum to show "whether, and in what amount," the employees who decided the claim received incentives or performance-based bonuses.[208] *Chamlee* ordered the compensation and incentive plans and performance metrics for the employees who reviewed the claim, and a deposition of Dr. Scott Norris on conflicts of interest.[209] *Zagante* ordered each outside consultant's total compensation, report count, and method of payment, "including any discounts or bonuses."[210]

Wittmann went furthest. The subpoena sought Dr. James H. Bress's total compensation from all medical work and the compensation Dr. Bress received from Unum, for 2014 through 2017. The court ordered both, with the first narrowed to a single record such as a tax return excerpt. It explained that "[t]he obvious purpose of plaintiff's two requests in combination is to establish the extent, by a percentage of his income, to which Dr. Bress is reliant for his livelihood on money he receives for providing his opinions to Unum."[211] That is the measure of financial dependence that Factor 1 describes, and a court ordered it produced once the request was framed as a comparison rather than a demand for a number. *Small* had reached the same kind of evidence in 1999 by subpoenaing the examining physician's own records of work for insurers.[212]

Unum has opposed this discovery from the earliest of these orders to the most recent. In 2003, a court refused a request for the payments Unum's corporate deponent had received from the defendants.[213] In *Akans*, Unum objected to interrogatories on the earnings and incentive targets of the physicians who reviewed the claim and stated that it did not intend to produce responsive documents. It later offered a compensation template, which the claimant said "did not confirm that each doctor did in fact receive a bonus under the plan, nor the amount." The court denied the

---

[206] *Waggener*, *supra*, 238 F. Supp. 2d at 1181, 1187–88.

[207] *Warner*, *supra*, 2013 WL 3874060, at *6.

[208] *Smith v. First Unum Life Ins. Co.*, No. 19 Civ. 00298 (NSR), 2020 WL 6281451, at *10 (S.D.N.Y. Oct. 21, 2020).

[209] *Chamlee*, *supra*, 2022 WL 22895707, at *3.

[210] *Zagante*, *supra*, 2026 WL 1413584, at *1–2; see Part V.A.

[211] *Wittmann, supra,* 2018 WL 3374164, at *2–4.

[212] *Small*, *supra*, 1999 WL 1128945, at *1–4; see Part IV.C.

[213] *Thompson v. Unum Life Ins. Co. of Am.*, No. Civ.A. 3:03-CV-0277-D, 2003 WL 22171706, at *5 (N.D. Tex. Sept. 17, 2003).

motion.[214] In *Wittmann*, Unum, rather than the physician, moved to quash the subpoena.[215] In *De Mello*, Unum argued that the amounts it paid its vendor, Dane Street, were "meaningless in isolation" and that it did not have the amounts Dane Street paid the reviewing physicians.[216]

What claimants received has often been less than what was ordered, in three ways.

First, courts separate the existence of an incentive from its size. *Schaefer* allowed discovery of incentive and bonus programs but held that Unum "need not turn over documents solely related to compensation," because the claimant had not explained "what value it would bring for her to discover the specific amounts." It applied the same limit to the vendor's personnel.[217] *Saldi* ordered payroll records for the vendor's investigators and directed that the pay information be redacted.[218]

Second, sworn summaries replace the records. In *Leung*, the claimant sought Unum's billing records and the tax forms issued to Dane Street. The court accepted a declaration stating yearly or monthly hire counts and the "total dollar amount that Defendant paid to Dane Street from 2016-2021," and added that "[n]o further production is required."[219]

Third, the vendor stands between the insurer and the reviewer. When a physician is engaged through a vendor, Unum's records show what Unum paid the vendor and nothing about what the vendor paid the physician. In *De Mello*, the court accepted Unum's statement that it lacked that information and added that the aggregate paid to the physicians "would say nothing about either doctor's dependence on work from Dane Street."[220] The comparison *Wittmann* ordered — what one source pays against the reviewer's total income — requires both figures. A claimant who can obtain neither figure from the insurer cannot calculate it. *Zagante* reached per-physician figures because the physicians were First Unum's own consultants.[221] Under the 2016 amendments described in Part I, a plan must address a vendor's practices "in the terms of its service contract and ongoing monitoring." In *De Mello*, Unum represented that it does not have access to what its vendor pays the physicians who review Unum's claims.[222]

D. Factor 2: the Reviewer's Outcomes

Courts have ordered outcome material where the request identified the reviewers and a defined class of claims. *Bronner* ordered statistics on heart attack claims for 2001 through 2004, although

---

[214] *Akans v. Unum Life Ins. Co. of Am.*, No. 3:23-cv-79-TRM-JEM, 2023 WL 12051358, at *2, 4–5 & n.6 (E.D. Tenn. Oct. 26, 2023).

[215] *Wittmann*, *supra*, 2018 WL 3374164, at *1.

[216] *De Mello v. First Unum Life Ins. Co.*, No. 25-cv-7933 (LJL), 2026 WL 2032059, at *2 (S.D.N.Y. July 14, 2026) (describing Unum's opposition).

[217] *Schaefer v. Unum Life Ins. Co. of Am.*, No. 4:24-CV-00590, 2026 WL 396445, at *4–5, 7 (M.D. Pa. Feb. 12, 2026).

[218] *Saldi*, *supra*, 224 F.R.D. at 191–92.

[219] *Leung*, *supra*, 2023 WL 4056041, at *7.

[220] *De Mello*, *supra*, 2026 WL 2032059, at *4.

[221] *Zagante*, *supra*, 2026 WL 1413584, at *1.

[222] 81 Fed. Reg. at 92,320; *De Mello*, 2026 WL 2032059, at *4.

Unum submitted a declaration that it did not keep the information in the statistical form requested.[223] In *Kelly*, Unum disclosed the number of examinations two physicians had performed, and the court ordered the production of their reports for 2005 through 2009, allowing the claimant "to decipher the 'outcomes'" of those examinations.[224] *Clark* ordered three staff physicians' opinions on pulmonary embolism claims over Unum's objection that reviewing them would require "a series of mini-trials"; the court found the request "clearly relevant" and limited it by condition and by date.[225] *Small* ordered the examining physician's records of examinations performed for insurers since 1990, redacted to show only the insurer, the analysis, and the recommendation.[226]

Where the request was put in general terms, it has been refused. Courts have declined to order per-reviewer counts and ratios (*Schaefer*), statistical summaries and the reviewers' other reports (*Warner*), denial and termination rates and the lawsuits alleging biased decisions by the decision makers (*Smith*), counts of claims found supported (*Choi*, *Akans*), and the number of claims denied within six months of each reviewer's review (*De Mello*).[227] In *Mercer*, the claimant asked for the evaluative files of Unum's reviewing physicians and cited an earlier case in which such files had been produced. The court declined to follow that order because it "contains no reasoning."[228]

The stated reason for those refusals is that a denial rate cannot show that any particular denial was wrong without a trial of that claim. Claimants do not offer the rate for that purpose. Outcome and volume figures are not offered to prove bias by themselves. They are among the factors from which a court decides whether an opinion is likely to have been procured rather than reached. *Demer* is the clearest statement of the point. The claimant there showed that two independent physician consultants had earned $125,000 to $175,000 a year from the insurer and had performed 200 to 300 reviews and addenda a year, and the Ninth Circuit held that "[t]he magnitudes of these numbers, particularly when combined, raise a fair inference that there is a financial conflict which influenced the IPCs' assessments." Because the claimant "did provide evidence of a financial conflict warranting an inference of bias, the burden shifted to MetLife to counter that evidence."[229] The court added that it is "not hard to imagine an outside medical examiner who does not engage in

---

[223] *Bronner v. Unum Life Ins. Co. of Am.*, No. 5:03-cv-05742 JF (RS), 2009 WL 248175, at *5 (N.D. Cal. Jan. 30, 2009).

[224] *Kelly*, *supra*, 2010 WL 3259997, at *3.

[225] *Clark* (D.S.D.), *supra*, 2022 WL 17251352, at *21–22; see Part V.A.

[226] *Small*, *supra*, 1999 WL 1128945, at *4. In *Small*, the court noted that the records were generated for the purpose of evaluating the medical condition of patients for third-parties and for the preparation of civil litigation, not the result of private medical examinations or that of a treating doctor-patient relationship, and thus, "any non-party privacy expectations in the contents of such non-therapeutic medical reports prepared only for the purpose of preparation for civil litigation, or for determining one's eligibility for insurance benefits, clearly enjoys a somewhat reduced expectation of privacy." *Id.*, at *3.

[227] *Schaefer*, *supra*, 2026 WL 396445, at *4, 7; *Warner*, *supra*, 2013 WL 3874060, at *6–7; *Smith*, *supra*, 2020 WL 6281451, at *10–11; *Choi*, *supra*, 2025 WL 2234903, at *6; *Akans*, *supra*, 2023 WL 12051358, at *2, 4–5; *De Mello*, *supra*, 2026 WL 2032059, at *4.

[228] *Mercer v. Unum Life Ins. Co. of Am.*, No. 3:22-CV-00337, 2023 WL 3131989, at *2–3 (M.D. Tenn. Apr. 27, 2023).

[229] *Demer, supra,* 835 F.3d at 902–03; see Part I (Factors 1 and 2).

a neutral, independent review, such as where the examiner receives hundreds of thousands of dollars from a single source and performs hundreds of reviews for that source every year," and that statistics "showing a parsimonious pattern of assessments disfavorable to claimants" would have been more powerful evidence still: their absence reduced the weight given to the conflict, but "that lack of such specific evidence does not mean that there is no conflict of interest."[230] In *Chacko*, the court verified a tabulation of a reviewer's conclusions against the reviewer's own conclusion pages, without trying any other claim.[231] Neither court treated the numbers as proof of bias standing alone, and neither needed a trial of any other claim to use them.

Those orders show that outcome evidence exists and can be produced. It reaches later claimants only if a court's order or a party's filing puts it on the public record. In *Mercer* and *Akans*, the claimants relied on an account, drawn from discovery in another case, that one Unum physician had supported termination in 98 percent of the claims that physician was asked to evaluate. The *Akans* court treated the showing as "conclusory."[232]

E. Factor 3: Procedural Irregularities

Part V described the irregularities that appear in the decisions. The discovery orders show Unum resisting discovery of the internal practices that produce them: recovery plans, weekly tracking reports, claim-closure targets, and the manuals and training that govern the handling of a claim.

In *Gray*, Unum asserted that no recovery plans were used on the claim. The court ordered the weekly tracking reports, the unit's communications about recovery plans, and a Rule 30(b)(6) deposition on how recovery plans are set and communicated, holding that it "cannot rely on Defendant Unum's conclusory objections."[233] *Clark* ordered documents on goals, targets and the methodology for calculating expected recoveries.[234] *Jacob* and *Choi* denied the same kind of discovery, and in *Choi* the court drew only the "fairly unremarkable" inference that an insurer keeps data on claim openings and terminations.[235] In *Stallman*, Unum's admitted use of weekly tracking reports was "insufficient on its own to raise a reasonable suspicion of misconduct."[236] In the same district as *Akans*, testimony by a Unum vice president about weekly tracking reports had been

[230] *Id.* at 903–04. The court also noted that the insurer "could have maintained records of its reviewers' findings on claims to show their neutrality in practice, but it did not," and so "missed an opportunity to negate any inference of a financial conflict of interest." *Id.* at 903.

[231] *Chacko, supra,* 690 F. Supp. 3d at 1150–51; see Part VII.F.

[232] *Mercer*, *supra*, 2023 WL 3131989, at *2; *Akans*, *supra*, 2023 WL 12051358, at *3 & n.5.

[233] *Gray*, *supra*, 2018 WL 4566850, at *4–6.

[234] *Clark* (D.S.D.), *supra*, 2022 WL 17251352, at *10, 19.

[235] *Jacob*, *supra*, 2019 WL 13298916, at *4, 7; *Choi*, *supra*, 2025 WL 2234903, at *4.

[236] *Stallman*, *supra*, 2024 WL 4988603, at *6.

found sufficient to open the door to discovery in other cases, which is the difference between an assertion about the reports and evidence about them.[237]

Some of these practices leave no document. In *Clark*, a claims supervisor testified that the team's performance was measured against a recovery plan, "a count of recoveries and a dollar figure," but that the numbers were passed on orally. The court concluded that "even crediting Peter's testimony wholly, there would be no documents showing this practice," and denied the request.[238] The same court later observed that reserve-setting "was discussed orally and not in writing."[239]

Discovery of claim manuals and training has usually been confined to the claimant's own file. *Allen* limited production to the rules and guidelines used on the claim, because the claimant was "not entitled to broad discovery into Defendants' general claims handling practices."[240] *Smith* limited training materials to those bearing on the policy terms at issue.[241] *D'Aprile* held that, under Florida law, discovery of claims-handling practices must await a ruling on coverage.[242] In the second *Kelly* order, the court held that a Unum executive's knowledge from her earlier years as house counsel was "not relevant to the issues in this case considering that Defendants entered into a Regulatory Settlement Agreement."[243]

Factor 3 also determines whether any other discovery is allowed. The District of New Jersey looks for "indicia of procedural irregularity, such as unexplained reversals of position, selective reliance on evidence, or failure to conduct a full and fair review."[244] In *Braun*, the claimant met that test by assembling published decisions criticizing the reviewer, and obtained the deposition.[245] In *De Mello*, the court held that criticisms of the reviewers' reports, although "couched in the language" of irregularities, were disagreements with the merits.[246] The irregularities must therefore be shown from the administrative record, which Section A above explains is compiled by Unum, or from decisions in other insureds' cases.

F. Factor 4: Selection and Oversight

Selection is the subject courts most consistently confine to the claimant's own file. In *Saldi*, the court denied discovery of Paul Revere's "practice of hiring biased independent medical examiners"

---

[237] *Akans*, *supra*, 2023 WL 12051358, at *4 (distinguishing *Olah* and *Mitchell*, in which the court had relied on that testimony).

[238] *Clark* (D.S.D.), *supra*, 2022 WL 17251352, at *9.

[239] *Id.* at *18.

[240] *Allen v. First Unum Life Ins. Co.*, No. 2:18-cv-69-FtM-29MRM, 2020 WL 6882169, at *13 (M.D. Fla. Sept. 30, 2020).

[241] *Smith*, *supra*, 2020 WL 6281451, at *9.

[242] *D'Aprile v. Unum Life Ins. Co. of Am.*, No. 2:09-cv-270-FtM-36SPC, 2010 WL 3340197, at *2–3 (M.D. Fla. Aug. 25, 2010).

[243] *Kelly, supra,* 2010 WL 5300807, at *2. The court dated the Regulatory Settlement Agreement to November 2005.

[244] *Stallman v. First Unum Life Ins. Co.*, No. 23-20975 (JXN) (LDW), 2025 WL 3749611, at *4 (D.N.J. Dec. 29, 2025).

[245] *Braun*, *supra*, 2022 WL 17740459, at *2–3; see Part V.A.

[246] *De Mello*, *supra*, 2026 WL 2032059, at *4 (quoting *Choi*, *supra*, 2025 WL 2234903, at *6).

because no independent examiner had been hired on the claim. However, the order allowed discovery of Unum's quality assurance program and the criteria used for monitoring the activities, quality and cost for internal staff and outside vendors, and other performance standards. The same order also allowed extensive discovery of the vendor, Genex, including the criteria for referring files and "Genex's interest in saving money for its clients," because Genex had handled the claim.[247]

In *Bronner*, the court refused a request to admit that Unum regularly used a particular cardiologist as a reviewer, because it sought "information not related solely to Bronner's claim."[248] In *Kelly*, a Rule 30(b)(6) topic on the criteria for selecting examiners was treated as answered by testimony about the period in which the two examiners at issue were hired.[249] *Waggener*, in 2002, is the order that reached selection generally, requiring Unum to produce documents on the "general selection of physicians for Independent Medical Examinations."[250]

Requests for Unum's measures to prevent or detect bias have fared the same way. In *Smith*, the court denied the request for "any steps that Unum may have taken to reduce potential bias and/or to promote accuracy." It reasoned that the request reached measures "without regard to whether that measure played any role in the determination to deny Plaintiff's benefits claim," such as "measures taken by Unum to prevent conflicts in retaining medical consultants to assess disability claims."[251] In *Kamerer*, the court denied discovery of Unum's efforts to mitigate the effects of its structural conflict, while allowing a two-hour deposition of the physician whose public comments suggested he "may favor insurers and employers."[252] In *Leung*, the court denied the claimant's requests for the quality instruments named in Unum's Statement of Work with its vendor, and whether those documents exist was never determined (Part VII.D).[253]

Where claimants did obtain discovery of Unum's oversight, it showed little. In *Kelly*, the only recorded evaluation of the two examiners concerned turnaround time and report length.[254] *Allen* ordered the results of Unum's Medical Quality Audit Program for any medical professional who reviewed the claim.[255] What an insurer forgoes by keeping no such record is set out in *Demer*.[256]

Under *Glenn*, a conflict should prove less important where the administrator "has taken active steps to reduce potential bias and to promote accuracy."[257] Several requests track *Glenn* in terms.

---

[247] *Saldi*, *supra*, 224 F.R.D. at 185, 197.

[248] *Bronner*, *supra*, 2009 WL 248175, at *5.

[249] *Kelly*, *supra*, 2010 WL 3259997, at *2–3.

[250] *Waggener*, *supra*, 238 F. Supp. 2d at 1181, 1187–88.

[251] *Smith*, *supra*, 2020 WL 6281451, at *12.

[252] *Kamerer v. Unum Life Ins. Co. of Am.*, 251 F. Supp. 3d 349, 352–53 (D. Mass. 2017).

[253] *Leung*, *supra*, 2023 WL 4056041, at *8–9.

[254] *Kelly*, *supra*, 2010 WL 3259997, at *3.

[255] *Allen*, *supra*, 2020 WL 6882169, at *15–16.

[256] *Demer*, *supra*, 835 F.3d at 903. See Part IV.G.

[257] *Glenn*, *supra*, 554 U.S. at 117.

In *Smith*, the claimant asked for documents on any steps Unum had taken to reduce potential bias and promote accuracy on the part of its decision makers.[258] In *Braun*, the deposition topics included the "steps [Unum] has taken to reduce bias and promote accuracy."[259] Those are the measures that, under *Glenn*, reduce the weight a conflict carries.

Unum asks courts to weigh its conflict lightly on the strength of its settlement, its regulators' statements and its policies.[260] In *Stallman* and *De Mello*, the courts had before them Unum's statements that its compensation programs do not reward claim outcomes, and denied further discovery without the records that would test those statements.[261] In *Smith*, *Kamerer* and *Leung*, Unum opposed discovery of what its measures are. Part VII examines the measures Unum relies on.

The instruction that accompanies a referral is a further gap. In *Hangarter*, the letter retaining the examiner carried the insurer's own conclusion.[262] Across the orders discussed here, claimants have sought Unum's general expectations of its vendors,[263] the quality instruments in a vendor contract, and the information available to reviewers on the claim system,[264] but in none of the orders reviewed here has a claimant sought the instructions that accompany Unum's referrals to reviewers across claims, as distinct from the referral in the claimant's own file.

G. The objections Unum raises

Unum's objections fall into four groups. Each has been accepted by some courts and rejected by others, and each is directed at keeping the inquiry general.

(1) The Threshold Showing. Section A above described the requirement that a claimant show, before discovery, that conflict affected the decision. Courts applying it acknowledge the difficulty. One court, quoting an earlier decision, observed that a claimant required to make a full good-cause showing "would be faced with a vicious circle: To obtain discovery, he would need to make a showing that, in many cases, could be satisfied only with the help of discovery."[265] The same court then denied every request before it.[266] Courts hold that "[t]he mere fact that an insurer both evaluates and pays claims does not, standing alone, warrant

---

[258] *Smith, supra,* 2020 WL 6281451, at *5.

[259] *Braun*, *supra*, 2022 WL 17740459, at *3.

[260] See *Braun*, *supra*, 2023 WL 4205536, at *7; *Warner*, *supra*, 2013 WL 3874060, at *3–4; *Stallman*, *supra*, 2025 WL 3749611, at *4.

[261] *Stallman*, *supra*, 2025 WL 3749611, at *4; *De Mello*, *supra*, 2026 WL 2032059, at *2.

[262] See Part II; *Hangarter*, *supra*, 373 F.3d at 1011.

[263] *Saldi*, *supra*, 224 F.R.D. at 190.

[264] *Leung*, *supra*, 2023 WL 4056041, at *8–9; *Zagante*, *supra*, 2026 WL 1413584, at *2.

[265] *De Mello*, *supra*, 2026 WL 2032059, at *3 (quoting *Anderson v. Sotheby's Inc. Severance Plan*, No. 04 Civ 8180 (SAS) (DFE), 2005 WL 6567123, at *6 (S.D.N.Y. May 13, 2005)).

[266] *Id.* at *1, 5.

conflict-of-interest discovery."[267] They also hold that the claimant's disagreement with the reviewer's opinion is not enough, because that disagreement is "inherent in every challenge under ERISA to the denial of benefits."[268]

Unum's own history has not satisfied the requirement either. In *Choi*, the court called the claimant's reliance on Unum's pre-settlement practices "outdated information."[269] In *Stallman*, the court was "not convinced that First Unum's entry into the [Regulatory Settlement Agreement] some twenty years ago creates a reasonable suspicion" that the claim decision was affected by a conflict.[270] The settlement that courts treat as too old to support discovery is the same settlement that, in *Braun*, persuaded the court that the conflict had been addressed.[271]

Where a claimant cannot make the showing, Unum's own statements fill the gap. In *Stallman*, the court "appropriately weighed Defendant's sworn representation that claims personnel are not evaluated or compensated based on claim outcomes."[272] In *De Mello*, the court noted that Unum "represents, without contradiction," that it does not have access to what its vendor paid the reviewing physicians.[273] In *Taekman*, a sworn declaration that the administrative record contained everything Unum considered was one of the grounds on which the court denied the claimant's second motion to compel.[274] In each case the representation was accepted without the records that would test it.

(2) The Statistics and the Mini-Trial. Unum's second objection is that a reviewer's denial rate means nothing, because showing that any particular denial was wrong would require a trial of that claim. In *De Mello*, as the court summarized Unum's position, the requested counts had "no statistical value with respect to the question of alleged financial bias" and "would require manual review of all the claims files."[275] The court agreed that "[b]are numbers or percentages of claim denials are meaningless without additional context—and that context cannot be provided without holding mini-trials on the other claims."[276] *Schaefer*, *Warner*, *Choi* and *Akans* reached the same result.[277] Section D sets out the answer: the numbers are

---

[267] *Stallman, supra,* 2025 WL 3749611, at *4 (affirming *Stallman*, *supra*, 2024 WL 4988603). See also *Jacob*, *supra*, 2019 WL 13298916, at *4 (requiring "a threshold evidentiary showing that this structural conflict of interest infected the insurance company's decision making").

[268] *De Mello*, *supra*, 2026 WL 2032059, at *4; see *Choi*, *supra*, 2025 WL 2234903, at *6.

[269] *Choi*, *supra*, 2025 WL 2234903, at *4.

[270] *Stallman*, *supra*, 2024 WL 4988603, at *6.

[271] See Part V.A; *Braun*, *supra*, 2023 WL 4205536, at *7.

[272] *Stallman*, *supra*, 2025 WL 3749611, at *4.

[273] *De Mello*, *supra*, 2026 WL 2032059, at *4.

[274] *Taekman, supra,* 2023 WL 6460377, at *8–9.

[275] *De Mello*, *supra*, 2026 WL 2032059, at *2 (describing Unum's opposition).

[276] *Id.* at *4 (quoting *Hughes v. Hartford Life & Accident Ins. Co.*, 507 F. Supp. 3d 384, 399 (D. Conn. 2020)).

[277] *Schaefer*, *supra*, 2026 WL 396445, at *4; *Warner*, *supra*, 2013 WL 3874060, at *6–7; *Choi*, *supra*, 2025 WL 2234903, at *6; *Akans*, *supra*, 2023 WL 12051358, at *4–5.

not offered to prove bias by themselves, and *Demer* and *Chacko* show courts using them as one factor among several without trying any other claim.

The objection is also applied at both ends. The statistics are refused because they lack the context the files would supply. The files are refused because producing them is too burdensome. In *Warner*, the court refused both the statistical summary and the five reports each reviewer wrote before and after the claimant's.[278] In *Mercer*, Unum supported its burden objection with a paralegal's estimate that reviewing one physician's evaluative files would take more than 300 hours, and the court denied production.[279] Where a claimant narrowed the request to a condition and a period, the objection failed: *Clark* ordered the opinions produced.[280] Unum and its trade association made arguments of the same kind to the Department of Labor in 2016: that a reviewer's reputation for outcomes cannot be measured, and that a high volume of denials can have innocent explanations. The Department kept the rule.[281]

(3) The Standard of Review. Unum's third objection is that bias does not matter when the court decides the claim afresh. In *Taekman*, Unum argued that the claimant's requests "may arguably relate to bias and conflict of interest for purposes of reviewing a claim decision for abuse of discretion but have no application to a de novo review."[282] In *Hardy*, the court accepted a similar argument, reasoning that even if the file had been reviewed by an employee with "a malign or corrupt attitude," de novo review would remove "such an employee's subjective attitude" from the analysis.[283] *Dwyer* and *Akans* also denied reviewer discovery on de novo review.[284]

The reasoning assumes that the court can weigh the reviewer's opinion without knowing anything about the reviewer. A court deciding a claim de novo still has to decide how much weight to give each medical opinion in the record. *Waggener*, also decided de novo, ordered discovery of "information regarding the independence or neutrality of the physicians utilized by Unum for medical opinions relative to Waggener's disability claim."[285] *Kamerer* allowed a deposition of an examining physician because the testimony "would aid the court in determining his credibility, and

---

[278] *Warner*, *supra*, 2013 WL 3874060, at *6–7.

[279] *Mercer*, *supra*, 2023 WL 3131989, at *3.

[280] *Clark* (D.S.D.), *supra*, 2022 WL 17251352, at *21–22; see Section C.

[281] Comment of Unum Group on RIN 1210-AB39, at 10 (Jan. 19, 2016); Comment of America's Health Insurance Plans on RIN 1210-AB39, at 9 (Jan. 19, 2016); 81 Fed. Reg. at 92,320. Part VII.F sets out the comments and the Department's response.

[282] *Taekman v. Unum Life Ins. Co. of Am.*, No. 1:22cv605, 2023 WL 4763724, at *7 (M.D.N.C. July 26, 2023) (quoting Unum's memorandum).

[283] *Hardy v. Unum Life Ins. Co. of Am.*, No. 23-cv-563 (JRT/JFD), 2023 WL 4841952, at *3 (D. Minn. July 28, 2023).

[284] *Dwyer*, *supra*, 470 F. Supp. 3d at 439–40; *Akans*, *supra*, 2023 WL 12051358, at *3–5.

[285] *Waggener*, *supra*, 238 F. Supp. 2d at 1187.

the appropriate weight to be given to his opinions."[286] The two lines of authority cannot both be right.

(4) Unsupported and Boilerplate Objections. Courts have repeatedly found Unum's objections unsupported, and in one case observed that interposing them to insulate discoverable material "appears to be a fairly typical practice for Unum." Section H sets out those findings.[287]

Taken together, the objections are answerable. They have been answered in these very cases, by claimants who identified the reviewer, tied the request to the reviewer's work on their own claim, narrowed it by condition and period, and supported it with what earlier decisions had already said about that reviewer.

H. Unum's Post-Production Response

Unum's response to an order compelling bias discovery has been consistent across the period this Part covers. In *Boles*, it moved on an emergency basis two days after the order issued, obtained an order prohibiting publication, asked the court to strike its own "broad accusatory statements about [Unum's] culture and claims practices," opposed the claimant's motion to make the order public, and settled while the restriction stood; the order remains restricted today.[288] In *Wittmann*, Unum — not the physician — moved to quash a subpoena to a reviewing physician who had raised no objection of his own, on what the court found to be "conclusory and unsupported assertions."[289] In *Taekman*, it sought an order that "[t]he Parties will not conduct any depositions," which the court denied, observing that "an attorney's unsworn argument does not constitute evidence."[290] In *Schaefer*, the court deemed eight general objections waived as "interposed in an attempt to insulate from discovery a large quantity of material that includes otherwise discoverable material," and observed that "it appears that this is a fairly typical practice for Unum."[291] In *Gray*, the court held Unum's boilerplate improper where it had "failed to submit any evidentiary declarations supporting such objections."[292] And in 2016 Unum asked the Department of Labor to delete the only federal provision addressed to the selection of reviewers (Part VII.F).

---

[286] *Kamerer*, *supra*, 251 F. Supp. 3d at 353; see Section E.

[287] See note 290.

[288] See notes 136–140 and 314.

[289] *Wittmann*, *supra*, 2018 WL 3374164, at *1, 3.

[290] *Taekman, supra,* 2023 WL 4763724, at *3, 7, 10.

[291] *Schaefer, supra,* 2026 WL 396445, at *3 & n.27. *Schaefer* also held that documents Unum designated under Rule 33(d) "must in fact contain the answer to the interrogatory." *Id.* at *3.

[292] *Gray, supra,* 2018 WL 4566850, at *4.

What is produced does not survive the case. Every production described in this Part was made under a protective order or a confidentiality agreement.[293] Most of the actions in which bias discovery was ordered then ended without a decision on the merits. Of the twelve such actions whose dockets are available, eight were settled or dismissed by stipulation, four of them within four months of the order.[294] *Gray* settled thirty-nine days after the order, before the extended deadline for completing the discovery it required. *Bronner* ended by stipulated dismissal one hundred and seventeen days after the order, following Unum's protective order and its filing of documents under seal. *Clark* ended one hundred and eight days after the order. In *Boles*, the court denied the motion to unrestrict as moot one hundred and eight days after the order, and judgment of dismissal followed on June 5, 2013.[295]

Four of the twelve reached a decision on the merits. *Waggener* was tried to the court on the administrative record, and judgment was entered for the claimant in 2005.[296] In *Allen*, a jury returned a verdict for Unum, and the Eleventh Circuit affirmed.[297] In *Braun*, the court granted summary judgment to Unum in an opinion that does not mention the deposition it had ordered.[298] In *Leung*, Unum obtained summary judgment on the bad faith claim, the court holding that a

---

[293] See, e.g., *Zagante*, *supra*, 2026 WL 1413584, at *1 (production "after execution of an appropriate confidentiality agreement"); *Wittmann*, *supra*, 2018 WL 3374164, at *4; *Leung*, *supra*, 2023 WL 4056041, at *7; *Gray*, *supra*, 2018 WL 4566850, at *4–6; *Bronner*, *supra*, No. 5:03-cv-05742, ECF No. 140.

[294] *Small*, *Bronner*, *Kelly*, *D'Aprile*, *Boles*, *Gray*, *Smith* and *Clark* (D.S.D.), ended in settlement or stipulated dismissal. Order Dismissing Action with Prejudice Pursuant to Local Rule 41.1(b), *Small*, *supra*, No. 2:98-cv-02934 (E.D. Pa. Nov. 15, 2001), ECF No. 79; Stipulation and Order re Dismissal with Prejudice, *Bronner*, *supra*, No. 5:03-cv-05742 (N.D. Cal. May 27, 2009), ECF No. 157; Order Dismissing Case, *Kelly*, *supra*, No. 1:09-cv-00070 (D. Vt. June 29, 2011), ECF No. 274 (entered a month after the court denied Unum's motions for judgment as a matter of law on the bad faith and punitive damages claims, Minute Entry, *id.* (May 25, 2011), ECF No. 269; no verdict appears on the docket); Joint Notice of Settlement, *D'Aprile*, No. 2:09-cv-270 (M.D. Fla. Apr. 25, 2011), ECF No. 197 (four weeks after the claimant won partial summary judgment, Order, *id.* (Mar. 30, 2011), ECF No. 195); Text Order, *Boles*, *supra*, No. 4:11-cv-03031 (D. Neb. May 10, 2013), ECF No. 89; Notice of Settlement, *Gray*, *supra*, No. 5:17-cv-01778 (C.D. Cal. Oct. 30, 2018), ECF No. 55; Order, *Smith*, *supra*, No. 7:19-cv-00298 (S.D.N.Y. Mar. 10, 2023), ECF No. 63 (the court having been advised that the case had settled; discovery was completed in 2021, Memo Endorsement, *id.* (May 12, 2021), ECF No. 58); Stipulation of Dismissal with Prejudice, *Clark v. Unum Grp.*, *supra*, No. 4:20-cv-04013 (D.S.D. Mar. 16, 2023), ECF No. 129. In *Small*, *supra*, the dismissal followed further disputes over compliance with the order and over the confidentiality of documents produced under a later order. Order, *id.* (Feb. 23, 2001), ECF No. 78.

[295] Order, *Gray*, *supra*, No. 5:17-cv-01778 (C.D. Cal. Oct. 10, 2018), ECF No. 53 (extending the deadline for the ordered discovery to November 16, 2018); Order Granting Motion for Protective Order, *Bronner*, No. 5:03-cv-05742 (N.D. Cal. Mar. 2, 2009), ECF No. 140; Order Allowing Documents to Be Filed Under Seal, *id.* (Mar. 9, 2009), ECF No. 143; see Part V.A (*Boles*).

[296] Findings of Fact and Conclusions of Law, *Waggener v. Unum Life Ins. Co. of Am.*, No. 3:02-cv-00695 (S.D. Cal. Apr. 28, 2005), ECF No. 84; Clerk's Judgment, *id.* (May 2, 2005), ECF No. 86.

[297] Jury Verdict, *Allen v. First Unum Life Ins. Co.*, No. 2:18-cv-69 (M.D. Fla. Mar. 29, 2022), ECF No. 243; Opinion and Order, *id.* (Mar. 20, 2023), ECF No. 291 (denying renewed motion for judgment as a matter of law); *Allen v. First Unum Life Ins. Co.*, No. 23-11039, 2025 WL 289490 (11th Cir. Jan. 24, 2025) (per curiam) (unpublished).

[298] *Braun*, *supra*, 2023 WL 4205536; Minute Entry, *Braun*, *supra*, No. 1:22-cv-01223 (N.D. Ill. Dec. 16, 2022), ECF No. 31. The claimant noticed an appeal. Notice of Appeal, *id.* (July 24, 2023), ECF No. 54.

genuine dispute existed because five physicians supported Unum's position, "only one of whom is alleged to have been dishonestly selected"; two of the five had been retained after the lawsuit was filed, and five months earlier the court had refused the claimant's requests for the quality-assurance documents identified in Unum's contract with the vendor that supplied one of those physicians.[299]

Actions in which discovery was denied were also settled. *Jacob* gave notice of settlement on the day discovery was denied, and *Choi* and *Stallman* settled after mediation and a settlement conference.[300] Nothing in these dockets shows why any case settled, and no such inference is needed. What they show is that the material a court orders Unum to produce seldom reaches a decision in which it is weighed, and never reaches anyone else.

The underlying claim files are therefore the mechanism. A claimant who can identify a reviewer, say what the reviewer was paid or how the reviewer's other opinions came out, and tie that to the handling of the claim will often get the discovery, as these orders show. What a claimant can say at the outset comes from other insureds' claims: the reports a reviewer wrote, the conclusions reached, the figures a court recited in an order that survived, and the decisions that followed. If the files those facts come from are destroyed, the first request fails, and everything that depends on it fails with it.

PART VII. UNUM'S THREE ARGUMENTS OPPOSING CONFLICT DISCOVERY

When a claimant seeks discovery of bias, or a court weighs Unum's conflict of interest, Unum has pointed to three things: statements by the New York Insurance Department that it complied with the settlement, its record of winning disability litigation, and its quality assurance function. Each is offered as a reasonable measure under Factor 4, the kind of "active steps to reduce potential bias and to promote accuracy" that, under *Glenn*, reduce the weight a conflict carries.[301] None of the three examines how a reviewer is selected, instructed, or paid, or how a reviewer's opinions come out. None of the three addresses the use of biased examiners, which is the conduct the settlements were entered to remedy.

A rule against selecting reviewers for their outcomes cannot enforce itself. As long as the insurer decides who receives the assignments, and the reviewer expects future income from them, compliance cannot be verified from inside the relationship. Such a rule can be enforced only where the selection leaves a record that can be inspected. Parts IV and VI describe what happens when it does not.

---

[299] *Leung, supra,* 2023 WL 7351581, at *16; *Leung*, *supra*, 2023 WL 4056041, at *8–9; see Section E.

[300] Notice of Settlement, *Jacob*, *supra*, No. 1:19-cv-00131 (E.D. Tenn. Dec. 17, 2019), ECF No. 34; Order Administratively Terminating Action Pending Consummation of Settlement, *Choi*, *supra*, No. 2:24-cv-06338 (D.N.J. Feb. 19, 2026), ECF No. 34; Order Administratively Terminating Action Pending Consummation of Settlement, *Stallman*, *supra*, No. 2:23-cv-20975 (D.N.J. Mar. 16, 2026), ECF No. 43.

[301] *Glenn*, *supra*, 554 U.S. at 117; see Part I.

A. Qualifications in Place of Bias

The three answers share a pattern that appears throughout the litigation. A claimant asks whether an opinion was procured; the insurer answers with the reviewer's credentials, its own record, or its procedures.

The pattern appears in the discovery orders. In *Warner*, Unum agreed to produce the reviewing physicians' qualifications and employment history, and opposed producing their compensation, their performance evaluations and any count of the claims they had denied.[302] In *Taekman*, Unum argued that "the signature blocks on the physicians' reports . . . are sufficient to demonstrate their credentials and the medical specialties in which they are board certified."[303] In *Braun*, Unum described the claimant's showing as one that "simply disparages Dr. Norris, professes that he is wrong on the medical merits, and demands a deposition."[304] Credentials say who the reviewer is. They say nothing about how the reviewer came to be chosen or what the reviewer has reason to conclude.

B. The New York Insurance Department's Statements

Unum has cited statements by the New York Insurance Department to argue that it complied with the settlement, made changes in its claims administration procedures required by that settlement, and is no longer engaging in any wrongful conduct.[305] In *Warner*, the court observed that "Unum apparently suggests that it should be afforded a clean bill of health with respect to claims administration." It declined to give one. "Without determining when Unum should be liberated from the cloud of its previous conduct," the court held that Unum's history warranted scrutiny of the conflict in that case.[306] The Southern District of New York reached the same result in *Tretola*: "the Court cannot take for granted First Unum's claim to have mended its ways."[307]

The statements made by the New York Insurance Department do not support the inference Unum draws from them. A statement that a company complied with a settlement is a statement about the settlement's requirements. Part IV showed that the settlements required no record of how a reviewer was selected or instructed, what a reviewer was paid, or how a reviewer's opinions came out, and that the follow-up examinations measured whether procedures were followed. A regulator certifying compliance with those instruments had no occasion to examine bias in the selection or use of reviewers, and the statements Unum cites do not say that it did. The settlements were

---

[302] *Warner*, *supra*, 2013 WL 3874060, at *5–7.

[303] *Taekman*, *supra*, 2023 WL 6460377, at *10 (quoting Unum's brief).

[304] *Braun*, *supra*, 2022 WL 17740459, at *3; see Part V.A.

[305] See e.g., *Warner, supra,* 2013 WL 3874060, at *3, *Murphy v. First Unum Life Ins. Co.*, No. 15-CV-820 (SJF)(SIL), 2016 WL 526243, at *5 n. 1 (E.D.N.Y. Feb. 9, 2016); *Mercado v. First Unum Life Ins. Co.,* No. 11 Civ. 4272 (RMB)(RLE), 2013 WL 633100, at *27 (S.D.N.Y. Feb. 21, 2013); *Kamerer, supra,* 251 F. Supp. 3d at 352.

[306] *Warner*, *supra*, 2013 WL 3874060, at *3–4.

[307] *Tretola v. First Unum Life Ins. Co.*, No. 13 Civ. 231 (PAE), 2013 WL 2896804, at *3 (S.D.N.Y. June 13, 2013); see *Murphy, supra,* 2016 WL 526243, at *5 (quoting *Tretola*).

entered to address bias in the handling of claims. The New York statements, as Unum has described them, do not mention it.

The statements are also offered without the examinations behind them. In *Bronner*, the court required Unum to produce "not only the final results of the multistate investigation, but also the documents that led to those findings."[308] A claimant who cannot see the examination cannot test what the statement means.

A claimant also cannot use the settlement against Unum. In *Gray*, the claimant sought a Rule 30(b)(6) deposition on whether Unum's handling of the claim complied with the 2005 California settlement. The court denied the topic for want of a showing of relevance, noting that the complaint alleged no violation of that agreement.[309] In *Choi* and *Stallman*, the courts treated the settlement as too old to support discovery.[310] In the second *Kelly* order, the court treated the settlement as a reason to exclude questions about an executive's earlier knowledge.[311] Unum cites the settlement as evidence that its conduct changed. When a claimant cites it, courts have held it too old, irrelevant, or a reason to close the inquiry.

C. The Litigation Record

Unum's second answer is that it prevails in most of the disability cases brought against it, and that its record of judgments shows that its claim administration and its reviewers are sound.

The judgments do not support that inference. In most of these cases, the court decided whether the denial was supported by the administrative record. It did not decide how the opinions in that record came to say what they said, and it had no evidence on whether Unum was using biased experts. Part VI showed why: courts refused discovery of selection, compensation, volume and outcome history, often at Unum's urging. Unum opposes the inquiry and then cites judgments entered without consideration of the relevant evidence.

The decisions in which discovery was granted show the same limit. *Braun* and *Leung* are the clearest instances.[312]

In *Allen*, the court ordered production of performance plans and quality audit results, and a jury later found for Unum.[313] A verdict for Unum after discovery was ordered decides that claim. It says nothing about how reviewers were selected in other claims.

A judgment entered on the administrative record does not test the points at which bias operates. It does not show whether the occupation was correctly described before the file went to the reviewer;

---

[308] *Bronner*, *supra*, 2009 WL 248175, at *5.

[309] *Gray*, *supra*, 2018 WL 4566850, at *6–7 (30(b)(6) Subject 15).

[310] *Choi*, *supra*, 2025 WL 2234903, at *4; *Stallman*, *supra*, 2024 WL 4988603, at *6; see Part VI.G.

[311] *Kelly*, *supra*, 2010 WL 5300807, at *2.

[312] See Part VI.H.

[313] *Allen*, *supra*, 2020 WL 6882169, at *15–16; Jury Verdict, *Allen*, No. 2:18-cv-69 (M.D. Fla. Mar. 29, 2022), ECF No. 243.

whether the reviewer was chosen for having decided similar questions a particular way; whether the referral letter supplied the conclusion, as it did in *Hangarter*; whether a condition was labeled self-reported so that the absence of objective evidence could be held against the claimant; whether an observed activity was treated as proof of capacity for sustained work; whether a physical finding was attributed to a psychological cause in order to apply a shorter benefit limit; or whether the reviewer's experience supported the premise the reviewer relied on, which in *Dwyer* it did not.[314] Part V.D showed that neither settlement requires a record of the reviewer's reasoning at those points. A judgment entered without that record shows what was proved in that case.

Unum's conduct in litigation shows that it treats the evidence as significant. It has opposed bias discovery in every decade covered by Part VI. In *Boles*, it obtained an order prohibiting publication of a discovery order two days after the order issued, asked the court to remove its findings about Unum's "culture and claims practices," and settled while the order remained restricted.[315] In 2016, it asked the Department of Labor to delete the one federal provision directed at the selection of reviewers (Section F). A party confident that the evidence would confirm its record would have little reason to keep it from courts and regulators.

What is asserted is narrower, and established by Unum's own conduct: Unum has opposed the production of this evidence, sealed it where it was produced, and asked the Department of Labor to remove the rule that would have generated it. The argument does not depend on showing that Unum never wins a fairly tested case, and it does not assert that Unum settles cases in order to suppress evidence. Part VI.H sets out what the dockets show on that question.

D. The Quality Assurance Function

Unum's third answer is that its quality assurance function ensures that the opinions it obtains are neutral and reliable.

The settlement established a quality function to review file documentation and the stated rationale for decisions, working with Unum's legal department, and a conduct pledge for employed clinical, vocational and medical professionals.[316] A documentation audit asks whether the file contains what the procedure requires. It cannot distinguish a well-documented biased denial from a well-documented sound one, because the two files look the same. It does not measure what a reviewer is paid, how often the reviewer is used, or how the reviewer's opinions come out.

When claimants have asked what Unum records about its reviewers, the answers have shown little. In *Kelly*, Unum's Rule 30(b)(6) designee testified that Unum had "no formal rating or evaluation system" for the examiners it hired, only feedback forms that internal physicians may complete, and that there was no evaluation of the two examiners' reports "except for the comment in Dr. Mann's

---

[314] See Part V.B–C; *Hangarter*, *supra*, 373 F.3d at 1011; *Dwyer*, *supra*, 548 F. Supp. 3d at 483–84; Order of the Commissioner, at 2–3.

[315] *Boles*, *supra*, 2013 WL 1079016, at *1–2; see Part V.A.

[316] Regulatory Settlement Agreement, Exs. 3, 5; see Part IV.E.

provider directory noting a very good turnaround time and extensive report."[317] Turnaround time and length are measures of production. They do not show whether the reviewer's conclusions agree with the treating physicians', survive appeal, or run in one direction. An insurer that records only how quickly a reviewer writes, and how much, has no basis in its own records for saying whether the reviewer is biased. What that costs the insurer is set out in *Demer*.[318]

When claimants have asked for the quality assurance documents themselves, Unum has resisted. In *Leung*, the claimant sought the Quality Assurance Tool, the Quality Assurance Standards, the monthly monitoring reports and the supplier reports named in Unum's Statement of Work with Dane Street. Unum responded that "Quality Assurance Standards" is not defined in its Pilot Services Agreement and that "monthly monitoring report," "monthly monitoring," and "monitoring report" do not appear in it. The court denied the requests because the claimant had not shown their relevance, and whether the documents exist was never determined.[319] In *Smith* and *Kamerer*, Unum successfully opposed discovery of what its measures are.[320] In *Kamerer*, the court denied discovery of Unum's efforts to mitigate its structural conflict.[321] *Allen* ordered the results of Unum's Medical Quality Audit Program for the professionals who reviewed the claim, but the order does not describe what the audit measures.[322]

In place of the documents, courts have received Unum's statements. In *Stallman*, the court weighed "Defendant's sworn representation that claims personnel are not evaluated or compensated based on claim outcomes."[323] In *De Mello*, Unum produced its incentive program documents and "represents that the programs do not incentivize claim outcomes."[324] In *Akans*, it offered a compensation template for its physicians, which the claimant said did not confirm whether any physician had received a bonus.[325]

Taken together, Unum says quality assurance addresses bias. The settlement's quality function reviews documentation. Unum's designee testified that no rating system for examiners exists. The quality instruments named in Unum's vendor contract were described as undefined when a claimant asked for them. And Unum's statements about its incentive programs have been accepted without the records that would test them. A measure that no one outside the company can inspect is an assertion.

---

[317] *Kelly*, *supra*, 2010 WL 3259997, at *2–3.

[318] *Demer, supra,* 835 F.3d at 903; see Part I (Factor 4) and Part IV.G.

[319] *Leung*, *supra*, 2023 WL 4056041, at *8–9 (RFPs 58, 59, 67, 68, 76).

[320] *Smith*, *supra*, 2020 WL 6281451, at *12 *Kamerer, supra*, 251 F. Supp. 3d at 352-53.

[321] *Kamerer*, *supra*, 251 F. Supp. 3d at 352–53.

[322] *Allen*, *supra*, 2020 WL 6882169, at *15–16.

[323] *Stallman*, *supra*, 2025 WL 3749611, at *4.

[324] *De Mello*, *supra*, 2026 WL 2032059, at *2.

[325] *Akans*, *supra*, 2023 WL 12051358, at *2.

E. What the Three Answers have in Common

The New York statements certify compliance with settlements that did not require bias to be measured. The litigation record rests on administrative records from which the evidence of bias was excluded, largely at Unum's urging. The quality function reviews documentation, and the only recorded evaluation of an examiner concerns speed and length.

None of the three examines selection, instruction, compensation, volume, the distribution of outcomes, or the basis on which a reviewer's opinion rests. Each answers a question about procurement with information about credentials or procedure.

Measured against *Glenn*, none of the three is a reasonable measure. *Glenn* gives two examples of steps that reduce a conflict's weight: "walling off claims administrators from those interested in firm finances," and "imposing management checks that penalize inaccurate decisionmaking irrespective of whom the inaccuracy benefits."[326] The incentives in this record are the recovery plans and weekly tracking reports whose discovery Unum resisted in *Gray*, *Jacob* and *Choi*, and whose targets in *Clark* were passed on orally; the net termination ratios that California found the companies managing to; and the vendor's "interest in saving money for its clients" that *Saldi* allowed the claimant to explore.[327] A regulator's statement, a count of judgments and a documentation audit do not separate claim decisions from any of those incentives, and none of them measures whether decisions are accurate.

The least visible form of the incentive is the one this record reaches least. A vendor's price can reflect the savings its reviews have produced without any contingent term in the contract. The reviewer is paid the same whatever the outcome, and neither the claim file nor the contract discloses the arrangement. *Leung* and *De Mello* show where the inquiry stops: Unum certified what it paid the vendor, stated that it did not know what the vendor paid the physicians, and described the quality terms in its own vendor contract as undefined.[328]

F. Unum's Request that the Department of Labor Delete the Selection Rule

Part I described the 2016 amendment to the claims regulation, 29 C.F.R. § 2560.503-1(b)(7), and the preamble's statement that a plan may not contract with a medical expert based on the expert's "reputation for outcomes in contested cases."[329] It was the first federal rule directed at how a reviewer is chosen.

On January 19, 2016, Unum Group asked the Department to remove it:[330]

---

[326] *Glenn*, *supra*, 554 U.S. at 117; see Part I.

[327] See Part VI.E; *Clark* (D.S.D.), *supra*, 2022 WL 17251352, at *9; Order of the Commissioner, at 3; *Saldi*, *supra*, 224 F.R.D. at 191.

[328] *Leung*, *supra*, 2023 WL 4056041, at *7–9; *De Mello*, 2026 WL 2032059, at *2, 4; see Part VI.C.

[329] 29 C.F.R. § 2560.503-1(b)(7); 81 Fed. Reg. at 92,319; see Part I.

[330] Comment of Unum Group on RIN 1210-AB39, at 10 (Jan. 19, 2016) (Gregory J. Breter, Senior Vice President).

> "Unum suggests that the requirements in subsection (b)(7) that hiring decisions not be made 'based upon the likelihood that the individual will support the denial of benefits' and that medical experts may not be hired based on 'reputation for outcomes' are unnecessary and should be deleted."

Unum gave these reasons:

> "Unum agrees with the concept that claim personnel should be unbiased. Unum's policy is that employment decisions cannot be made based on claim outcomes, whether they be approvals or denials. The concern with the proposal as currently drafted is that it potentially invites broad discovery and will increase litigation expense substantially. That is contrary to the Department's stated intention. With respect to medical experts, the preamble refers to an expert's 'reputation for outcomes in disputed cases.' In practice and in theory, there is no way to measure 'reputation' in this context. Again, this invites litigation. Moreover, courts already take 'conflict of interest' into account when reviewing benefit determinations and parties are certainly in a position to argue reputation issues, whether they apply to experts hired by plans or experts hired by claimant's or their lawyers."

Unum's objection was to the inquiry. It argued that the rule "potentially invites broad discovery" and "invites litigation," and it did not argue that the rule would disqualify reviewers who were not biased.

Unum's statement of its own policy cannot be checked against its own records. Unum told the Department that employment decisions "cannot be made based on claim outcomes." Six years earlier, its designee in *Kelly* had testified that the company kept no rating or evaluation system for the examiners it hired.[331] A company that does not record its reviewers' outcomes cannot show that it does not select on them, and no one can show that it does.

The Claim that Reputation Cannot be Measured

The measurement had been made before Unum said it could not be. A court had already recited Unum's own answers giving a reviewing physician's annual claim volume and his average annual compensation from Unum, three years earlier, in an order Unum had sealed within two days and which remained restricted when the case settled (Part V.A).[332] Those figures are public only because a claimants' bar association quoted them to the Department in this same rulemaking, together with a decision identifying reviewers hired repeatedly by one insurer and deposition testimony in which a psychiatrist reported about 1,800 file reviews in a single year for two insurers, with income itemized by insurer.[333] Courts had also ordered Unum to produce claim statistics over

---

[331] *Kelly*, *supra*, 2010 WL 3259997, at *2–3.

[332] *Boles*, *supra*, 2013 WL 1079016, at *1–2 & n.1; Text Order, *Boles, supra*, No. 4:11-cv-03031 (D. Neb. May 10, 2013), ECF No. 89; see Part V.A.

[333] Comment of the Massachusetts Employment Lawyers Association on RIN 1210-AB39, at 8–10 (Jan. 19, 2016) (Jonathan M. Feigenbaum, ERISA Committee Chair) (quoting the *Boles* order and *Maiden v. Aetna Life Ins. Co.*, No.

its declaration that it did not keep them in the form requested, and, after the rule took effect, ordered a reviewing physician's compensation from Unum alongside his total compensation from all medical work.[334]

A court has also checked such a measurement against the source documents, and this is where the answer to Unum's claim is plainest. *Chacko* is not an Unum case. It involved the AT&T disability plan, its claims administrator, Sedgwick, and a reviewer engaged through a vendor, NMR. The reviewer had prepared 88 reviews for 61 claimants. The plan produced the conclusion pages of those reviews "in lieu of providing specific responses" to interrogatories asking how often the reviewer had found that a claimant lacked capacity for full-time work. Counsel tabulated them: 50 of the 61 claimants, 82 percent, were found not disabled, 8 were found disabled from some type of work, and 3 were found partially disabled. The plan called the tabulation a "simplistic categorization" but withheld the conclusion pages "[f]or confidentiality reasons." The claimant filed them under seal, and the court compared them with the tabulation. It found that "plaintiff's representations are accurate and supported by the conclusion pages themselves," and it "reject[ed] defendant's challenge to the accuracy of the statistics."[335] The measurement required no compensation discovery and no admission from the insurer, only the reports. Claimants against Unum's affiliates now plead the measure, and in *Zagante* an allegation that a consultant physician "has a track record of recommending denial of LTD benefits in 82% of the matters considered" was held sufficient to support discovery of that physician's compensation and report volume.[336]

Unum's trade association identified the measure in the same rulemaking. America's Health Insurance Plans asked the Department not to adopt standards that disqualify an adjudicator "based solely on a 'reputational standard' such as the volume of claim denials," and explained that an expert "may subsequently have a high volume of denials due to the types of claims submitted and/or the lack of supporting evidence submitted by claimants."[337] That is an explanation for a number that can be counted. One insurer told the Department that reputation cannot be measured; its trade association named the measure and argued about what it means. The industry's own submissions show that the measure exists and that its meaning can be disputed, which is a reason to disclose it and let the parties dispute the inference.

Unum's comment also treated the rule as though it rested entirely on reputation for outcomes. The codified text does not use that phrase. It prohibits hiring decisions based on the likelihood that the individual will support a denial, and that prohibition can be tested with compensation, volume, and the insurer's own selection records, which are Factor 1 and Factor 4 evidence.

3:14-cv-901, 2016 WL 81489, at *2 (N.D. Ind. Jan. 6, 2016), and excerpting deposition testimony from *Kinser v. Plans Admin. Comm. of Citigroup, Inc.*, 488 F. Supp. 2d 1369 (M.D. Ga. 2007)).

[334] *Bronner*, *supra*, 2009 WL 248175, at *5; see Part VI.D; *Wittmann*, *supra*, 2018 WL 3374164, at *2–4; see Part VI.C.

[335] *Chacko, supra,* 690 F. Supp. 3d 1150–51.

[336] *Zagante*, *supra*, 2026 WL 1413584, at *1. The figure is the claimant's allegation, and the court made no finding on its accuracy.

[337] Comment of America's Health Insurance Plans on RIN 1210-AB39, at 9 (Jan. 19, 2016).

The Department of Labor's Response

The Department kept the rule and restated it. It recited the concern that the preamble statement "might result in claimants requesting statistics and other information" about the cases in which a medical expert supported denial, and concluded that "the preamble statement accurately describes one way that the independence and impartiality standard could be violated."[338] It was asked to delete the statement, considered the objection that it would lead to requests for statistics, and reaffirmed it.

The Department then added two sentences, the first declining to enlarge the administrative record and the second preserving discovery: the independence and impartiality requirements "do not modify the scope of 'relevant documents' subject to the disclosure requirements," and "[n]or do [they] prescribe limits on the extent to which information about consulting experts would be discoverable in a court proceeding as part of an evaluation of the extent to which the claims administrator or insurer was acting under a conflict of interest."[339] The industry read the two sentences the same way. In December 2017, when the rule was reopened, Cigna, which was asking the Department to revise the Final Rule, and objected at length to its other provisions, supported the conflict-of-interest provision "without change" as "consumer-oriented." It rested that support on the first sentence and not the second: "Our support is based on our agreement with the Department's commentary in the Preamble adopting the Final Rule which clarified that the conflict of interest 'requirements in the rule do not modify the scope of relevant documents subject to the disclosure requirements.'".[340]

The Department declined to create an affirmative duty to disclose compensation and volume, giving two reasons: the parallel health-plan rule under the Affordable Care Act contains no such provision, and "an attempt to establish specific measures or other standards would benefit from a further proposal and public input." It acknowledged that such standards "might provide additional protections against conflicts of interest."[341] It did not find the measures unworkable, did not find that reputation cannot be measured, and did not find the discovery burden excessive.

The Department also extended the rule's coverage in ways the claimant side had sought. It added vocational experts to the codified text, confirmed that the requirements reach consulting experts and not only the person who decides the claim, and extended them to experts hired or compensated by third parties engaged by the plan, which must address the service provider's practices "in the terms of its service contract and ongoing monitoring."[342] Unum told one court that it did not know what its vendor paid the physicians who reviewed its claims, and told another that

---

[338] 81 Fed. Reg. at 92,320.

[339] *Id.*

[340] Comment of Cigna Corporation on RIN 1210-AB39, at 2 (Dec. 11, 2017) (David Schwartz).

[341] 81 Fed. Reg. at 92,320.

[342] *Id.*; 29 C.F.R. § 2560.503-1(b)(7).

the quality terms in its own vendor contract were undefined (Part VI.C, Part VII.D). The preamble describes what such a contract is expected to contain.

The Limits of the Rule

The reputational criterion appears in the preamble. Paragraph (b)(7) codifies the sentence on hiring, compensation, termination and promotion, and does not use the word "reputation." An insurer may call the criterion interpretive commentary. It is the Department's own reading of its own rule, and the Department reaffirmed it after being asked to delete it.

No reported decision applying § 2560.503-1(b)(7) to a challenge to the selection of a reviewer has been located. That result follows from a rule that requires no record. Part IV describes the same result for the settlement's selection provision. A court cannot apply a rule without evidence, and a rule that creates no record produces none.

PART VIII. CONCLUSION

The record set out above establishes four things.

The practice was identified, in the largest multistate disability examination the record discloses. The multistate examiners found excessive reliance on in-house medical professionals and inferred a "Company bias." California found that the companies used independent medical examinations to their own advantage, overruled their own physicians when those physicians supported a finding of disability, and decided claims in roundtable sessions the files did not record. The courts had found the same things earlier, with names attached.[343]

The remedy did not address it. The settlements prohibited selecting an examiner by prior results and then required no record of what any examiner was paid, how often any examiner was used, how any examiner's opinions came out, or how any examiner was chosen. Compliance was measured by a file-level error rate that a company sending every examination to a physician who had never found a claimant disabled would have passed. California wrote a disclosure rule, an appearance-of-partiality standard, and a pattern-and-practice removal mechanism into the same agreement, and applied them to the reviewer it appointed itself.[344]

The practice continued. Courts deciding claims denied after 2004 have found the companies' reviewers reasoning from the expected course of a condition rather than from the claimant's record, treating pain and weakness as self-reported so that the absence of objective proof could be held against the claimant, and drafting the conclusion and inviting the treating physician to adopt it. Where a claimant was permitted to look, the relationship behind the reviewer was what *Hangarter* had shown: a physician averaging 250 of the company's claims a year at $237,500, a

[343] See Parts III.A and III.B.

[344] See Parts IV.B through IV.F, and Part IV.G.

consultant alleged to recommend denial in 82 percent of the matters considered, a reviewer whose income from the company a court ordered stated as a share of his total income.[345]

Every one of those facts came from another insured's claim file. None came from an examination, a market conduct report, or a settlement. Each came from a claimant who sued, asked, obtained an order, and left a record a later claimant could use.[346] The threshold showing that ERISA discovery requires can be met only with such a fact, and such facts exist only in other insureds' files. The *Boles* order shows what closing that route costs: the insurer had the order sealed two days after it issued, settled while the seal stood, and the figures survive only because a bar association quoted them to a federal agency.[347]

The 2004 settlements are the precedent for what is now proposed. The regulators then prohibited a practice and built an instrument in which compliance with the prohibition could not be observed. The evidence of that practice has since come from files the companies were required to keep. A proposal that permits those files to be destroyed does not leave the 2004 arrangement where it stands. It removes the one source of evidence that survived it, and it does so in the name of the insureds whose files are the evidence.

Two consequences follow.

The first is that retention of those files is not, for this purpose, a privacy question. What a claimant seeks from another insured's file is the reviewer's analysis, the reviewer's conclusion, and the company's record of engaging and paying the reviewer. No order described in this article required the other insured's identity or medical history to be disclosed, and the one order that addressed the question directed that the medical content be redacted. That order, in 1999, directed that the examiner's reports show only the insurer, the analysis, and the recommendation. A court supplied the answer twenty-seven years ago, and no decision since has found it unworkable. Redaction preserves the evidence and removes the privacy interest.[348]

The second is that public enforcement will not supply what destruction would remove. The multistate examination and the California proceeding are the most substantial instance of public enforcement this record contains. They identified the mechanism and wrote a remedy that could not detect whether it stopped. A regulator cannot be expected to find in destroyed files what the regulators did not find when the files existed.[349]

The insurer's own submissions confirm that the evidence matters. Asked in 2016 to strike the federal rule on the selection of reviewers, Unum told the Department of Labor that a reviewer's reputation for outcomes could not be measured and that the rule "invites litigation." Its trade association said a high volume of denials might have innocent explanations. One commenter

[345] See Parts V.A through V.D.

[346] See Parts V.A and VI.A through VI.C.

[347] See Parts V.A and VII.F.

[348] See Part IV.C (*Small*).

[349] See Parts III.B, IV.F and IV.G.

called the measure impossible; the other explained what it means. The Department kept the rule.[350]

A closed claim file holds the only evidence from which the neutrality of a medical opinion has been tested in this industry, and the only route by which that evidence has reached a court. Its destruction would resolve, in favor of the insurer and without argument, every question the insurer has contested for three decades.

[350] See Part VII.F.

Chuck Bell

Date: September 22, 2026

To: NAIC Privacy Protections (H) Working Group

Re: Revised Exposure Draft of the NAIC Privacy of Consumer Information Act Model 672 (Draft dated July 24, 2026)

From: Chuck Bell, NAIC Consumer Representative
Programs Director, Advocacy, Consumer Reports[1]

Executive Summary

Thank you for the NAIC Privacy Working Group's substantial work to modernize Model 672. The July 24 exposure draft broadens the definition of covered information, adds access, correction, and deletion rights, strengthens third-party accountability, requires affirmative opt-in consent for sales and disclosures of sensitive information, and creates a targeted-advertising opt-out. These are important improvements that states should be able to adopt without weakening existing protections.

However, the draft still leaves two central gaps:

1. The absence of a general data-minimization rule, and
2. The absence of safeguards for automated decision systems and external consumer data used in consequential insurance decisions.

Given the working group's direction and the industry's likely opposition to reopening the broader Model 674 debate relating to data minimization, I recommend that the NAIC add a practical, targeted enhancement to Model 672: adoption of a *Telematics Guardrail Package* that addresses one of the most urgent and high-risk data-minimization gaps in today's insurance ecosystem.

Telematics data—collected by automakers, apps, SDKs, and data brokers—has become one of the most sensitive and consequential categories of consumer information used in underwriting, pricing, claims, fraud detection, and customer segmentation. Recent investigations and enforcement actions involving GM/OnStar, LexisNexis, Verisk, Allstate/Arity, and multiple state Attorneys General demonstrate that existing GLBA-style frameworks do not adequately govern modern telematics data pipelines.[2]

---

[1] Organization listed for affiliation purposes only. Consumer Reports agrees with some of the positions expressed in these comments, but this comment letter reflects my personal views.

[2] See Hill, Kashmir, *Automakers Are Sharing Consumer Driving Behavior with Insurance Companies*, 3/11/24, available at: https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html?unlocked_article_code=1.6FA.6d9M.mY0TQHInsLYv&smid=url-share; Hill, Kashmir, *Texas Sues Allstate Over Its Collection of Driver Data*, 01/13/25, available at: https://www.nytimes.com/2025/01/13/technology/texas-allstate-driver-data-lawsuit.html; State of California Department of Justice, *When It Comes to Data Privacy, Consumers Must Be In the Driver's Seat*, Press Release, 05/08/26,

The guardrails proposed below are narrow, feasible, and directly responsive to documented harms. They do not require NAIC to abandon Model 672 or officially revive Model 674. Instead, they provide a sector-specific, minimally disruptive way to ensure that telematics programs are transparent, consent-based, purpose-bound, and subject to reasonable retention limits.

I also propose that the Working Group add a dedicated article governing automated decision systems and external consumer data used in consequential insurance decisions, that would authorize state regulators to require impact assessments, accuracy and bias testing, less-discriminatory alternatives, consumer notice, explanations, correction, appeal, and human review.

I. The Draft Makes Important and Necessary Progress

Thanks to the hard work of the Working Group, the exposure draft contains many important provisions that strengthen consumer privacy, including:

- **Modernized coverage of personal information:** Section 4 defines nonpublic personal information broadly as personally identifiable information linked or reasonably linkable to an identified person, excluding only de-identified and publicly available information. This is a meaningful improvement over a narrower financial-information framework.

- **Third-party accountability:** Section 5 requires purpose-limited contracts, deletion or return of data, flow-down protections for subcontractors, security safeguards, assistance with consumer requests, and prompt notice of noncompliance. It also makes the licensee responsible for the handling of information by service providers.

- **Access, correction, and deletion:** Section 6 creates affirmative rights to obtain information, identify service providers that received it, correct inaccuracies, delete information subject to defined exceptions, and appeal adverse responses.

- **Targeted-advertising controls:** Section 19 provides a right to opt out of targeted advertising and limits repeated attempts to reverse the consumer's choice.

- **Preservation of state protections:** Section 29 states that the health-information article does not preempt existing state privacy laws. Model 672 should include strong protections for all types of information, so I recommend broadening that savings clause to the full Act.

These provisions represent significant progress in modernizing insurance privacy and should be supported and retained. I also support the proposed suggestions for improvements submitted in the group consumer letter submitted by NAIC Consumer Representative Harry Ting.

available at: http://oag.ca.gov/news/press-releases/when-it-comes-data-privacy-consumers-must-be-driver%E2%80%99s-seat-attorney-general

II. Data Minimization Should Be the Foundation of a Model State Insurance Privacy Law

The exposure draft primarily regulates disclosure and gives consumers choices after information has been collected. That is not enough. Privacy should be protected by default. A consumer obtaining insurance should not have to identify every company holding their data, decipher notices, and repeatedly opt out of unnecessary processing. Nor should an insurer be permitted to collect unlimited information merely because the practice appears in a notice. From a consumer perspective, Model 672 should include a general data-minimization and purpose-limitation duty applicable to collection, use, retention, and disclosure. I appreciate that most of the insurance industry opposes this position, but I think it is important to state for the record how important a strong, affirmative data minimization standard is for consumers.

III. A Practical Path Forward: The Telematics Guardrail Package

Given the working group's decision not to further develop Model 674's comprehensive minimization framework, NAIC should adopt a targeted, high-impact set of guardrails addressing the most urgent data-minimization gap in insurance: vehicle telematics data. Telematics reduces risky driving behavior by giving drivers real-time feedback, clear safety coaching, and transparent incentives that encourage smoother braking, safer speeds, and more consistent driving habits. However, the primary benefits of risk-mitigation and more affordable premiums are put at risk when insurers do not effectively safeguard driver data for its primary intended purpose, and are found to be using manufacturer- or digital app data acquired from other sources in unexpected ways.

Telematics data is uniquely sensitive, revealing daily routines for travel to work, school, medical visits, shopping, religious worship, and visits to friends, family and community organizations. It is increasingly used in underwriting, pricing, claims handling, fraud detection, and customer segmentation. Recent investigations and enforcement actions regarding General Motors On-Star, Verisk and Allstate's Arity app show that telematics data pipelines often involve deceptive consent, incompatible processing, opaque multi-actor data flows, and long-term retention.[3] Companies like General Motors (via OnStar Smart Driver), Kia, Subaru, and Mitsubishi enrolled drivers—often through default infotainment app setups without explicit knowledge. For GM alone, vehicle data was collected from over 14 million vehicles, often without full driver knowledge or informed consent. Drivers were often shocked and dismayed to find their driving data was being used to set their insurance premiums.[4]

Similarly, Allstate, through its subsidiary data analytics company Arity, paid app developers to incorporate its software in third party apps such as Life360, GasBuddy and Fuel Rewards to track

[3] Op cit. Note #2.

[4] "… [The California Department of Justice] investigation determined GM failed to give consumers any notice of the sales to Lexis and Verisk and misled consumers by implying that data would only be used to provide OnStar subscribers with requested services. In its privacy policy, GM even stated that it did not sell any driving or location data and that if it did disclose any such data for insurance purposes, it would be at the consumer's express direction. Additionally, GM sold consumers' data to Lexis and Verisk without customers' knowledge or consent, despite an internal privacy compliance program that required GM to inform consumers how their personal information would be used and the third parties that may receive it." Op.cit. Note #2.

consumers' driving data, according to the Texas Attorney General's lawsuit. "Allstate collected trillions of miles worth of location data from over 45 million consumers nationwide and used the data to create the 'world's largest driving behavior database… When a consumer requested a quote or renewed their coverage, Allstate and other insurers would use that consumer's data to justify increasing their car insurance premium."[5]

Model 672 does not structurally prevent these harms. The following guardrails would.

A. Program-Specific Opt-In for Telematics-Based Decisions

A licensee may not collect, purchase, or use telematics data for underwriting, pricing, eligibility, or claims decisions unless the consumer has provided affirmative, program-specific opt-in.

Opt-in must be separate from general app consent, vehicle purchase agreements, or OEM terms of service. The insurer who is operating the telematics program and/or acquiring third-party data from OEMs or other sources should get explicit consumer opt-in for the insurance use of that information, so that the insured customer knows where the data is coming from, how it is being collected, and how to contest a third-party score if that is being used. The opt-in should be free of dark patterns or manipulative designs so that the insured is not unfairly tricked into giving consent.

B. Purpose Limitation for Telematics Data

Telematics data collected for safety, maintenance, navigation, driver assistance or in third-party apps may not be repurposed for insurance pricing or eligibility decisions without fresh, program-specific opt-in.

C. Restrictions on Third-Party Telematics Sources

Insurers may not purchase or use telematics-derived risk scores from OEMs, data brokers, analytics subsidiaries, or mobile apps unless the consumer has provided program-specific opt-in.

D. Retention and Deletion Requirements

Licensees must delete telematics data and derived scores within 90 days after the consumer exits the telematics program or the data is no longer necessary for the permitted purpose.

Third-party vendors must contractually agree to matching deletion timelines.

E. Full Ban on Marketing Use of Telematics Data

[5] Attorney General Bill Paxton, *Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies,*
Press Release, 1/13/25, available at: https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45

A licensee shall not use vehicle telematics data or any telematics-derived risk score for marketing, targeted advertising, cross-selling, retention campaigns, or any promotional purpose. Telematics data collected for underwriting, pricing, claims, fraud detection, or a telematics program shall not be processed for any marketing-related purpose, and no inference derived from telematics data may be used to target or segment consumers for marketing.

F. One-Page Telematics Disclosure

Licensees must provide a concise disclosure explaining:

- What telematics data is collected
- How it affects pricing or eligibility
- Which third parties receive it
- How long it is retained
- How consumers can access, correct, delete, or revoke consent

G. Regulator Filing of Telematics Programs

Licensees must file telematics programs and scoring models with regulators, including:

- Data elements used
- Necessity and proportionality justification
- Retention schedules
- Vendor/broker relationships

These proposed provisions would be popular with consumers, and create a trusted framework for drivers to opt-in to telematics programs with full informed consent and knowledge that their sensitive data will be protected. Without guardrails, Model 672 would allow insurers to continue to acquire and use telematics-derived risk scores when upstream collection was deceptive or incompatible with consumer expectations, leading to further exposés, enforcement actions and reputational damage for insurance companies and data brokers.

As it exists now, the Model 672 exposure draft's GLBA-style framework could also leave consumers vulnerable to many other emerging unexpected data use scenarios beyond telematics. For example, connected home devices (smart thermostats, security systems, voice assistants) increasingly generate behavioral data that can be repurposed for insurance risk scoring without explicit consent. Health-adjacent data from wearables, fitness apps, and pharmacy loyalty programs can be sold to brokers and used to infer medical conditions or lifestyle risks. Retail purchase histories, mobility data from rideshare apps, and geolocation patterns from mobile advertising networks can be combined to create detailed risk profiles that consumers never see.

Because Model 672 lacks strict necessity, proportionality, and incompatible-processing rules, insurers can ingest these datasets as long as they fit within broad "permitted uses," even when upstream collection was deceptive or incompatible with consumer expectations. Policymakers

should anticipate these data pipelines and unexpected use cases now—before they become the next GM/OnStar-style scandal.

IV. Automated Decision Systems and Algorithmic Fairness

A dedicated article should be added to Model 672 that governs the use of automated decision systems and external consumer data used in consequential insurance decisions. This section explicitly enable regulators to require impact assessments, accuracy and bias testing, less-discriminatory alternatives, consumer notice, explanations, correction, appeal, and human review.

The Model 672 draft is largely silent on how insurers use data to make decisions. That silence is a major gap. Automated systems can affect whether a consumer is offered coverage, how much the consumer pays, whether a claim is flagged or delayed, and how the consumer is treated throughout the insurance lifecycle. Errors or biased models can scale harm quickly, and reliance on proxy variables can reproduce discrimination even when a protected characteristic is not expressly used. Insurers should be required to demonstrate that external consumer data and AI systems are not unfairly or unlawfully discriminatory and to evaluate less discriminatory alternatives.

While NAIC has issued a Model Bulletin on AI, there are many additional issues relating to data privacy and use that should be addressed as part of Model 672. The bulletin is supervisory guidance: it outlines expectations for insurer governance, documentation, and oversight, but it does not regulate the data inputs, data sources, consumer rights, or algorithmic impacts that increasingly determine eligibility, pricing, claims handling, and fraud detection.

The most consequential harms in modern insurance arise not from model architecture but from the data pipelines feeding those models—including telematics, mobility data, retail purchase histories, device data, and health-adjacent information. These sources are often purchased from brokers or analytics vendors and used without consumer knowledge, provenance checks, accuracy requirements, or disparate-impact testing. The bulletin does not govern these inputs, does not create consumer rights, and does not give regulators clear authority to inspect external data, scoring models, or vendor relationships. Model 672 is the only place where NAIC can create binding, statutory rules for data governance, fairness, and consumer protection.

Model 672 could also fill critical gaps the bulletin cannot reach. The bulletin does not regulate proxy discrimination, claims-fraud algorithms, telematics pipelines, incompatible processing, retention limits, or consumer access to scores and factors. It does not require insurers to test external data for bias, evaluate less-discriminatory alternatives, explain automated decisions, or provide human review. It does not give consumers the ability to correct inaccurate external data or challenge automated outcomes. And it does not give regulators the authority to obtain data dictionaries, model documentation, or impact assessments.

As insurers increasingly rely on automated systems and external consumer data for underwriting, pricing, claims, and fraud detection, these gaps are becoming more consequential. The potential

impact on consumers will be significant, and this gap will become glaringly apparent if it is not addressed immediately. A dedicated AI/ECDIS section in Model 672 ensures that the bulletin's high-level principles can be backed by clear, enforceable rules governing data inputs, fairness testing, consumer rights, and regulator access—creating a coherent, modern privacy and algorithmic-governance framework that matches the realities of today's insurance market.

Recommended new article: Automated Decision Systems

- **Definitions.** Define "automated decision system," "consequential decision," "profiling," "external consumer data and information source," and "substantial factor" broadly enough to cover systems that assist or materially influence a human decision.
- **Pre-use impact assessment**. Before deployment, require a documented assessment of the system's purpose, data sources, validity, accuracy, foreseeable risks, privacy impacts, disparate impacts, security, explainability, and alternatives.
- **Fairness testing**. Require testing across protected and vulnerable groups, including intersectional analysis where feasible, and periodic retesting after material changes or evidence of drift.
- **Less discriminatory alternatives**. Require insurers to identify and implement reasonably available alternatives that achieve legitimate objectives with less discriminatory impact.
- **Data quality and provenance**. Require documentation of the source, relevance, representativeness, completeness, legality, and known limitations of training, validation, and operational data.
- **Consumer notice and explanation**. Before or at the time of a consequential decision, tell the consumer that an automated system was used, identify the principal factors and data categories, and explain how to obtain more information.
- **Access, correction, appeal, and human review**. Permit consumers to correct data, contest outcomes, submit additional information, and obtain timely review by a qualified person with authority to change the decision.
- **Adverse-action specificity**. Explanations must be specific and accurate; generic statements, opaque "risk scores," or claims that a model is proprietary should not defeat consumer rights.
- **Governance and accountability**. Require board or senior-management oversight, written policies, vendor due diligence, recordkeeping, regulator access, and independent review for high-risk uses.
- **Public and regulatory transparency**. Require submission of impact assessments to regulators and public summaries that protect legitimate security information without concealing material risks or discriminatory effects.

IV. Strengthen Civil-Rights and Nondiscrimination Protections

Section 31 prohibits unfair discrimination against a consumer for exercising certain privacy rights. That is useful but too narrow. It does not address discrimination arising from the collection, inference, use, or disclosure of data, nor does it expressly address disparate impacts from automated systems or proxy variables.

NAIC should add a substantive nondiscrimination provision applicable to all processing under the Act. At a minimum, a licensee should be prohibited from processing personal information in a manner that causes unlawful discrimination or an unjustified disparate impact in access to

insurance, price, coverage, benefits, claims, or service. The provision should require testing and mitigation, not merely intent-based compliance.

Recommended Additions

- Expand "sensitive personal information" to include precise geolocation, health and disability information, financial account credentials, immigration status, sex or gender identity, status as a victim of crime, and other data commonly treated as sensitive under modern privacy laws.
- Prohibit inferring sensitive traits for uses the licensee could not lawfully undertake using the trait directly.
- Prohibit discrimination through proxies, including location, purchasing behavior, device data, browsing activity, social media, education, occupation, and other correlated variables where they produce unjustified disparate impacts.
- Require meaningful review of claims-fraud tools and other systems that may delay, burden, or discourage valid claims, not only underwriting and pricing systems.
- Clarify that privacy rights and nondiscrimination protections apply to applicants, policyholders, insureds, beneficiaries, claimants, and other individuals whose information is processed.

V. Improve Consumer Rights and Reduce Friction

The rights in Section 6 are an important advance. They should be strengthened to ensure they work in practice, especially for consumers dealing with multiple insurers, producers, vendors, data brokers, and scoring providers.

- **Authorized agents.** Expressly allow consumers to use authorized agents for access, correction, deletion, opt-out, and opt-in revocation requests, with reasonable verification safeguards.
- **Portability.** Add a right to obtain information in a structured, commonly used, machine-readable format where technically feasible.
- **No authentication for opt-out.** Do not require identity authentication for requests that only restrict processing, unless reasonably necessary to prevent fraud.
- **No dark patterns.** Prohibit interfaces that materially interfere with or impair consumer choice, including unequal steps, misleading language, repeated prompts, and bundled consent.
- **Universal signals.** Require recognition of approved universal opt-out preference signals for targeted advertising and other opt-out rights when the consumer interacts online.
- **Free requests.** Clarify that requests and appeals are free except for manifestly unfounded or excessive requests, with the burden on the licensee.
- **Consistent deadlines.** Harmonize the 10-day and 15-day opt-out implementation periods and require prompt downstream communication to affiliates and service providers.
- **Access to decision data.** Ensure access includes data, scores, inferences, and principal factors used in consequential decisions, not merely raw information supplied by the consumer.
- **Deletion propagation.** Require the licensee to notify each service provider and third party of a validated deletion request unless impossible or disproportionate, and tell the consumer which entities were notified.

VI. Narrow Exceptions and Close Avoidable Loopholes

Exceptions are necessary for core insurance functions and legal obligations, but they should be interpreted narrowly. Several provisions are broad enough to permit extensive processing without meaningful consumer control.

- **Service providers and joint marketing (Section 22):** Joint marketing should not be treated as equivalent to operational servicing. At minimum, marketing-related disclosure should be separately identified, limited to necessary data, and subject to an effective opt-out. Service providers should be prohibited from combining insurer data with data from other clients except where strictly necessary for security or fraud prevention.
- **Transaction and servicing exception (Section 23):** Replace "usual, appropriate or acceptable" with "reasonably necessary and proportionate." Clarify that underwriting and claims functions do not authorize collection of unrelated data or use of unlawfully discriminatory models.
- **Research exception (Sections 23 and 25):** Require a documented public-interest, scientific, or actuarial purpose; minimization; de-identification where feasible; security; and restrictions on individual-level decisions and commercial reuse.
- **Mergers and transfers (Sections 14 and 24):** Require the recipient to honor prior consumer choices, use data only for compatible purposes, provide notice of material changes, and obtain consent where the acquiring entity proposes materially different processing.
- **HIPAA compliance safe harbor (Section 28):** A broad entity-level or data-handling safe harbor may leave insurance data outside the model's protections. Any safe harbor should be limited to the specific data and processing actually subject to equivalent HIPAA requirements.
- **De-identification:** Add enforceable requirements: reasonable technical and administrative measures, a public commitment not to reidentify, contractual restrictions on recipients, and periodic assessment of reidentification risk.

VII. Enforcement and Remedies Must Be Meaningful

Section 34 states that the Act does not create or imply a private cause of action. An express bar on individual remedies weakens deterrence and leaves consumers without meaningful recourse when misuse of personal information causes financial, dignitary, or discriminatory harm.

Model 672 should provide a private right of action for material violations, including unlawful sale or disclosure, failure to honor consumer rights, discriminatory automated decisions, and security failures. At minimum, the model should not foreclose remedies that otherwise exist under state law and should include strong regulator authority, civil penalties calibrated to the seriousness and duration of the violation, enhanced penalties for knowing or reckless conduct, restitution, injunctive relief, and no mandatory cure period for serious violations.

Regulators should also have express authority to obtain algorithms, data dictionaries, model documentation, impact assessments, testing results, vendor contracts, and other information necessary to evaluate compliance. Trade-secret claims should protect legitimate confidential

information from public disclosure, but should never bar regulator access or prevent meaningful consumer explanations.

Conclusion

The revised Model 672 is a significant modernization of insurance privacy protections. NAIC should preserve its strongest provisions and improve them before final adoption. Given the working group's direction and industry opposition to reopening the broader Model 674 debate, the proposed *Telematics Guardrail Package* offers a practical, targeted, and urgently needed enhancement that addresses the most consequential data-minimization gap in today's insurance ecosystem. And the section on *Automated Decision Systems and External Data* addressed a glaring gap in protections for use of customer data acquired from third party sources that is used in AI models.

Thank you for considering these comments. I welcome the opportunity to work with NAIC, state regulators, industry, and other stakeholders to refine these proposed provisions.

Submitted By:

Chuck Bell
Programs Director, Advocacy
c/o Consumer Reports
101 Truman Avenue
Yonkers, NY 10703
(914) 378-2507
chuck.bell@consumer.org

Appendix A. Recommended Priority Amendments

1	New section	Add data minimization, purpose limitation, and retention limits.	Protect privacy by default and reduce security and discrimination risks.
2	New article	Regulate automated decision systems used in consequential insurance decisions.	The model currently regulates data transfers more than decision-making uses.
3	§31	Add substantive algorithmic nondiscrimination and disparate-impact protections.	Current language only protects exercise of privacy choices.
4	§§23–25	Tie all exceptions to necessity and proportionality; narrow underwriting, fraud, research, and internal-use exceptions.	Prevents exceptions from swallowing the rule.
5	§4	Expand sensitive data; strengthen public-data and de-identification definitions.	Modern data ecosystems enable sensitive inferences and reidentification.
6	§6	Add portability, authorized agents, decision-data access, and downstream deletion.	Makes consumer rights practical and useful.
7.	New article, add after §5 or §6 relating to consumer rights and third-party accountability	Add telematics guardrail package	Addresses data protections issues relating to vehicle telematics
7	§19	Require universal opt-out signals and prohibit dark patterns.	Reduces friction and makes choices scalable.
8	§28	Limit HIPAA safe harbor to equivalent data and processing.	Avoids broad gaps in protection.

9	§29	Extend the savings clause to the entire Act.	Preserves stronger state privacy and insurance laws.
10	§34	Provide meaningful individual remedies or remove the express bar.	Improves accountability and consumer redress.

Harry Ting on behalf of Consumer Representatives (see TOC or pg. 3 of this document)

FROM THE NAIC CONSUMER REPRESENTATIVES

TO: NAIC Privacy Protections (H) Working Group
sent via email to: privacywg@naic.org

DATE: September 22, 2026

RE: **Consumer Representative Comments on Full Draft of Revised Model 672**

Thank you to the Privacy Protections (H) Working Group for the opportunity to comment on the fully revised Draft Model 672 that was exposed on July 24, 2026. We appreciated the opportunity to provide comments during the last round of reviews of the Model and feel that many improvements were made in the process. Reviewing this latest version, there are some areas where we feel Model 672 should be revised further. This document presents the rationale for several of our major revisions. In addition, it expresses our support for some changes submitted by a fellow NAIC Consumer Representative on behalf of the Coalition Against Insurance Fraud. Following these sections are our detailed revision recommendations. They are shown in WORD redline format, with additional comments in the margin.

I. Require Transparency & Ease of Making Privacy Choices

Protecting consumers from harmful uses of their nonpublic personal information should be the goal of the new Model 672. We have stated at many Privacy Protection Working Group sessions that the best way to provide that protection is to require that nonpublic personal information (NPI) should only be used to execute transactions and service accounts sought by consumers, unless a consumer explicitly gives permission for it to be shared for other purposes.

However, recognizing that a comprehensive opt-in approach is unlikely to be adopted by NAIC, it is critical that Model 672 include requirements that:

- guarantee informed choice about the data that might be collected and shared through transparency of privacy policies; and
- enable consumers to easily exercise their privacy rights.

Transparency

In order for consumers to have true informed choice about their ability to limit NPI sharing, it is essential that there be full transparency about the NPI that licensees may collect and share. Revised Model 672 requires licensees to inform consumers about the categories of NPI that they may collect and share, but it allows licensees to choose what those categories are. The categories listed in the federal Model Forms in Appendix B of the Revised Model 672 are antiquated and totally misleading. Most consumers would not realize that many types of NPI that we list in our revisions to Section 9 might also be collected and shared. Therefore, we believe the categories listed in our revisions should be required to be used by licensees, and Appendix B should be deleted.

Ease of Making Privacy Choices - Prohibit Dark Patterns

Another essential feature of Model 672 should be to prohibit the use of "dark patterns"; namely, practices that manipulate users into making choices they would not otherwise have made. It is common knowledge that most consumers will not read privacy policies in their entirety, because most policies are too lengthy, confusing, and many are too technical. There is nothing in the Draft Model 672 that would prevent licensees from using dark patterns. To prohibit those practices, we have added to Section 7 in the Draft Model 672 a subsection that would have that effect. It is noteworthy that the CCPA regulations in California have similar requirements to prohibit the use of dark patterns.

II. Making Disclosure of Privacy Policies Reasonably Understandable, Conspicuous, and Accessible

Within the definitions of "understandable" and "conspicuous," we have added revisions to improve their application. Under the definition of "conspicuous," we also address requirements that should exist for digital platforms, which are not addressed in Draft Model 672.

In addition, we have added "accessible" as an additional requirement for privacy policies. That addition recognizes the need to accommodate consumers with disabilities and those whose primary language is not English. Those needs are also not addressed by the Draft Model.

III. Sensitive Information

We have added to the definition of "sensitive personal information" in Section 4 two additional categories:

- Any nonpublic personal health information (PHI) that is not covered by the federal Health Insurance Portability and Accountability Act (HIPAA) or other federal regulations.
- All nonpublic personal information of individuals who are 18 years old or younger.

These days, the same types of personal health information (PHI) that are covered by HIPAA and other federal PHI privacy regulations are also collected from sources that are not covered by those laws. Examples include nonpublic PHI collected from consumers' online activity and from the Internet of Things. Sharing such information can cause equal harm regardless of its sources. Therefore, all nonpublic PHI should have the same protections as provided by HIPAA and other federal regulations; namely consumers should have to opt-in for their nonpublic PHI to be shared.

We have also added the NPI of individuals 18 years old or younger, because minors might not be able to consent, monitor, or correct NPI disclosures, and the harms from exposed NPI can be more severe, longer lasting, and harder to detect than for adults.

IV. Antifraud Provisions

Mr. Brent Walker is submitting revision recommendations to Model 672 on behalf of the Coalition Against Consumer Fraud. He is also an NAIC Consumer Representative. We have reviewed the Coalition's comments and are fully supportive of the changes it is proposing to Section 6 of Model 672.

© 2026 National Association of Insurance Commissioners

Signed by NAIC Consumer Representatives

Adam Fox
Amy Bach
Anna Hyde
Anna Schwamlein Howard
Brenda Cude
Brendan Bridgeland
Brent Walker
Bonnie Burns
Carl Schmid
Deborah Darcy
Deborah Steinberg
Elizabeth Hagan
Eric Ellsworth
Erica Eversman
Harold Ting
Kellan Baker
Kenneth Klein
Laura Colbert
Marguerite Herman
Michael DeLong
Milo Vieland
Peter Kochenburger
Richard Weber
Shamus Durac
Silvia Yee
Stephanie Hengst
Wayne Turner

© 2026 National Association of Insurance Commissioners

Appendix: NAIC Consumer Representatives Model 672 Revisions and Detailed Comments

PRIVACY OF CONSUMER INFORMATION ACT

Table of Contents

ARTICLE I. GENERAL PROVISIONS

Section 1. Purpose
Section 2. Scope and Compliance
Section 3. Rule of Construction
Section 4. Definitions

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Section 5. Third-Party Service Provider Arrangements

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7. Initial and Subsequent Delivery Notice of Information Practices to Consumers Required
Section 8. Annual Notice of Information Practices to Consumers Required
Section 9. Information to be Included in Notices of Information Practices
Section 10. Short Form Initial Notice of Information Practices
Section 11. Form of Opt-In Notice to Consumers and Opt-In Methods
Section 12. Form of Opt-Out Notice to Consumers and Opt-Out Methods
Section 13. Revised Notice of Information Practices
Section 14. Notice of Information Practices to Group Policyholders
Section 15. Delivery

ARTICLE V. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 16. General Rules for Use and Disclosure of Nonpublic Personal Information
Section 17. Limits on Redisclosure and Reuse of Nonpublic Personal Information
Section 18. Limits on Sharing Access Number or Access Code Information for Marketing Purposes
Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted Advertising
Section 20. Limits on Sale of Nonpublic Personal Information
Section 21. Limits on Disclosure of Sensitive Personal Information

© 2026 National Association of Insurance Commissioners

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 22. Exception to Opt Out Requirements for Disclosure of Nonpublic Personal Information for Service Providers and Joint Marketing
Section 23. Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Information for Processing and Servicing Transactions
Section 24. Other Exceptions to Notice and Opt Out Requirements for Disclosure of Nonpublic Personal Information

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 25. When Authorization Required for Disclosure of Nonpublic Personal Health Information
Section 26. Authorizations
Section 27 Authorization Request Delivery
Section 28. Relationship to Federal Rules
Section 29. Relationship to State Laws

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 30. Protection of Fair Credit Reporting Act
Section 31. Nondiscrimination
Section 32. Violation
Section 33. Severability
Section 34. Individual Remedies
Section 35. Effective Date

APPENDICES

Appendix A Sample Clauses
Appendix B Federal Model Privacy Form
Model Law Forms

© 2026 National Association of Insurance Commissioners

ARTICLE I. GENERAL PROVISIONS

Section 1. Purpose

Purpose. This Act governs the treatment of nonpublic personal health information and nonpublic personal information about individuals by all licensees of the state insurance department. This Act:

A. Requires a licensee to provide notice to individuals about its privacy policies and practices;

B. Describes the conditions under which a licensee may disclose nonpublic personal health information and nonpublic personal information about individuals to affiliates and nonaffiliated third parties; and

C. Provides methods for individuals to prevent a licensee from disclosing that information.

Drafting Note: Whether this model is adopted as an Act or Regulation will depend upon individual state law. If a state adopts the model as an Act, reference to the model as an Act should be updated throughout the model.

Section 2. Scope and Compliance

A. Scope. This Act applies to:

(1) Nonpublic personal information about individuals who obtain or are claimants or beneficiaries of products or services primarily for personal, family or household purposes from licensees. This Act does not apply to information about companies or about individuals who obtain products or services for business, commercial or agricultural purposes; and

(2) All nonpublic personal health information.

B. Compliance. A licensee domiciled in this state that is in compliance with this Act in a state that has not enacted laws or regulations that meet the requirements of Title V of the Gramm-Leach-Bliley Act (PL 102-106) may nonetheless be deemed to be in compliance with Title V of the Gramm-Leach-Bliley Act in the other state.

Drafting Note: Subsection B is intended to give licensees some guidance for complying with Title V of the Gramm-Leach-Bliley Act in those states that do not have laws or regulations that meet GLBA's privacy requirements.

© 2026 National Association of Insurance Commissioners

Section 3. Rule of Construction

The examples in this Act, the sample clauses in Appendix A, and the Federal Model Privacy Form in Appendix B of this Act are not exclusive. Compliance with an example, use of a sample clause, or the Federal Privacy Model Form, to the extent applicable, constitutes compliance with this Act.

Licensees may rely on use of the Federal Privacy Form in Appendix B, consistent with the attached instructions, as a safe harbor of compliance with the Notice of Information Practices content requirements of this Act.

Use of the Federal Model Privacy Form is not required. Licensees may continue to use other types of privacy notices, including notices that contain the examples in this Act and/or the sample clauses in Appendix A, provided that such notices accurately describe the Licensee's privacy practices and otherwise meet the notice content requirements of this Act.

Section 4. Definitions

As used in this Act, unless the context requires otherwise:

A. "Affiliate" means a company that controls, is controlled by or is under common control with another company.

B. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a voiceprint, eye retinas, irises, genetic information or other unique biological patterns or characteristics that are used to identify a specific individual. "Biometric data" does not include a digital or physical photograph, an audio or video recording, or any data generated from a digital or physical photograph, or an audio or video recording, unless such data is generated to identify a specific individual.

C. ~~(1)~~ "Reasonably understandable" means Information presented in a way that an average, non-expert reader can grasp without unusual effort. ~~Clear and conspicuous" means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.~~

~~(2) Examples.~~

~~(a)~~ Examples: ~~Reasonably understandable.~~ A licensee makes its notice reasonably understandable if it:

(a~~i~~) Presents the information in the notice in clear, concise sentences, paragraphs and sections;

(b~~ii~~) Uses short explanatory sentences or bullet lists whenever possible;

(c~~iii~~) Uses definite, concrete, everyday words and active voice whenever possible;

(d~~iv~~) Avoids multiple negatives;

(e~~v~~) Avoids legal and highly technical business terminology whenever possible; and

© 2026 National Association of Insurance Commissioners

(fvi) Avoids explanations that are imprecise and readily subject to different interpretations.

(2b) "Conspicuous" means the notice is dDesigned to call attention to it. Examples: A licensee designs its notice to call attention to the nature and significance of the information in it if the licensee:

(ai) Uses a plain-language heading to call attention to the notice;

(bii) Uses a typeface and type size that are easy to read;

(ciii) Provides wide margins and ample line spacing;

(div) Uses boldface or italics for key words; and

(ev) if the notice is iIn a form that combines the licensee's notice with other information, uses distinctive type size, style, and graphic devices, such as shading or sidebars.

(fc) Notices on web sites. If a licensee provides a notice on a web page, the licensee designs its notice to ~~call attention to the nature and significance of the information in it~~be conspicuous if the licensee uses text or visual cues to encourage scrolling down the page if necessary to view the entire notice, uses recognizable labels, and ensures that other elements on the web site (such as text, graphics, hyperlinks or sound) do not distract attention from the notice, and the licensee either:

(i) Places the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(ii) Places a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

(g) Notices on digital applications. If a licensee provides a notice on a digital application, the notice shall be considered conspicuous if the licensee uses text or visual cues to encourage scrolling down the screen if necessary to view the entire notice, uses recognizable labels, and ensures that other elements on the application (such as text, graphics, hyperlinks or sound) do not distract attention from the notice, and the licensee either:

(i) Places the notice on a screen that consumers frequently access, such as through the application's settings menu or on the application's platform or download page; or

(ii) Places a link on a screen that consumers frequently access, , such as through the application's settings menu or on the application's platform or download page, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

(3) "Accessible" means consumers can easily find, understand, and use information without unnecessary barriers. Notices are considered to be accessible if:

Commented [CR1]: We leave to PPWG the task of moving placement of this definition of "reasonably understandable" to its proper place in Section 4, based on alphabetical order.

© 2026 National Association of Insurance Commissioners

(a) They are available in the languages in which the licensee in its ordinary course of business provides contracts, disclaimers, sale announcements, and other information to consumers.

(b) Licensee has taken reasonable measures to make the notice accessible to consumers with disabilities, such as:

(i) Following current generally recognized industry standards, such as the Web Content Accessibility Guidelines, version 2.1, from the World Wide Web Consortium, or the most recent version for online notices.

(j) Taking reasonable steps to ensure that consumers with disabilities may access the notices in an alternative format.

Commented [CR2]: We leave to PPWG the task of moving placement of this definition of "accessible" to its proper place in Section 4, based on alphabetical order.

D. "Collect" means to obtain information that the licensee organizes or can retrieve by the name of an individual or by identifying number, symbol or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

E. "Commissioner" means the chief insurance regulatory official of the state.

Drafting Note: Use the title of the chief insurance regulatory official wherever the term "commissioner" appears. If the jurisdiction of certain health licensees, such as health maintenance organizations, lies with some state agency other than the insurance department, or if there is dual regulation, a state should add language referencing that agency to ensure the appropriate coordination of responsibilities.

F. "Company" means a corporation, limited liability company, business trust, general or limited partnership, association, sole proprietorship or similar organization.

G. (1) "Consumer" means an individual who seeks to obtain, obtains or has obtained an insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, and about whom the licensee has nonpublic personal information, or that individual's legal representative.

(2) Examples.

(a) An individual who provides nonpublic personal information to a licensee in connection with obtaining or seeking to obtain financial, investment or economic advisory services relating to an insurance product or service is a consumer regardless of whether the licensee establishes an ongoing advisory relationship.

(b) An applicant for insurance prior to the inception of insurance coverage is a licensee's consumer.

(c) An individual who is a consumer of another financial institution is not a licensee's consumer solely because the licensee is acting as agent for, or provides processing or other services to, that financial institution.

(d) An individual is a licensee's consumer if:

© 2026 National Association of Insurance Commissioners

(i) (I) The individual is a beneficiary of a life insurance policy underwritten by the licensee;

(II) The individual is a claimant under an insurance policy issued by the licensee;

(III) The individual is an insured or an annuitant under an insurance policy or an annuity, respectively, issued by the licensee; or

(IV) The individual is a mortgagor of a mortgage covered under a mortgage insurance policy; and

(ii) The licensee discloses nonpublic personal information about the individual to a nonaffiliated third party other than as permitted under Sections 22, 23, and 24 of this Act.

(e) Provided that the licensee provides the initial, annual and revised notices under Sections 7, 8, and 13 of this Act to the plan sponsor, group or blanket insurance policyholder or group annuity contractholder, or workers' compensation policyholder, and further provided that the licensee does not disclose to a nonaffiliated third party nonpublic personal financial information about an individual described in Item (i), (ii) or (iii), other than as permitted under Sections 22, 23, or 24 of this Act, such an individual is not the consumer of the licensee solely because he or she is:

(i) A participant or a beneficiary of an employee benefit plan that the licensee administers or sponsors or for which the licensee acts as a trustee, insurer or fiduciary;

(ii) Covered under a group or blanket insurance policy or group annuity contract issued by the licensee; or

(iii) A claimant covered by a workers' compensation plan.

Drafting Note: In states where the workers' compensation self-insurance or workers' compensation state fund coverage is outside the commissioner's jurisdiction, regulators may wish to urge the applicable agency or agencies to promulgate a regulation similar to this Act in order to ensure parity in treatment of workers' compensation plans and to ensure that all workers covered by such plans have privacy protections.

(f) (i) The individuals described in Subparagraph (e)(i) through (iii) of this paragraph are consumers of a licensee if the licensee does not meet all the conditions of Subparagraph (e).

(ii) In no event shall the individuals, solely by virtue of the status described in Subparagraph (e)(i) through (iii) above, be deemed to be consumers for purposes of this Act.

(g) An individual is not a licensee's consumer solely because he or she is a beneficiary of a trust for which the licensee is a trustee.

© 2026 National Association of Insurance Commissioners

(h) An individual is not a licensee's consumer solely because he or she has designated the licensee as trustee for a trust.

H. "Consumer reporting agency" has the same meaning as in Section 603(f) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

I. "Control" means:

(1) Ownership, control or power to vote twenty-five percent (25%) or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

(2) Control in any manner over the election of a majority of the directors, trustees or general partners (or individuals exercising similar functions) of the company; or

(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company, as the commissioner determines.

J. "De-identified data" means information that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual.

K. (1) "Financial institution" means any institution the business of which is engaging in activities that are financial in nature or incidental to such financial activities as described in Section 1843(k)(4)(B**)** of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial institution does not include:

(a) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 *et seq.*);

(b) The Federal Agricultural Mortgage Corporation or any entity charged and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 *et seq.*); or

(c) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as the institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party.

L. (1) "Financial product or service" means a product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under Section 1843(k)(4)(B**)** of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)).

(2) Financial service includes a financial institution's evaluation or brokerage of information that the financial institution collects in connection with a request or an application from a consumer for a financial product or service.

© 2026 National Association of Insurance Commissioners

M. "Insurance product or service" means any product or service that is offered by a licensee pursuant to the insurance laws of this state.

N. (1) "Licensee" means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Insurance Law of this state, [and health maintenance organizations holding a certificate of authority pursuant to Section [insert section] of this state's Public Health Law].

Drafting Note: Add bracketed language if HMOs are licensed under other than insurance statutes and cite appropriate state law.

(2) A licensee is not subject to the notice and opt out requirements for nonpublic personal information set forth in Articles I, II, III and IV of this Act if the licensee is an employee, agent or other representative of another licensee ("the principal") and:

(a) The principal otherwise complies with, and provides the notices required by, the provisions of this Act; and

(b) The licensee does not disclose any nonpublic personal information to any person other than the principal or its affiliates in a manner permitted by this Act.

(3) (a) Subject to Subparagraph (b), "licensee" shall also include an unauthorized insurer that accepts business placed through a licensed excess lines broker in this state, but only in regard to the excess lines placements placed pursuant to Section [insert section] of this state's laws.

(b) An excess lines broker or excess lines insurer shall be deemed to be in compliance with the notice and opt out requirements for nonpublic personal information set forth in Articles I, II, III and IV of this Act provided:

(i) The broker or insurer does not disclose nonpublic personal information of a consumer to nonaffiliated third parties for any purpose, including joint servicing or marketing under Section 22 of this Act, except as permitted by Section 23 or 24 of this Act; and

(ii) The broker or insurer delivers a notice to the consumer at the time a consumer relationship is established on which the following is printed in 16-point type:

NOTICE OF INFORMATION PRACTICES
"Neither the U.S. brokers that handled this insurance nor the insurers that have underwritten this insurance will disclose nonpublic personal information concerning the buyer to nonaffiliates of the brokers or insurers except as permitted by law."

Drafting Note: References to "excess lines broker" and "excess lines insurer" should be changed as necessary to correspond with the applicable terms used in each state.

O. (1) "Nonaffiliated third party" means any person except:

© 2026 National Association of Insurance Commissioners

(a) A licensee's affiliate; or

(b) A person employed jointly by a licensee and any company that is not the licensee's affiliate (but nonaffiliated third party includes the other company that jointly employs the person).

(2) Nonaffiliated third party includes any company that is an affiliate solely by virtue of the direct or indirect ownership or control of the company by the licensee or its affiliate in conducting merchant banking or investment banking activities of the type described in Section 4(k)(4)(H) or insurance company investment activities of the type described in Section 4(k)(4)(I) of the federal Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

P. "Nonpublic personal health information" means any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of an individual;

(2) The provision of health care to an individual; or

(3) Payment for the provision of health care to an individual.

Q. "Nonpublic personal information" means any personally identifiable information that is linked or reasonably linkable to an identified natural person. Nonpublic personal information does not include de-identified data or publicly available information.

R. (1) "Personally identifiable information" means any information:

(a) A consumer provides to a licensee to obtain an insurance product or service from the licensee;

(b) About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

(c) The licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.

(2) Examples.

(a) Information included. Personally identifiable information includes:

(i) Information a consumer provides to a licensee on an application to obtain an insurance product or service;

(ii) Account balance information and payment history;

(iii) The fact that an individual is or has been one of the licensee's consumers or has obtained an insurance product or service from the licensee;

© 2026 National Association of Insurance Commissioners

(iv) Any information about the licensee's consumer if it is disclosed in a manner that indicates that the individual is or has been the licensee's consumer;

(v) Any information that a consumer provides to a licensee or that the licensee or its agent otherwise obtains in connection with collecting on a loan or servicing a loan;

(vi) Any information the licensee collects through an Internet cookie (an information-collecting device from a web server); and

(vii) Information from a consumer report.

(b) Information not included. Personally identifiable information does not include:

(i) A list of names and addresses of customers of an entity that is not a financial institution; and

(ii) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names or addresses.

S. "Opt in" means an affirmative direction by a consumer that authorizes a licensee to disclose the consumer's information.

T. "Opt out" means a direction by a consumer that the licensee may not disclose nonpublic personal information about the consumer to a nonaffiliated third party, except as permitted under Sections 22,23, or 24 .

U. (1) "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

(a) Federal, state or local government records;

(b) Widely distributed media; or

(c) Disclosures to the general public that are required to be made by federal, state or local law.

(2) Reasonable basis. A licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

(a) That the information is of the type that is available to the general public; and

(b) Whether an individual can direct that the information not be made available to the general public and, if so, that the licensee's consumer has not done so.

© 2026 National Association of Insurance Commissioners

(3) Examples.

(a) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.

(b) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.

(c) Reasonable basis.

(i) A licensee has a reasonable basis to believe that mortgage information is lawfully made available to the general public if the licensee has determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.

(ii) A licensee has a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if the licensee has located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.

V. "Reasonable opportunity" means any of the following:

(1) The licensee mails the notices required to the consumer and allows the consumer to opt out by mailing a form, calling a toll-free telephone number or any other reasonable means within sixty (60) days from the date the licensee mailed the notices;

(2) Where a consumer agrees to receive the notices required by this Act electronically in accordance with UETA [insert state electronic transactions act statute], the licensee allows the consumer to opt out by any reasonable means at any time; or

(3) For an isolated transaction, such as providing the consumer with an insurance quote, the licensee provides the notices required by this Act at the time of the transaction and requests that the consumer decide, as a necessary part of the transaction.

X. "Sale" or "selling" means the exchange of nonpublic personal information for monetary or other valuable consideration. A licensee does not sell nonpublic personal information when:

(1) The disclosure is to a third party for the purpose of or in support of providing a product or service requested by the consumer.

(2) A licensee provides information to or receives anything of value from an insurance

© 2026 National Association of Insurance Commissioners

support organization, statistical agent, or reinsurer;

(3) A licensee provides nonpublic personal information to an affiliate or to a financial institution with which the licensee performs joint marketing;

(4) The business transfers to a third party the nonpublic personal information as an asset that is part of a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction in which the party assumes control of all or part of the licensee's assets; or

(5) A consumer uses or directs the business to (i) disclose nonpublic personal information; or (ii) interact with one or more third parties including but not limited to referrals to other licensees.

Y. "Sensitive Personal Information" means personally identifiable "nonpublic personal information" about a consumer that includes:

(1) Racial or ethnic origin, religious beliefs, sexual orientation, or citizenship or citizenship status; or

(2) Genetic information or biometric data that may be processed for the purpose of uniquely identifying an individual.

(3) Any nonpublic health information that is not covered by the federal Health Insurance Portability and Accountability Act or other federal and state regulations, including:

a. Past, present, or future physical, mental or behavioral health or condition of an individual;
b. The provision of healthcare to an individual; or
c. Payment for the provision of healthcare or healthcare-related devices, supplies, or mobile apps to an individual.

~~(2)~~(4) All nonpublic personal information of individuals who are 18 years old or younger.

Z. (1) "Targeted advertising" means displaying advertisements to a consumer where the advertisement is selected based on personal data obtained from that consumer's activities over time and across nonaffiliated websites or online applications to predict such consumer's preferences or interests.

(2) "Targeted advertising" does not include:

(a) Online advertisements based on activities within a Licensee's own websites or online applications;

(b) Online advertisements based on the context of a consumer's current search query, visit to a website, or online application;

(c) Online advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(d) Processing Nonpublic Personal Information solely for measuring or reporting

© 2026 National Association of Insurance Commissioners

advertising performance, reach, or frequency.

AA. "Third party service provider" or "third party" means a person or entity not otherwise defined as a licensee or affiliate of a licensee that:

(1) Provides services to the licensee; and

(2) Maintains, processes or otherwise is permitted access to nonpublic personal information through its provisions of services to the licensee.

© 2026 National Association of Insurance Commissioners

ARTICLE II. THIRD-PARTY SERVICE PROVIDER ARRANGEMENTS

Section 5. Third-Party Service Provider Arrangements

A. Contract Requirements.

A licensee that discloses a consumer's nonpublic personal information to a third-party service provider shall enter into a written contract with the third-party service provider that:

(1) Prohibits the third-party service provider from processing the nonpublic personal information for any purpose other than those related to providing the services specified in the contract with the licensee, unless processing is necessary to comply with the law or a valid and binding order of a governmental body, in which case the third-party service provider must notify the licensee within 48 hours unless prohibited by law;

(2) Requires the third-party service provider to delete, destroy, de-identify or return all nonpublic personal information to the licensee when requested by the licensee; or to delete nonpublic personal information after it is no longer necessary to fulfill a legal requirement or to meet the record retention requirements of the licensee or third-party service provider, and to notify the licensee of the action taken;

(3) Requires the third-party service provider to notify the licensee if it can no longer comply with its obligations under this contract and provides the licensee with a right to terminate the contract;

(4) Requires that any contract between a third-party service provider and a subcontractor with access to a consumer's nonpublic personal information must contain provisions no less protective of nonpublic personal information than those contained in the third-party service provider's agreement with the licensee;

(5) Requires the third-party service provider to provide assistance to the licensee in fulfilling obligations to respond to consumer requests under Article III of this Act;

(6) Requires the third-party service provider to implement and maintain administrative, technical, and physical data security practices to protect the nonpublic personal information from unauthorized access, destruction, use, modification, or disclosure;

(7) Requires the third-party service provider to notify the licensee of a failure to meet the obligations of Subsections (1) to (6) above within 48 hours of discovery by the third-party service provider.

B. A licensee that discloses a consumer's nonpublic personal information to a third-party service provider remains fully responsible for compliance with this Act and the handling of nonpublic personal information.

© 2026 National Association of Insurance Commissioners

ARTICLE III. CONSUMER REQUESTS

Section 6. Access, Correction, and Deletion of Nonpublic Personal Information

A. A consumer may file the following requests with a licensee, which shall be processed in accordance with the following standards:

(1) Within 45 days of receiving an authenticated request from a consumer for their nonpublic personal information, a licensee shall disclose:

(a) All nonpublic personal information about the consumer that is maintained by the licensee or any contracted third-party service provider; and

(b) A list of all third-party service providers to whom the licensee disclosed the consumer's nonpublic personal information.

(2) A licensee shall not be required to disclose the following:

(a) A consumer's Social Security Number, driver's license number or other government-issued identification number, financial account number(s), any health insurance or medical identification number, any account password(s), security questions and answers, unique biometric data or other information that could create a high risk of identity theft. The licensee may instead disclose the types of nonpublic personal information maintained by listing each type of nonpublic personal information it has about the consumer;

(b) Duplicative nonpublic personal information, if it is described in a manner reasonably understandable by the consumer and the consumer is offered an opportunity to review the nonpublic personal information for inconsistencies; or

(c) Information that is outside the scope of the request, if the consumer has requested only specified items or categories of information.

B. Correction of nonpublic personal information.

(1) A consumer may make an authenticated request for the correction of their nonpublic personal information by filing a request with the licensee that:

(a) Identifies the specific nonpublic personal information the consumer wishes to correct; and

(b) Provides an explanation of why the nonpublic personal information is incorrect.

(2) Within 45 days of receipt of the request under this subsection, a licensee shall take one of the following actions and notify the consumer:

(a) Correct the nonpublic personal information in dispute as requested by the consumer;

© 2026 National Association of Insurance Commissioners

(b) Delete the nonpublic personal information in dispute; or

(c) Deny the request and provide:

(i) The basis for refusal to correct the nonpublic personal information as requested;

(ii) Information about how the consumer may appeal the denial; and

(iii) An explanation of how the appeal will be reviewed and how the consumer will be notified of the decision on appeal.

(3) A licensee may deny a request for correction if:

(a) The nonpublic personal information is accurate and complete and if the licensee provides a process for appeal of the decision; or

(b) The nonpublic personal information that is the subject of the request was not created by the licensee, unless there is a reasonable basis to believe that the originator of the nonpublic personal information is no longer available to act on the requested correction, and the consumer has independently demonstrated the information is incorrect.

~~(b)~~(c) If the nonpublic personal information that is the subject of the request was not created by the licensee, and there is reasonable basis to believe that the originator of the nonpublic information is available to act on the requested correction, then the licensee shall provide the consumer with the identity of the originator and information on how to contact the originator to correct the information.

C. Deletion of nonpublic personal information.

(1) Within 45 days of an authenticated request from a consumer, a licensee shall delete the nonpublic personal information about the consumer that is maintained by the licensee or direct a third-party service provider to delete the nonpublic personal information on the licensee's behalf.

(2) The licensee is not required to delete nonpublic personal information if:

(a) The licensee is required by law or regulation to retain the nonpublic personal information;

(b) The nonpublic personal information may be necessary to perform the contract or service requested by or benefiting the consumer;

(c) The information is necessary to comply with a legal obligation; or

(d) The information is maintained in reasonable anticipation of a claim or civil or criminal proceeding.

© 2026 National Association of Insurance Commissioners

(3) A licensee may delay fulfilling a consumer's request, up to 45 days, to delete nonpublic personal information stored on an archived or backup system. A licensee must notify the consumer of such delay. During this delay, the licensee shall not share that information with any third parties.

D. Request and Response Procedures

(1) Except as provided in Subsection D(1)(b), a licensee shall respond to requests submitted under this section within 45 days in the following manner:

(a) A licensee may use its secure communications portal to authenticate requests from consumers holding current accounts with the licensee, unless the licensee has reason to believe the request has been submitted through an account that has been compromised. Otherwise, the licensee may use methods that are commercially reasonable, but not unduly burdensome, to authenticate the identity of the person making the request and to verify that this person is either:

(i) The consumer;

(ii) A person acting with the consumer's written authorization, including but not limited to a valid power of attorney;

(iii) The parent or legal guardian of a consumer who is a minor, except where the information relates to health insurance claims in circumstances where the child has a legal right to obtain the services in question without the parent's or guardian's consent;

(iv) The legal guardian or other person authorized by law to act on behalf of an incapacitated consumer; or

(v) The personal representative or other person authorized by law to act on behalf of a deceased consumer.

(b) A licensee is required to notify the consumer if either of the following prevents the licensee from complying with the request:

(i) The specific nonpublic personal information at issue is not locatable or retrievable by the licensee; or

Drafting Note: Examiners should review licensees' notifications to consumers regarding nonpublic personal information that is not locatable or retrievable by the licensee and its justifications for irretrievability during Market Conduct and/or IT Exams.

(ii) The licensee is unable to verify the request after requesting that the consumer provide additional information necessary to authenticate the identity of the consumer and authenticate the consumer's request.

(c) If a licensee declines the consumer's request, the licensee shall inform the consumer of the basis for declining the request and provide instructions for how to request review of the decision.

© 2026 National Association of Insurance Commissioners

(2) There shall be no cap on the number of requests to correct or delete nonpublic personal information.

(3) If a consumer disagrees with a licensee's refusal to correct or delete nonpublic personal information per the consumer's request, the consumer shall be permitted to file with the licensee:

(a) A concise statement setting forth why the consumer disagrees with the licensee's refusal and what the consumer thinks is the correct, relevant or fair information; and

(b) The licensee shall maintain the statement with the disputed nonpublic personal information and allow anyone reviewing the disputed nonpublic personal information to be made aware of the dispute and have access to the consumer's statement.

© 2026 National Association of Insurance Commissioners

ARTICLE IV. NOTICE OF INFORMATION PRACTICES AND OPT-OUT AND OPT-IN NOTICES FOR NONPUBLIC PERSONAL INFORMATION

Section 7. Initial and Subsequent Delivery Notice of Information Practices to Consumers Required

A. Initial Delivery of Notice. A licensee shall provide a ~~clear~~ reasonably understandable, ~~and~~ conspicuous, and accessible notice that accurately reflects its privacy policies and practices to all consumers no later than when the licensee obtains access to the consumer's nonpublic personal information, except that a licensee may provide the initial notice within a reasonable time after access to the consumer's nonpublic personal information if:

(1) Obtaining access to the consumer's nonpublic personal information is not at the consumer's election and the licensee follows the Notice of Information Practices previously sent to the consumer; or

(2) Providing notice when the licensee obtains access to the consumer's nonpublic personal information would substantially delay the consumer's transaction and the consumer agrees to receive the notice at a later time.

B. Subsequent Delivery of Notice

When a consumer with an existing relationship with a licensee obtains a new insurance product or service from a licensee that is to be used primarily for personal, family or household purposes, the licensee satisfies the initial notice requirements of Subsection A of this section as follows:

(1) The licensee may provide a revised notice, under Section 13 , that covers the consumer's new insurance product or service; or

(2) If the initial, revised or annual notice that the licensee most recently provided to that consumer was accurate with respect to the new insurance product or service, the licensee does not need to provide a new notice of information practices under Subsection A of this section.

C. For purposes of this section:

(1) "Not at consumer's election" includes the scenario where a licensee acquires or is assigned a consumer's policy from another financial institution or residual market mechanism and the consumer does not have a choice about the licensee's acquisition or assignment.

(2) "Substantially delay the consumer's transaction" includes the scenario where the licensee and the individual agree over the telephone or electronically to enter into a consumer relationship involving prompt delivery of the insurance product or service but does not include the scenario where the relationship is initiated in person at the licensee's office or through other means by which the consumer may view the notice, such as on a website.

D. Prohibition on Use of Dark Patterns

© 2026 National Association of Insurance Commissioners

The licensee shall not use, and shall not permit any third party acting on its behalf to use, a dark pattern in any privacy notice, privacy policy, consent request, preference center, cookie banner, or other interface through which an individual receives privacy information or makes a privacy-related choice.

A dark pattern means a user-interface design, content, default setting, workflow, or other practice that has the purpose or substantial effect of subverting, impairing, obscuring, delaying, pressuring, manipulating, or materially interfering with an individual's autonomy, decision-making, or ability to make an informed and voluntary privacy choice. Without limiting this prohibition, the licensee shall not:

(1) Use misleading, ambiguous, contradictory, or unnecessarily technical language;

(2) Preselect consent or privacy-invasive settings;

(3) Require more steps, time, information, or effort to decline, opt out, withdraw consent, or select a more privacy-protective option than to accept, opt in, or select a less privacy-protective option;

(4) Make one choice more visually prominent through unequal size, color, placement, wording, or repeated prompts in a manner that steers an individual's decision;

(5) Bundle separate processing purposes into a single consent choice when separate choice is feasible;

(6) Hide, obscure, or make privacy choices difficult to locate, understand, or exercise; or

(7) Condition a service on consent that is not necessary to provide that service.

Any consent or authorization obtained through a prohibited practice is invalid and shall not be relied upon as a legal basis for collecting, using, disclosing, selling, sharing, or otherwise processing personal information.

E. Providing Time to Respond to Initial and Subsequent Delivery Notices

Licensees shall not disclose nonpublic personal information for 30 days after a consumer has received an initial notice of information practices or a subsequent notice of information practices that provides new opt-in or opt-out options. This is to give the consumer time to review and respond to those options.

Section 8. Annual Notice of Information Practices to Consumers Required

General rule. A licensee shall provide a ~~clear and~~reasonably understandable, conspicuous, and accessible notice to consumers that accurately reflects its privacy policies and practices at least once in any period of twelve (12) consecutive months. A licensee may define the twelve-consecutive-month period, but the licensee shall apply it to the consumer on a consistent basis.

A. Example. A licensee provides a notice annually if it defines the twelve-consecutive-month period as a calendar year and provides the annual notice to the consumer once in each calendar year following the calendar year in which the licensee provided the initial notice. For example, if a consumer opens an account on any day of year 1, the licensee shall provide an annual notice to that consumer by December 31 of year 2.

© 2026 National Association of Insurance Commissioners

(1) Exceptions.

(1) A licensee that provides nonpublic personal information to nonaffiliated third parties only in accordance with Sections 22, 23, or 24 and has not changed its policies and practices with regard to disclosing Nonpublic Personal Information from the policies and practices that were disclosed in the most recent disclosure sent to consumers in accordance with this section or Section 7 shall not be required to provide an annual disclosure under this section until such time as the licensee fails to comply with any criteria described in this paragraph.

(2) A licensee is not required to provide notice if the licensee no longer has access to the consumer's nonpublic personal information.

(2) For the purposes of this Act, a licensee no longer has an obligation to continue to notify a consumer if the licensee's records do not contain a valid address. An address is deemed invalid if electronic or regular mail sent to that address by the licensee has been returned as undeliverable and if subsequent attempts by the licensee to obtain a current valid address for the individual have been unsuccessful.

Section 9. Information to be Included in Notices of Information Practices

A. General rule. The initial, annual and revised Notice of Information Practices that a licensee provides under Sections 7,8, and 13 shall include each of the following items of information, in addition to any other information the licensee wishes to provide, that applies to the licensee and to the consumers to whom the licensee sends its Notice of Information Practices:

(1) The categories of nonpublic personal information that the licensee collects, including, but not limited to, whether information is collected from the consumer, through the consumer's transactions with affiliates or nonaffiliated third parties, or consumer reporting agencies. The notices shall include at least the following categories, with examples of the types of nonpublic personal information for each category:

(a) **Identifiers:** Such as real name, alias, email address, Social Security number, passport number, Internet Protocol address, postal address and other contact information;

(b) **Classifications:** Such as race, gender, gender identity, age, religion, disability;

(c) **Financial Information:** Such as income, assets, past financial transactions, payment history;

(d) **Commercial information:** Such as personal property records, purchase history, preferences, insurance coverage and claims history;

(e) **Biometric Information:** Such as fingerprints, faceprints, voiceprints, genetic information;

(f) **Internet or Other Electronic Network Activity Information:** Such as browsing history, search history, interactions with chatbots, interactions with our

© 2026 National Association of Insurance Commissioners

website, social media activities;

(g) **Geolocation Data:** Such as your physical location or movements and travel patterns;

(h) **Audio, Electronic, Visual, Thermal, Olfactory, or Similar Information:** Such as audio recordings, electronic communications, video recordings;

(i) **Professional or Employment-Related Information:** Such as job history, professional qualifications;

(j) **Education Information:** Education information that is not publicly available;

~~(a)~~(k) **Inferences Drawn from Other Personal Information:** Such as creating a profile about a consumer based on the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.

(2) ~~The~~ Which categories of nonpublic personal information that the licensee collects are ~~discloses~~disclosed, including at least one example in each category. ~~Categories may include, but are not limited to, application information, transaction information, or consumer reports;~~

(3) The categories of affiliates and nonaffiliated third parties, and the types of business in which they engage, to whom the licensee discloses nonpublic personal information, other than those parties to whom the licensee discloses information under Sections 22, 23, and 24. The types of businesses may be described in general terms only if the licensee uses illustrative examples of each significant line of business;

(4) An explanation of the consumer's right under Section 12 to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the methods by which the consumer may exercise that right at that time;

(5) An explanation of the consumer's rights with regard to the sale of nonpublic personal information and disclosure of sensitive personal information pursuant to Sections 20 and 21;

(6) A description of the consumer's options to request access, correction, or deletion of nonpublic personal information about the consumer as established under this Act and the instructions for exercising such options;

(7) Any disclosures that the licensee makes under Section 603(d)(2)(A)(iii) of the federal Fair Credit Reporting Act (15 U.S.C. 1681a(d)(2)(A)(iii)) (that is, notices regarding the ability to opt out of disclosures of information among affiliates);

(8) The licensee's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information; by

(a) Describing in general terms who is authorized to have access to the information; and

© 2026 National Association of Insurance Commissioners

(b) Stating whether the licensee has security practices and procedures in place to ensure the confidentiality of the information in accordance with the licensee's policy. The licensee is not required to describe technical information about the safeguards it uses; and

(c) Any disclosure that the licensee makes as authorized under Section 22, 23, or 24, except that the licensee is not required to list those exceptions in the initial or annual Notice of Information Practices required by Sections 7 and 8. When describing the categories of parties to whom disclosure is made, the licensee is required to state only that it makes disclosures to other affiliated or nonaffiliated third parties, as applicable, as permitted by law.

B. The licensee's notice may include:

(1) Categories of nonpublic personal information that the licensee reserves the right to disclose in the future, but does not currently disclose; and

(2) Categories of affiliates or nonaffiliated third parties to whom the licensee reserves the right in the future to disclose, but to whom the licensee does not currently disclose, nonpublic personal information.

C. Exceptions:

If a licensee does not disclose, and does not reserve the right to disclose, nonpublic personal information about consumers to affiliates or nonaffiliated third parties except as authorized under Sections22, 23, or 24, the licensee shall state that in its notice, in addition to the information it shall provide under Subsections A(1) and A(8) and Subsection B of this section.

D. Sample Clauses and Federal Model Privacy Form.

(1) Licensees are not required to use any prescribed clauses or model form.

(2) The commissioner may determine that a Licensee's use of any of the following constitutes compliance with this Act:

(a) Sample clauses illustrating some of the notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner;

(b) Model forms illustrating notice content required by this section which are developed by the National Association of Insurance Commissioners or the commissioner; or

(c) The Federal Model Privacy Forms are included in Appendix A and Appendix B, of this Act.

© 2026 National Association of Insurance Commissioners

Section 10. Short Form Initial Notice of Information Practices

A. A licensee may satisfy the initial notice requirements in Sections 7A and 13A by providing a Short Form Initial Notice of Information Practices at the same time the licensee delivers an opt-out notice as required in Section 12 if:

(1) The licensee provides the consumer a reasonable means to obtain its Notice of Information Practices; and

(2) The licensee provides the Notice of Information Practices upon request.

B. A Short Form Initial Notice of Information Practices shall meet all of the following requirements.

(1) Be ~~clear~~ reasonably understandable, ~~and~~ conspicuous, and accessible;

(2) State that the licensee's Notice of Information Practices is available upon request;

(3) Explain the reasonable means to obtain the licensee's Notice of Information Practices;

(4) Contain contact information for the commissioner; and

(5) Describe how the consumer can request access to or correction of their nonpublic personal information.

C. For purposes of this section "reasonable means to obtain the licensee's Notice of Information Practices" includes:

(1) Providing a toll-free telephone number that the consumer may call to request the notice;

(2) Providing a website or other electronic medium that is easily accessible by the consumer; or

(3) Maintaining copies of the notice at the licensee's place of business to be provided upon request.

Section 11. Form of Opt-In Notice to Consumers and Opt-In Methods

A. If a licensee is required to provide an opt-int notice under Sections 20 or 21, it shall provide a ~~clear and~~reasonably understandable, conspicuous, and accessible notice to each of its consumers that accurately explains the information proposed to be disclosed, the use of that information, and the consumer's option to opt in to that use. The notice shall state:

(1) The licensee discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;

(2) The consumer has the option to opt in to that disclosure; and

(3) A reasonable means by which the consumer may exercise the option to opt in.

B. The licensee shall not disclose that information to a nonaffiliated third party unless the consumer has affirmatively opted in to the use.

© 2026 National Association of Insurance Commissioners

C. The opt-in must be an affirmative act by the consumer. The licensee cannot deem a failure to respond as an opt-in or use pre-checked boxes.

D. The opt-in should be obtained separately from any other communication or consent.

E. The opt-in may be revoked at any time by the consumer.

F. Unless stated herein clearly and specifically, if a licensee wishes to sell or share NPI for purposes in whole or in part beyond providing insurance to a consumer, then the licensee can only do so if the consumer opts-in.

G. A licensee cannot provide NPI to a large learning AI model, unless the consumer has agreed to do so via an opt-in.

Commented [CR3]: We have added Section 11.F for two reasons. 1) Sharing NPI should only be used for insurance purposes, unless a consumer opts-in to its use more broadly. 2) If situations arise where there is ambiguity under this Model whether opt-in or opt-out applies, then opt-in should apply.

Section 12. Form of Opt-Out Notice to Consumers and Opt-Out Methods

A. (1) If a licensee is required to provide an opt-out notice, it shall provide a ~~clear and~~reasonably understandable, ~~-~~conspicuous, and accessible ~~-~~notice to each consumer that accurately explains the right to opt out under that section. To the extent applicable, the notice shall state:

(a) That the licensee discloses or reserves the right to disclose nonpublic personal information about its consumer to a nonaffiliated third party;

(b) That the consumer has the right to opt out of that disclosure; and

(c) A reasonable means by which the consumer may exercise the opt-out right.

(2) Requirements

(a) A licensee provides adequate notice that the consumer can opt out of the disclosure of nonpublic personal information to a nonaffiliated third party if the licensee:

(i) Identifies all of the categories of nonpublic personal information it discloses or reserves the right to disclose, and all of the categories of nonaffiliated third parties to whom the licensee discloses the information, as described in Section 9A(2) and (3), and states the consumer can opt out of the disclosure of that information; and

(ii) Identifies the insurance products or services the consumer obtains from the licensee, either singly or jointly, to which the opt-out would apply.

(iii) The categories that should be identified shall include at least the following and examples of nonpublic information in each should be provided:

- **Identifiers:** Such as real name, alias, email address, Social Security number, passport number, Internet Protocol address, postal address and other contact information;
- **Classifications:** Such as race, gender, gender identity, age, religion, disability;

© 2026 National Association of Insurance Commissioners

- **Financial Information:** Such as income, assets, past financial transactions, payment history;
- **Commercial information:** Such as personal property records, purchase history, preferences, insurance coverage and claims history;
- **Biometric Information:** Such as fingerprints, faceprints, voiceprints, genetic information;
- **Internet or Other Electronic Network Activity Information:** Such as browsing history, search history, interactions with chatbots, interactions with our website, social media activities;
- **Geolocation Data:** Such as your physical location or movements and travel patterns;
- **Audio, Electronic, Visual, Thermal, Olfactory, or Similar Information:** Such as audio recordings, electronic communications, video recordings;
- **Professional or Employment-Related Information:** Such as job history, professional qualifications;
- **Education Information:** Education information that is not publicly available;
- **Inferences Drawn from Other Personal Information:** Such as creating a profile about a consumer based on the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.

(b) A licensee provides a reasonable means to exercise an opt-out right if it:

(i) Designates check-off boxes in a prominent position on the relevant forms with the opt-out notice;

(ii) Includes a reply form together with the opt-out notice;

(iii) Provides an electronic means to opt out, such as a form that can be sent via electronic mail or a process at the licensee's website, if the consumer agrees to the electronic delivery of information; or

(iv) Provides a toll-free telephone number that consumers may call to opt out.

(c) A licensee does not provide a reasonable means of opting out if:

(i) The only means of opting out is for the consumer to write a letter to the licensee to exercise their opt-out right; or

(ii) The only means of opting out as described in any notice subsequent to the initial notice is to use a check-off box that the licensee provided with the initial notice but did not include with the subsequent notice.

(d) A licensee may require each consumer to opt out through a specific means, as long as that means is reasonable for that consumer.

© 2026 National Association of Insurance Commissioners

B. A licensee may provide the opt-out notice together with or on the same written or electronic form as the initial notice the licensee provides in accordance with Section 7.

C. If a licensee provides the opt-out notice after it provides the initial notice, the licensee shall include a copy of the initial notice with the opt-out notice in writing or, if the consumer agrees, electronically.

D. Joint relationships.

(1) If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may provide a single opt-out notice. The licensee's opt-out notice shall explain how the licensee will treat an opt-out direction by a joint consumer (as explained in Paragraph (2) of this subsection).

(2) Any of the joint consumers may exercise the right to opt out. The licensee may either:

(a) Treat an opt-out direction by a joint consumer as applying to all of the associated joint consumers; or

(b) Permit each joint consumer to opt out separately.

(3) If a licensee permits each joint consumer to opt out separately, the licensee shall permit one of the joint consumers to opt out on behalf of all the joint consumers.

(4) A licensee may not require all joint consumers to opt out before it implements any opt-out direction.

E. A licensee shall comply with a consumer's opt-out direction as soon as reasonably practicable but no later than 10 days after the licensee receives it.

F. A consumer may exercise the right to opt out at any time. A consumer's direction to opt-out under this section is effective until the consumer revokes it in writing or, if the consumer agrees, electronically.

Section 13. Revised Notice of Information Practices

A. Except as otherwise authorized in this Act, a licensee shall not, directly or through an affiliate, disclose any nonpublic personal information about a consumer to a nonaffiliated third party other than as described in the initial notice that the licensee provided to that consumer under Section 7, unless:

(1) The licensee has provided to the consumer a ~~clear and~~reasonably understandable, conspicuous, and accessible revised notice that accurately describes its policies and practices;

(2) The licensee has provided to the consumer a new opt-out notice;

(3) The licensee has given the consumer a reasonable opportunity, before the licensee discloses the information to the nonaffiliated third party, to opt out of the disclosure; and

(4) The consumer does not opt out.

© 2026 National Association of Insurance Commissioners

B. Examples.

(1) Except as otherwise permitted by Sections 19, 20 and 21, a licensee shall provide a revised notice before it:

(a) Discloses a new category of nonpublic personal information to any nonaffiliated third party; or

(b) Discloses nonpublic personal information to a new category of nonaffiliated third party.

(2) A revised notice is not required if the licensee discloses nonpublic personal information to a new nonaffiliated third party that the licensee adequately described in its prior notice.

Section 14. Notice of Information Practices to Group Policyholders

Unless a licensee is providing notices of information practices directly to covered individuals described in Section 4G)2)(e)(i), (ii) or (iii), a licensee shall provide initial, annual and revised notices to the plan sponsor, group or blanket insurance policyholder or group annuity contract holder, or workers' compensation policyholder, in the manner described in Sections 7 through 13 of this Act, describing the licensee's privacy practices with respect to nonpublic personal information about individuals covered under the policies, contracts or plans. Compliance with this section satisfies the licensees initial, annual and renewal Notice of Information Practices as required by Sections 7 and 8 and delivery provisions of Section 15.

Section 15. Delivery

A. A licensee shall provide any notices that this Act requires so that each consumer can reasonably be expected to receive actual notice in writing or, if the consumer interacts with the licensee online or in some other electronic fashion, electronically.

B. (1) A licensee may reasonably expect that a consumer will receive actual notice if the licensee:

(a) Hand-delivers a printed copy of the notice to the consumer;

(b) Mails a printed copy of the notice to the last known address of the consumer separately, or in a policy, billing or other written communication;

(c) For a consumer who conducts transactions electronically, in accordance with UETA (insert state electronic transactions act statute), posts the notice on the electronic site and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining a particular insurance product or service;

(i) The notice should be posted in a manner that enables a consumer to print or save it using programs or apps that are widely available and free of charge.

© 2026 National Association of Insurance Commissioners

(ii) Notice is available electronically as long as it is in force.

(d) For an isolated transaction with a consumer, such as the licensee providing an insurance quote or selling the consumer travel insurance, posts the notice and requires the consumer to acknowledge receipt of the notice as a necessary step to obtaining the particular insurance product or service.

(e) Provides the notice by any other means authorized by the commissioner.

(2) Examples of unreasonable expectation of actual notice. A licensee may not, however, reasonably expect that a consumer will receive actual notice of its privacy policies and practices if it:

(a) Only posts a sign in its office or generally publishes advertisements of its privacy policies and practices; or

(b) Sends the notice via electronic mail to a consumer who does not otherwise communicate with the licensee electronically.

C. A licensee may reasonably expect that a consumer will receive actual notice of the licensee's Notice of Information Practices if:

(1) The consumer uses the licensee's web site to access insurance products and services electronically and agrees to receive notices at the web site and the licensee posts its current privacy notice continuously in a ~~clear and~~ reasonably understandable, conspicuous, and accessible manner on the web site; or

(2) The consumer has requested that the licensee refrain from sending any information regarding the consumer relationship, and the licensee's current privacy notice remains available to the consumer upon request.

D. A licensee may not provide any notice required by this Act solely by orally explaining the notice, either in person or over the telephone.

E. A licensee may provide a joint notice from the licensee and one or more of its affiliates or other financial institutions, as identified in the notice, as long as the notice is accurate with respect to the licensee and the other institutions. A licensee also may provide a notice on behalf of another financial institution.

F. If two (2) or more consumers jointly obtain an insurance product or service from a licensee, the licensee may satisfy the initial, annual and revised notice requirements of Sections 7A, 8A and 13A, respectively, by providing one notice to those consumers jointly.

© 2026 National Association of Insurance Commissioners

ARTICLE V. LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 16. General Rules for Use and Disclosure of Nonpublic Personal Information

A. Use and Disclosure

(1) A licensee may use and disclose nonpublic personal information about a consumer for purposes of processing a business transaction requested or authorized by the consumer.

(2) A licensee may disclose nonpublic personal information with affiliates, provided the affiliates' use and disclosure comply with this Act.

(3) A licensee shall not disclose nonpublic personal information to a nonaffiliated third party except as permitted by this Act.

(4) This section applies to nonpublic personal information collected before and after a consumer exercises an opt-out right under Section 19 or an opt-in right under Sections 20 and 21.(5) If a consumer submits an opt-out request during a transaction and the requested information is necessary to complete that transaction, the licensee shall:

(a) Inform the consumer that the transaction cannot be completed without the information; and

(b) Confirm whether the consumer wishes to proceed.

B. Limits on Disclosure**.** Except as provided by Section 16A(1), before disclosing a consumer's nonpublic personal information to a nonaffiliated third party, whether directly or through an affiliate, a licensee shall:

(1) Provide the initial notice required by Section 7;

(2) Provide a ~~clear and~~reasonably understandable, conspicuous and accessible notice to the consumer that details:

(a) The consumer's right to opt out of disclosure for targeted advertising under Section 19;

(b) The consumer's option to opt in to the sale of nonpublic personal information under Section 20; or

(c) The consumer's option to opt in to the disclosure of sensitive personal information Section 21.

(3) Provide a reasonable opportunity for the consumer to exercise any applicable opt-out right before disclosure; and

(4) Obtain and document the consumer's opt-in or opt-out election, as applicable.

© 2026 National Association of Insurance Commissioners

Section 17. Limits on Redisclosure and Reuse of Nonpublic Personal Information

A. If a licensee receives nonpublic personal information from a nonaffiliated third-party service provider under an exception in Article VI of this Act, the licensee may use and disclose the information in the ordinary course of business to carry out the activity covered by the exception under which the licensee received the information.

B. (1) If a licensee receives nonpublic personal information from a nonaffiliated third-party service provider other than under an exception in Article VI of this Act, the licensee may disclose the information only to ~~the following,~~affiliates of the licensee provided the disclosure is consistent with this Act:

~~(a) Affiliates of the third party-service provider from which the licensee received the information; and~~

~~(b) Affiliates of the licensee who may disclose the information only to the extent that the disclosure would be permissible by the licensee pursuant to this Act.~~

(2) Example. If a licensee obtains a customer list from a nonaffiliated third-party service provider outside of the exceptions in Article VI:

(a) The licensee may use that list for its own purposes consistent with this Act; and

(b) The licensee may disclose that list to another nonaffiliated third-party service provider only as permitted by this Act.

C. If a licensee discloses nonpublic personal information to a nonaffiliated third-party service provider under an exception in S Article VI of this Act, the third party-service provider:

(1) May disclose the information to the licensee's affiliates; and

(2) May disclose and use the information in the ordinary course of business to carry out the activity covered by the exception under which it received the information.

D. If a licensee discloses nonpublic personal information to a nonaffiliated third-party service provider other than under an exception in Article VI of this Act, the third-party service provider may disclose the information only:

(1) To the licensee's affiliates who may disclose the information only to the extent that it would be permissible for the licensee to disclose the information pursuant to this Act: and

(2) To any other person, if the disclosure would be lawful if the licensee made it directly to that person.

© 2026 National Association of Insurance Commissioners

Section 18. Limits on Sharing Access Number or Access Code Information for Marketing Purposes

A. A licensee shall not, directly or through an affiliate, disclose, other than to a consumer reporting agency, a policy number or similar form of access number or access code for a consumer's policy or transaction account to any nonaffiliated third party for use in telemarketing, direct mail marketing or other marketing through electronic mail to the consumer.

B. Exceptions. Subsection A of this section does not apply if a licensee discloses a policy number or similar form of access number or access code:

(1) To the licensee's service provider solely in order to perform marketing for the licensee's own products or services, as long as the service provider is not authorized to directly initiate charges to the account;

(2) To a licensee who is a producer solely in order to perform marketing for the licensee's own products or services; or

(3) To a participant in an affinity or similar program where the participants in the program are identified to the consumer when the consumer enters into the program.

(4) Where the policy number, or similar form of access number or access code, is in an encrypted form, as long as the licensee does not provide a means to decode the access number or access code.

Section 19. Limits on Disclosure of Nonpublic Personal Information in Targeted ~~Marketing~~ Advertising

A. Except as otherwise authorized in this Act, a licensee may not, directly or through any affiliate, disclose for the purpose of targeted advertising any nonpublic personal information about a consumer to a nonaffiliated third party unless the consumer has been provided a ~~clear and~~reasonably understandable, conspicuous, and accessible notice and a reasonable opportunity to opt out of targeted advertising in accordance with the requirements of Section 12 of this Act.

B. A licensee shall act on a consumer's request to opt out within 15 days of receipt.

C. A licensee is under no obligation to obtain additional information to execute the opt-out request.

D. A licensee may not solicit the consumer to change their election to opt out for twelve months.

E. A consumer has the right to opt out at any time.

Section 20. Limits on Sale of Nonpublic Personal Information

Before a licensee may sell nonpublic personal information:

A. The licensee shall provide a ~~clear and~~reasonably understandable, conspicuous, and accessible notice to the consumer in accordance with the requirements of Section 11; and

B. The consumer must affirmatively opt in to the sale of their nonpublic personal information.

© 2026 National Association of Insurance Commissioners

Section 21. Limits on Disclosure of Sensitive Personal Information

A. Except as provided by Subsection B below, a licensee may disclose a consumer's sensitive personal information only for those purposes and uses identified in Article VI and as expressly permitted or required by Article VI or other provisions of this Act.

B. Before a licensee may disclose a consumer's sensitive personal information for purposes other than those specified in subsection A of this section:

(1) A licensee shall provide a ~~clear and~~ reasonably understandable, conspicuous, and accessible notice to the consumer in accordance with the requirements of Section 11; and

(2) The consumer must affirmatively opt in to disclosure of their sensitive personal information.

© 2026 National Association of Insurance Commissioners

ARTICLE VI. EXCEPTIONS TO LIMITS ON DISCLOSURES OF NONPUBLIC PERSONAL INFORMATION

Section 22. Exception to Opt-Out Requirements for Disclosure of Nonpublic Personal Information for Service Providers and Joint Marketing

A. General rule.

(1) The opt-out requirements in Sections 12 and 19 do not apply when a licensee provides nonpublic personal information to a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf, if the licensee:

(a) Provides the initial notice in accordance with Section7; and

(b) Enters into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which the licensee disclosed the information, including use under an exception in Sections 23 or 24 in the ordinary course of business to carry out those purposes.

(2) Example. If a licensee discloses nonpublic personal information under this section to a financial institution with which the licensee performs joint marketing, the licensee's contractual agreement with that institution meets the requirements of Paragraph (1)(b) of this subsection if it prohibits the institution from disclosing or using the nonpublic personal information except as necessary to carry out the joint marketing or under an exception in Sections 23 or 24 in the ordinary course of business to carry out that joint marketing.

B. Service may include joint marketing. The services a nonaffiliated third party performs for a licensee under Subsection A of this section may include marketing of the licensee's own products or services or marketing of financial products or services offered pursuant to joint agreements between the licensee and one or more financial institutions.

C. Definition of "joint agreement." For purposes of this section, "joint agreement" means a written contract pursuant to which a licensee and one or more financial institutions jointly offer, endorse or sponsor a financial product or service.

Section 23. Exceptions to Notice and Opt-Out Requirements for Disclosure of Nonpublic Personal Information for Processing and Servicing Transactions

A. Exceptions for processing transactions at consumer's request. The requirements for initial notice in Section 7A(2), the opt-out in Sections 12 and 19, and service providers and joint marketing in Section 22 do not apply if the licensee discloses nonpublic personal information as necessary to effect, administer or enforce a transaction that a consumer requests or authorizes, or in connection with:

(1) Servicing or processing an insurance product or service that a consumer requests or authorizes;

© 2026 National Association of Insurance Commissioners

© 2026 National Association of Insurance Commissioners

(2) Maintaining or servicing the consumer's account with a licensee, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity;

(3) A proposed or actual securitization, secondary market sale (including sales of servicing rights) or similar transaction related to a transaction of the consumer; or

(4) Reinsurance or stop loss or excess loss insurance.

B. "Necessary to effect, administer or enforce a transaction" means that the disclosure is:

(1) Required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out the financial transaction or providing the product or service; or

(2) Required, or is a usual, appropriate or acceptable method:

(a) To carry out the transaction or the product or service business of which the transaction is a part, and record, service or maintain the consumer's account in the ordinary course of providing the insurance product or service;

(b) To administer or service benefits or claims relating to the transaction or the product or service business of which it is a part;

(c) To provide a confirmation, statement or other record of the transaction, or information on the status or value of the insurance product or service to the consumer or the consumer's agent or broker;

(d) To accrue or recognize incentives or bonuses associated with the transaction that are provided by a licensee or any other party;

(e) To underwrite insurance at the consumer's request or for any of the following purposes as they relate to a consumer's insurance: account administration, reporting, investigating or preventing fraud or material misrepresentation, processing premium payments, processing insurance claims, administering insurance benefits (including utilization review activities), participating in research projects or as otherwise required or specifically permitted by federal or state law; or

(f) In connection with:

(i) The authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited or otherwise paid using a debit, credit or other payment card, check or account number, or by other payment means;

(ii) The transfer of receivables, accounts or interests therein; or

(iii) The audit of debit, credit or other payment information.

© 2026 National Association of Insurance Commissioners

Section 24. Other Exceptions to Notice and Opt-Out Requirements for Disclosure of Nonpublic Personal Information

A. Exceptions to opt out requirements. The requirements for initial notice to consumers in Section 7A(2), the opt-out in Sections 12 and 19, and service providers and joint marketing in Section 22 do not apply when a licensee discloses nonpublic personal information:

(1) With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;

(2) (a) To protect the confidentiality or security of a licensee's records pertaining to the consumer, service, product or transaction;

(b) To protect against or prevent actual or potential fraud or unauthorized transactions;

(c) For required institutional risk control or for resolving consumer disputes or inquiries;

(d) To persons holding a legal or beneficial interest relating to the consumer; or

(e) To persons acting in a fiduciary or representative capacity on behalf of the consumer;

(f) To prevent, detect, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted nonpublic personal information.

(3) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that are rating a licensee, persons that are assessing the licensee's compliance with industry standards, and the licensee's attorneys, accountants and auditors;

(4) To the extent specifically permitted or required under other provisions of law and in accordance with the federal Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.), to law enforcement agencies (including the Federal Reserve Board, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, the Securities and Exchange Commission, the Secretary of the Treasury, with respect to 31 U.S.C. Chapter 53, Subchapter II (Records and Reports on Monetary Instruments and Transactions) and 12 U.S.C. Chapter 21 (Financial Recordkeeping), a state insurance authority, and the Federal Trade Commission), self-regulatory organizations or for an investigation on a matter related to public safety;

(5) (a) To a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.); or

(b) From a consumer report reported by a consumer reporting agency;

© 2026 National Association of Insurance Commissioners

(6) In connection with a proposed or actual sale, merger, transfer or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of the business or unit;

(7) (a) To comply with federal, state or local laws, rules and other applicable legal requirements;

(b) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, state or local authorities; or

(c) To respond to judicial process or government regulatory authorities having jurisdiction over a licensee for examination, compliance or other purposes as authorized by law; or

(8) For purposes related to the replacement of a group benefit plan, a group health plan, a group welfare plan or a workers' compensation plan.

B. Example of revocation of consent. A consumer may revoke consent by subsequently exercising the right to opt out of future disclosures of nonpublic personal information as permitted under Section 12F.

~~**Drafting Note:** Because the notice requirements of this Act could be a financial burden on a company in liquidation or receivership and negatively impact the ability of the liquidator or receiver to pay claims, regulators may want to consider adding an additional exception providing that licensees in liquidation or receivership are not subject to the notice provisions of this Act.~~

Commented [CR4]: Protecting consumers' NPI should not be compromised, just because a licensee is in receivership/reorganization or liquidation. Otherwise a receiver or liquidator could have the incentive to sell consumer NPI to data brokers or other non-covered companies. This could impose substantial harm to consumers, and it would be unfair to other licensees that must follow this act.
The FTC recognized this danger, when the company 23&me was sold under bankruptcy. To protect information on the DNA of seven million people, it wrote a letter to the agency overseeing the bankruptcy saying 23&me should be bound by the same privacy agreement as the company's existing policy.

© 2026 National Association of Insurance Commissioners

ARTICLE VII. RULES FOR HEALTH INFORMATION

Section 25. When Authorization Required for Disclosure of Nonpublic Personal Health Information

A. A licensee shall not disclose nonpublic personal health information about a consumer unless an authorization is obtained from the consumer whose nonpublic personal health information is sought to be disclosed.

B. Nothing in this section shall prohibit, restrict or require an authorization for the disclosure of nonpublic personal health information by a licensee for the performance of the following insurance functions by or on behalf of the licensee:

(1) Claims administration any processing;

(2) Claims adjustment and management;

(3) Detection, investigation or reporting of actual or potential fraud, misrepresentation or criminal activity;

(4) Underwriting;

(5) Policy placement or issuance;

(6) Loss control;

(7) Ratemaking and guaranty fund functions;

(8) Reinsurance and excess loss insurance;

(9) Risk management;

(10) Case management;

(11) Disease management;

(12) Quality assurance;

(13) Quality improvement;

(14) Performance evaluation;

(15) Provider credentialing verification;

(16) Utilization review;

(17) Peer review activities;

~~(18) Actuarial, scientific, medical or public policy research;~~

(19) Grievance procedures;

Commented [CR5]: Items 18 and 26 should not be included in this section. For actuarial, scientific, medical or public policy research or external accreditation examinations, consumer NPI should be deidentified, before it is used.

© 2026 National Association of Insurance Commissioners

(20) Internal administration of compliance, managerial, and information systems;

(21) Policyholder service functions;

(22) Auditing;

(23) Reporting;

(24) Database security;

(25) Administration of consumer disputes and inquiries;

~~(26) External accreditation standards;~~

(27) The replacement of a group benefit plan or workers' compensation policy or program;

(28) Activities in connection with a sale, merger, transfer or exchange of all or part of a business or operating unit;

(29) Any activity that permits disclosure without authorization pursuant to the federal Health Insurance Portability and Accountability Act privacy rules promulgated by the U.S. Department of Health and Human Services or other applicable laws;

(30) Disclosure that is required, or is one of the lawful or appropriate methods, to enforce the licensee's rights or the rights of other persons engaged in carrying out a transaction or providing a product or service that a consumer requests or authorizes including subrogation, and

(31) Any activity otherwise permitted by law, required pursuant to governmental reporting authority, or to comply with the legal process.

C. Additional insurance functions may be added with the approval of the commissioner to the extent they are necessary for appropriate performance of insurance functions and are fair and reasonable

Section 26. Authorizations

A. A valid authorization to disclose nonpublic personal health information pursuant to this Article VII shall be in written or electronic form and shall contain all of the following:

(1) The identity of the consumer who is the subject of the nonpublic personal health information;

(2) A ~~general~~ specific and meaningful description of the types of nonpublic personal health information to be disclosed;

Commented [CR6]: HIPAA and 42 CFR Part 2 require the purpose to be "specific and meaningful"

(3) General descriptions of the parties to whom the licensee discloses nonpublic personal health information, the purpose of the disclosure and how the information will be used;

© 2026 National Association of Insurance Commissioners

(4) The signature, including electronic signatures, of the consumer who is the subject of the nonpublic personal health information or the individual who is legally empowered to grant authority and the date signed; and

(5) Notice of the length of time for which the authorization is valid and that the consumer may revoke the authorization at any time and the procedure for making a revocation.

(6) Any additional information necessary to comply with HIPAA or any other applicable law, including the federal confidentiality protections for substance abuse disorder treatment records (42 USC Section 290dd-2 and 42 CFR Part 2) as well as state laws.

B. An authorization for the purposes of this Article VII shall specify a length of time for which the authorization shall remain valid, which in no event shall be for more than twenty-four (24) months.

C. A consumer who is the subject of nonpublic personal health information may revoke an authorization provided pursuant to this Article VII at any time, subject to the rights of an individual who acted in reliance on the authorization prior to notice of the revocation.

D. A licensee shall retain the authorization or a copy thereof in the record of the individual who is the subject of nonpublic personal health information.

E. A signed copy of the authorization shall be provided to the consumer.

Section 27. Authorization Request Delivery

A request for authorization and an authorization form may be delivered to a consumer as part of an opt-out notice pursuant to Section 12, provided that the request and the authorization form are ~~clear and~~reasonably understandable, conspicuous, and accessible. An authorization form is not required to be delivered to the consumer or included in any other notices unless the licensee intends to disclose protected health information pursuant to Section 25A.

Section 28. Relationship to Federal Rules

A licensee that is subject to and governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), and the Health Information Technology for Economic and Clinical Health Act (Public Law 111-5, HITECH), and that maintains nonpublic personal information in the same manner as protected health information shall be deemed to comply with the requirements of this Act.

This Act shall not apply to ~~nonprofits, such as~~ ~~nonprofits, such as~~ the National Association of Insurance Commissioners or the National Insurance Crime Bureau, when processing or sharing information solely for investigating criminal or fraudulent insurance acts.

Commented [CR7]: Section 28 should not exempt all nonprofits. Doing so would exempt vigilante nonprofits that have no legitimate criminal investigation authority to collect protected NPI.

Section 29. Relationship to State Laws

Nothing in this Article shall preempt or supersede existing state law related to medical records, consumer data privacy, health or insurance information privacy.

© 2026 National Association of Insurance Commissioners

© 2026 National Association of Insurance Commissioners

ARTICLE VIII. ADDITIONAL PROVISIONS

Section 30. Protection of Fair Credit Reporting Act

Nothing in this Act shall be construed to modify, limit or supersede the operation of the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), and no inference shall be made regarding whether information is transaction or experience information under Section 603 of that Act.

Section 31. Nondiscrimination

A. A licensee shall not unfairly discriminate against any consumer because that consumer has opted out from the disclosure of his or her nonpublic personal information pursuant to the provisions of this Act.

B. A licensee shall not unfairly discriminate against a consumer because that consumer has not granted authorization for the disclosure of his or her nonpublic personal health information pursuant to the provisions of this Act.

Section 32. Violation

Drafting Note: Cite state unfair trade practices act or other applicable state law.

Section 33. Severability

If any section or portion of a section of this Act or its applicability to any person or circumstance is held invalid by a court, the remainder of the Act or the applicability of the provision to other persons or circumstances shall not be affected.

Section 34. Individual Remedies

This Act may not be construed to create or imply a private cause of action for violation of its provisions, nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Section 35. Effective Date

A. Effective date. This Act has been effective since November 13, 2000. The amendments to this Act are effective [Insert Effective Date]. In order to provide sufficient time for licensees to establish policies and systems to comply with the amendments to this Act, the commissioner has extended the time for compliance with the amendments to this Act until [Insert Compliance Date].

B. By [Insert Compliance Date], a licensee shall provide an initial notice, as required by Section 7, to any existing consumer who has not previously received a notice that complies with the amendments to this Act.

C. Two-year grandfathering of service agreements. Until [Insert Compliance Date], a contract that a licensee has entered into with a nonaffiliated third party to perform services for the licensee or functions on the licensee's behalf satisfies the provisions of Section 22A(1)(b) of this Act, even if the contract does not include a requirement that the third party maintain the confidentiality of nonpublic personal information, as long as the licensee entered into the agreement on or before

© 2026 National Association of Insurance Commissioners

[Insert Compliance Date].

© 2026 National Association of Insurance Commissioners

APPENDIX A – SAMPLE CLAUSES

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the following sample clauses, if the clause is accurate for each institution that uses the notice. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt out of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A-1–Categories of information a licensee collects (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(1) to describe the categories of nonpublic personal information the licensee collects.

Commented [CR8]: This clause should only be used, if the categories we have prescribed for Section 12 are used.

Sample Clause A-1:

We collect nonpublic personal information about you from the following sources:

Information we receive from you on applications or other forms;
Information about your transactions with us, our affiliates or others; and
Information we ~~r~~We receive from a ~~consumer reporting agency.~~ [INSERT NAMES OF ACTUAL CONSUMER REPORTING AGENCIES USED and TYPES OF INFORMATION THEY COLLECT.]

Commented [CR9]: Sample Clause A-1: The term "consumer reporting agency" should not never be used. Consumers don't know what consumer reporting agencies are.

A-2–Categories of information a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use one of these clauses, as applicable, to meet the requirement of Section 9A(2) to describe the categories of nonpublic personal information the licensee discloses. The licensee may use these clauses if it discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

~~Sample Clause A-2, Alternative 1:~~

~~We may disclose the following kinds of nonpublic personal information about you:~~

~~Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];~~

~~Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premiums, and payment history"]; and~~

~~Information we receive from a consumer reporting agency, [such as [provide illustrative examples, such as "your creditworthiness and credit history"].~~

Commented [CR10]: Sample Clause A-2, Alternative 1: This wording gives the consumer the incorrect impression that the licensee can disclose information to anyone, including non-affiliates. Also it gives the impression that information from consumer reporting agencies can be shared with anyone, which is not the case. Some NPI collected by consumer reporting agencies includes PHI that is protected by HIPAA and other federal and state privacy regulations.

~~Sample Clause A-2, Alternative 2:~~

~~We may disclose all of the information that we collect, as described [describe location in the notice, such as "above" or "below"].~~

Commented [CR11]: Sample Clause A-2, Alternative 2 should never be used. It deludes the consumer that s/he has no rights. No licensee can disclose sensitive NPI it collects, unless given permission by the consumer. In addition, health related NPI covered by HIPAA and other federal and some state laws cannot be shared with anyone.

A-3–Categories of information a licensee discloses and parties to whom the licensee discloses (institutions that do

© 2026 National Association of Insurance Commissioners

not disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirements of Sections 9A(2) and (3) to describe the categories of nonpublic personal information the licensee discloses and the categories of affiliates and nonaffiliated third parties to whom the licensee discloses. A licensee may use this clause if the licensee does not disclose nonpublic personal information to any party, other than as permitted by the exceptions in Sections 23 and 24.

~~Sample Clause A-3:~~

~~We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.~~

Commented [CR12]: Sample Clause A-3: This sample is totally unacceptable. It is totally deceptive, because it gives consumers the impression that only in exceptional cases will NPI be shared, ignoring the fact that most NPI collected can be shared, unless the consumer opts out of certain sharing.

A-4–Categories of parties to whom a licensee discloses (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(3) to describe the categories of affiliates and nonaffiliated third parties to whom the licensee discloses nonpublic personal information. This clause may be used if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-4:

We may disclose nonpublic personal information about you to the following types of third parties, unless you indicate that you do not want it shared with unaffiliated third parties, as explained in our opt-out procedure:

Commented [CR13]: Sample Clause A-4: Again the bias in these samples is to give consumers the impression that they have very little ability to limit sharing of their NPI. Instead, the text of samples should highlight the ability of consumers to limit sharing, with an explanation of how that can be requested.

- Financial service providers, such as [provide illustrative examples, such as "life insurers, automobile insurers, mortgage bankers, securities broker-dealers, and insurance agents"];
- Non-financial companies, such as [provide illustrative examples, such as "retailers, direct marketers, airlines, and publishers"]; and
- Others, such as [provide illustrative examples, such as "non-profit organizations"].

~~We may also disclose nonpublic personal information about you to nonaffiliated third parties as permitted by law.~~

A-5–Service provider/joint marketing exception
A licensee may use one of these clauses, as applicable, to meet the requirements of Section 9A(2) related to the exception for service providers and joint marketers in Section 22. If a licensee discloses nonpublic personal information under this exception, the licensee shall describe the categories of nonpublic personal information the licensee discloses and the categories of third parties with which the licensee has contracted.

Sample Clause A-5, Alternative 1:

We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

- Information we receive from you on applications or other forms, such as [provide illustrative examples, such as "your name, address, social security number, assets, income, and beneficiaries"];

© 2026 National Association of Insurance Commissioners

- Information about your transactions with us, our affiliates or others, such as [provide illustrative examples, such as "your policy coverage, premium, and payment history"]; and

- Information we receive from a ~~consumer reporting agency, such as [provide illustrative examples, such as "your creditworthiness and credit history"].~~ [INSERT NAMES OF ACTUAL CONSUMER REPORTING AGENCIES USED and TYPES OF INFORMATION THEY COLLECT.]

Sample Clause A-5, Alternative 2:

We may disclose all of the information we collect, as described [describe location in the notice, such as "above" or "below"] to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.

A-6–Explanation of opt- out right (institutions that disclose outside of the exceptions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(4) to provide an explanation of the consumer's right to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right. The licensee may use this clause if the licensee discloses nonpublic personal information other than as permitted by the exceptions in Sections 22, 23 and 24.

Sample Clause A-6:

If you prefer that we not disclose nonpublic personal information about you to nonaffiliated third parties, you may opt out of those disclosures, that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to nonaffiliated third parties, ~~you may [~~describe ~~a reasonable~~ all means of opting out, such as "call the following toll-free number: (insert number)].

A-7–Confidentiality and security (all institutions)
A licensee may use this clause, as applicable, to meet the requirement of Section 9A(8) to describe its policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

Sample Clause A-7:

We restrict access to nonpublic personal information about you to [provide an appropriate description, such as "those employees who need to know that information to provide products or services to you"]. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

Commented [CR14]: Sample Clause A-5, Alternative 1: The wording in this sample should only be used if the three categories of sources cited are the only ones that will be used to share NPI for joint marketing agreements. If there are other sources of NPI that will be shared for joint marketing, then their categories should also be listed in a way that provides transparency to consumers.

Commented [CR15]: Sample Clause A-1: The term "consumer reporting agency" should not never be used. Consumers don't know what consumer reporting agencies are.

© 2026 National Association of Insurance Commissioners

APPENDIX B – FEDERAL MODEL PRIVACY FORM

Licensees, including a group of financial holding company affiliates that use a common privacy notice, may use the Federal Model Privacy Form, if the Form is accurate for each institution that uses the Form. (Note that disclosure of certain information, such as assets, income and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act, such as a requirement to permit a consumer to opt of disclosures to affiliates or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.)

A. General Instructions

1. How the Model Privacy Form is used.

(a) The Model Form may be used, at the option of a "licensee", including a group of licensees or other financial institutions that use a common privacy notice, to meet the content requirements of the privacy notice and opt out notice set forth in [insert citation for sections of statute or regulation sections that parallel Sections 9and 11 of the NAIC *Privacy of Consumer Information Act*]

(b) The Model Form is a standardized form, including page layout, content, format, style, pagination, and shading. Licensees seeking to obtain the safe harbor through use of the Model Form may modify it only as described in these Instructions.

(c) Note that disclosure of certain information, such as assets, income, and information from a consumer reporting agency, may give rise to obligations under the federal Fair Credit Reporting Act (FCRA), codified at 15 U.S.C. §§ 1681-1681x, such as a requirement to permit a consumer to opt out of disclosures to affiliates, or designation as a consumer reporting agency if disclosures are made to nonaffiliated third parties.

(d) The word "consumer" may be replaced by the word "member," whenever it appears in the Model Form, as appropriate.

2. The Contents of the Model Privacy Form

The Model Form consists of two pages, which may be printed on both sides of a single sheet of paper or may appear on two separate pages. Where a licensee provides a long list of licensees or financial institutions at the end of the Model Form in accordance with Instruction B3(a)(i), or provides additional information in accordance with Instruction B3(c) and such list or additional information exceeds the space available on Page Two of the Model Form, such list or additional information may extend to a third page.

(a) Page One. The first page consists of the following components:

(1) Date last revised (upper right hand corner)
(2) Title
(3) Key frame (Why? What? How?)
(4) Disclosure table ("Reasons we can share your personal information")
(5) "To limit our sharing" box, as needed, for the licensee's opt out information
(6) "Questions" box, for customer service contact information
(7) Mail in opt out form, as needed

(b) Page Two. The second page consists of the following components:

© 2026 National Association of Insurance Commissioners

(1) Heading (Page 2)
(2) Frequently Asked Questions ("Who we are" and "What we do")
(3) Definitions
(4) "Other important information" box, as needed

3. The format of the Model Privacy Form.

The format of the Model Form may be modified only as described below.

(a) Easily readable type font. Licensees that use the Model Form must use an easily readable type font. While a number of factors together produce easily readable font, licensees are required to use a minimum of 10-point font (unless otherwise expressly permitted in these Instructions) and sufficient spacing between lines.

(b) Logo. A licensee may include a corporate logo on any page of the notice, so long as it does not interfere with the readability of the Model Form or the space constraints of each page.

(c) Page size and orientation. Each page of the Model Form must be printed in portrait orientation, the size of which must be sufficient to meet the layout and minimum font size requirements, with sufficient white space on the top, bottom, and sides of the content.

(d) Color. The Model Form must be printed on white or light color paper (such as cream) with black or other contrasting ink color. Spot color may be used to achieve visual interest, so long as the color contrast is distinctive and the color does not detract from the readability of the Model Form. Logos may also be printed in color.

(e) Languages. The Model Form may be translated into languages other than English.

B. Information Required in the Model Privacy Form

The information in the Model Form may be modified only as described below.

1. Name of licensee or group of affiliated licensees or institutions providing the notice
Insert the name of the licensee providing the notice, or a common identity of the affiliated licensees or financial institutions jointly providing the notice on the form, wherever [name of licensee] appears.

2. Page One

(a) Last revised date. The licensee must insert in the upper right-hand corner the date on which the notice was last revised. The information shall appear in minimum 8-point font as "rev. [month/year]" using either the name or number of the month, such as "rev. July 2016" or "rev. 7/16."

(b) General instructions for the "What?" box

(i) The bulleted list identifies the types of personal information that the licensee collects and shares. All licensees must use the term "Social Security Number" in the first bullet.

(ii) A licensee must use five (5) of the following terms, to complete the bulleted list: income; account balances; payment history; transaction history; transaction or loss history; credit history; credit scores; assets; investment experience; credit-based insurance scores; insurance claim history; medical information; overdraft

© 2026 National Association of Insurance Commissioners

history; purchase history; account transactions; risk tolerance; medical related debts; credit card or other debt; mortgage rates and payments; retirement assets; checking account information; employment information; wire transfer instructions.

(c) General instructions for the disclosure table. The left column lists reasons for sharing or using personal information. Each reason correlates to a specific legal provision described in Paragraph 2(d) of this Instruction. In the middle column, each licensee must provide a "Yes" or "No" response that accurately reflects its information-sharing policies and practices with respect to the reason listed on the left. In the right column, each licensee must provide in each box one of the following three (3) responses, as applicable, that reflects whether a consumer can limit such sharing:

"Yes," if it is required to or voluntarily provides an opt-out; "No," if it does not provide an opt-out; or

"We don't share," if it answers "No" in the middle column.

Only the sixth row ("For our affiliates to market to you") may be omitted at the option of the licensee. See Paragraph 2(d)(6) of this instruction.

(d) Specific disclosures and corresponding legal provisions

(i) For our everyday business purposes. This reason incorporates sharing information under [insert citation for sections of statute or regulation sections that parallel Sections 23 and 24 of NAIC model *Privacy of Consumer Information Act*] and with service providers pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*] other than the disclosures described in Paragraphs (2)(d)(ii) or (2)(d)(iii) of this instruction.

(ii) For our marketing purposes. This reason incorporates sharing information with service providers by a licensee for its own marketing pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iii) For joint marketing with other financial companies. This reason incorporates sharing information under joint marketing agreements between 2 or more licensees or financial institutions and with any service provider used in conjunction with such agreement pursuant to [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*]. A licensee that shares for this reason may choose to provide an opt-out.

(iv) For our affiliates' everyday business purposes – information about transactions and experiences. This reason incorporates sharing information specified in Sections 603(d)(2)(A)(i) and (ii) of the FCRA. A licensee that shares information for this reason may choose to provide an opt-out.

(v) For our affiliates' everyday business purposes – information about creditworthiness. This reason incorporates sharing information pursuant to Section 603(d)(2)(A)(iii) of the FCRA. A licensee that shares information for this reason must provide an opt-out.

(vi) For our affiliates to market to you. This reason incorporates sharing information specified in Section 624 of the FCRA. This reason may be omitted from the disclosure table when: the licensee does not have affiliates (or does not disclose personal information to its affiliates); the licensee's affiliates do not use personal information in a manner that requires an opt-out; or the licensee provides the affiliate marketing notice separately. Licensees that include this reason must provide an opt-out of indefinite duration. A licensee that is required to provide an

© 2026 National Association of Insurance Commissioners

affiliate marketing opt-out, but does not include that opt-out in the Model Form under this part, must comply with Section 624 of the FCRA and [insert citation for statute or regulation that parallels NAIC *Privacy of Consumer Information Act*], with respect to the initial notice and opt-out and any subsequent renewal notice and opt-out. A licensee not required to provide an opt-out under this subparagraph may elect to include this reason in the Model Form.

(vii) For nonaffiliates to market to you. This reason incorporates sharing described in [insert citation for sections of statute or regulation sections that parallel Sections 11 and 16(B) of NAIC *Privacy of Consumer Information Act*]. A licensee that shares personal information for this reason must provide an opt-out.

(c) To limit our sharing. A licensee must include this section of the Model Form only if it provides an opt-out. The word "choice" may be written in either the singular or plural, as appropriate. Licensees must select one or more of the applicable opt-out methods described: telephone, such as by a toll-free number; a web site; or use of a mail-in opt-out form. Licensees may include the word "toll-free" before telephone, as appropriate. A licensee that allows consumers to opt out online must provide either a specific web address that takes consumers directly to the opt-out page or a general web address that provides a clear and reasonably understandable, conspicuous, and accessible direct link to the opt-out page. The opt-out choices made available to the consumer who contacts the licensee through these methods must correspond accurately to the "Yes" responses in the third column of the disclosure table. In the part entitled "Please note," licensees may insert a number that is 30 days or greater in the space marked "[30]." Instructions on voluntary or state privacy law opt-out information are in Paragraph 2(g)(v) of these Instructions.

(f) Questions box. Customer service contact information must be inserted as appropriate where [phone number] or [web site] appear. Licensees may elect to provide either a phone number, such as a toll-free number, or a web address, or both. Licensees may include the words "toll free" before the telephone number, as appropriate.

(g) Mail-in opt-out form. Licensees must include this mail-in form only if they state in the "To limit our sharing" box that consumers can opt out by mail. The mail-in form must provide opt-out options that correspond accurately to the "Yes" responses in the third column of the disclosure table. Licensees that require consumers to provide only name and address may omit the section identified as "[account #]." Licensees that require additional or different information, such as a random opt-out number or a truncated account number to implement an opt-out election should modify the "[account #]" reference accordingly. This includes licensees that require customers consumers with multiple accounts to identify each account to which the opt-out should apply. A licensee must enter its opt-out mailing address in the far right of this form (see version 3), or below the form (see version 4). The reverse side of the mail-in opt-out form must not include any content of the Model Form.

(i) Joint accountholder. Only licensees that provide their joint accountholders the choice to opt-out for only one accountholder, in accordance with Paragraph 3(a)(5) of these Instructions, must include in the far left column of the mail-in form the following statement:

If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below.

□ Apply my choice(s) only to me.

The word "choice" may be written in either the singular or plural, as appropriate. Licensees that provide insurance products or services, provide this option, and elect to use the Model Form may substitute the word "policy" for "account" in this statement. Licensees that do not provide this option may eliminate this left column from the mail-in form.

© 2026 National Association of Insurance Commissioners

(ii) FCRA Section 603(d)(2)(A)(iii) opt-out. If the licensee shares personal information pursuant to Section 603(d)(2)(A)(iii) of the FCRA, it must include in the mail-in opt-out form the following statement:

□ Do not share information about my creditworthiness with your affiliates for their everyday business purposes.

(iii) FCRA Section 624 opt-out. If the licensee uses Section 624 of the FCRA, in accord with paragraph 2(d)(6) of these Instructions, it must include in the mail-in opt-out form the following statement:

□ Do not allow your affiliates to use my personal information to market to me.

(iv) Nonaffiliate opt-out. If the licensee shares personal information pursuant to [insert citation for section of statute or regulation that parallels Section 16(B) of NAIC *Privacy of Consumer Information Act*], it must include in the mail-in opt-out form the following statement:

□ Do not share my personal information with nonaffiliates to market their products and services to me.

(v) Additional opt-outs. Licensees that use the disclosure table to provide opt-out options beyond those required by Federal law must provide those opt-outs in this section of the Model Form. A licensee that chooses to offer an opt-out for its own marketing in the mail-in opt-out form must include one of the two following statements:

□ Do not share my personal information to market to me. or

□ Do not use my personal information to market to me.

A licensee that chooses to offer an opt-out for joint marketing must include the following statement:

□ Do not share my personal information with other financial institutions to jointly market to me.

(h) Barcodes. A licensee may elect to include a barcode and/or "tagline" (an internal identifier) in 6-point type at the bottom of page one, as needed for information internal to the licensee, so long as these do not interfere with the clarity or text of the form.

3. Page Two

(a) General Instructions for the Questions. Certain Questions on the Model Form may be customized as follows:

(i) "Who is providing this notice?" This question may be omitted where only one licensee provides the Model Form and that licensee is clearly identified in the title on Page One. Two or more licensees or financial institutions that jointly provide the Model Form must use this question to identify themselves as required by [insert citation for section of statute or regulation that parallels Section 15(E) of NAIC model *Privacy of Consumer Information Act*]. Where the list of licensees or financial institutions exceeds four (4) lines, the licensee must describe in the response to this question the general types of licensees or financial institutions jointly providing the notice and must separately identify those licensees or financial institutions, in minimum 8-point font, directly following the "Other important information" box, or, if that box is not included in the licensee's form, directly following the "Definitions." The list may appear in a multi-column format.

(ii) "How does [name of licensee] protect my personal information?" The licensee may only provide additional information pertaining to its safeguards practices following the designated response to this question.

© 2026 National Association of Insurance Commissioners

Such information may include information about the licensee's use of cookies or other measures it uses to safeguard personal information. Licensees are limited to a maximum of 30 additional words.

(iii) "How does [name of licensee] collect my personal information?" Licensees must use five (5) of the following terms to complete the bulleted list for this question: open an account; deposit money; pay your bills; apply for a loan; use your credit or debit card; seek financial or tax advice; apply for insurance; pay insurance premiums; file an insurance claim; seek advice about your investments; buy securities from us; sell securities to us; direct us to buy securities; direct us to sell your securities; make deposits or withdrawals from your account; enter into an investment advisory contract; give us your income information; provide employment information; give us your employment history; tell us about your investment or retirement portfolio; tell us about your investment or retirement earnings; apply for financing; apply for a lease; provide account information; give us your contact information; pay us by check; give us your wage statements; provide your mortgage information; make a wire transfer; tell us who receives the money; tell us where to send the money; show your government-issued ID; show your driver's license; order a commodity futures or option trade.

Licensees that collect personal information from their affiliates and/or credit bureaus must include the following statement after the bulleted list: "We also collect your personal information from others, such as credit bureaus, affiliates, or other companies." Licensees that do not collect personal information from their affiliates or credit bureaus but do collect information from other companies must include the following statement instead: "We also collect your personal information from other companies." Only licensees that do not collect any personal information from affiliates, credit bureaus, or other companies can omit both statements.

(iv) "Why can't I limit all sharing?" Licensees that describe state privacy law provisions in the "Other important information" box must use the bracketed sentence: "See below for more on your rights under state law." Other licensees must omit this sentence.

(v) "What happens when I limit sharing for an account I hold jointly with someone else?" Only licensees that provide opt-out options must use this question. Other licensees must omit this question. Licensees must choose one of the following two statements to respond to this question: "Your choices will apply to everyone on your account." or "Your choices will apply to everyone on your account—unless you tell us otherwise." Licensees may substitute the word "policy" for "account" in these statements.

(b) General Instructions for the Definitions. The licensee must customize the space below the responses to the three definitions in this section. This specific information must be in italicized lettering to set off the information from the standardized definitions.

(i) Affiliates. As required by [insert citation for section of statute or regulation that parallels Section 9(A)(3) of NAIC *Privacy of Consumer Information Act*], where [affiliate information] appears, the licensee must:

(a) If it has no affiliates, state: "[name of licensee] has no affiliates";

(b) If it has affiliates but does not share personal information with them, state: "[name of licensee] does not share with our affiliates"; or

(c) If it shares with its affiliates, state, as applicable: "Our affiliates include companies with a [common corporate identity of licensee] name; financial companies such as [insert illustrative list of companies]; nonfinancial companies, such as [insert illustrative list of companies]; and others, such as [insert illustrative list]."

(ii) Nonaffiliates. As required by [insert citation for section of statute or regulation that parallels Section 9)(A)(3) of NAIC *Privacy of Consumer Information Act*], where [nonaffiliate information] appears, the licensee must:

© 2026 National Association of Insurance Commissioners

(a) If it does not share with nonaffiliated third parties, state: "[name of licensee] does not share with nonaffiliates so they can market to you"; or

(b) If it shares with nonaffiliated third parties, state, as applicable: "Nonaffiliates we share with can include [list categories of companies such as mortgage companies, insurance companies, direct marketing companies, and nonprofit organizations]."

(iii) Joint Marketing. As required by [insert citation for section of statute or regulation that parallels Section 22 of NAIC *Privacy of Consumer Information Act*], where [joint marketing] appears, the licensee must:

(a) If it does not engage in joint marketing, state: "[name of licensee] doesn't jointly market"; or

(b) If it shares personal information for joint marketing, state, as applicable: "Our joint marketing partners include [list categories of companies such as credit card companies]."

(c) General instructions for the "Other important information" box. This box is optional. The space provided for information in this box is not limited, and an additional page may be used if necessary. Only the following types of information can appear in this box:

(i) State and/or international privacy law information; and/or

(ii) A form by which the consumer may acknowledge receipt of the notice.

Chronological Summary of Actions (all references are to the Proceedings of the NAIC)

2000 Proc. 3rd Quarter 7, 10, 14-36, 904 (adopted).
2002 Proc. 3rd Quarter12, 13, 71, 72-73 (amended).
2017 Spring National Meeting (amended).

© 2026 National Association of Insurance Commissioners

~~Per our comments in~~

Version 1:
Model Form with No Opt-Out

Rev. [insert date]

FACTS	**WHAT DOES** [Name of Licensee] **DO WITH YOUR PERSONAL INFORMATION?**
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores] When you are *no longer* our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

Questions?	Call [phone number] or go to [web site]

© 2026 National Association of Insurance Commissioners

Page 2

Who we are	
Who is providing this notice?	[insert]

What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]

Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*

Other important information
[insert other important information]

© 2026 National Association of Insurance Commissioners

Version 2: Model Form with Opt-Out by Telephone and/or Online

Rev. [insert date]

FACTS	WHAT DOES [NAME OF LICENSEE] DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

To limit our sharing	■ Call [phone number] —our menu will prompt you through your choice(s) **or** ■ Visit us online: [web site] **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

© 2026 National Association of Insurance Commissioners

Page 2

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ■ [open an account] or [deposit money] ■ [pay your bills] or [apply for a loan] ■ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ■ sharing for affiliates' everyday business purposes—information about your creditworthiness ■ affiliates from using your information to market to you ■ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Rev. [insert date

Version 3: Model Form with Mail-in Opt-Out Form

FACTS	WHAT DOES **[NAME OF LICENSEE]** DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and [income] ■ [account balances] and [payment history] ■ [credit history] and [credit scores]
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does [name of licensee] share?	Can you limit this sharing?
For our everyday business purposes— such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		
For our marketing purposes— to offer our products and services to you		
For joint marketing with other financial companies		
For our affiliates' everyday business purposes— information about your transactions and experiences		
For our affiliates' everyday business purposes— information about your creditworthiness		
For our affiliates to market to you		
For nonaffiliates to market to you		

© 2026 National Association of Insurance Commissioners

To limit our sharing	▪ Call [phone number] —our menu will prompt you through your choice(s) ▪ Visit us online: [web site] or ▪ Mail the form below **Please note:** If you are a *new* customer, we can begin sharing your information [30] days from the date we sent this notice. When you are *no longer* our customer, we continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.
Questions?	Call [phone number] or go to [web site]

Mail-in Form

Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless your mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me.	
	Name	
	Address	
	City, State, Zip	
	[Account #]	
Mail To:	[Name of Licensee] [Address] [City], [ST] [ZIP]	

© 2026 National Association of Insurance Commissioners

Page 3

Who we are	
Who is providing this notice?	[insert]
What we do	
How does [name of licensee] protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. [insert]
How does [name of licensee] collect my personal information?	We collect your personal information, for example, when you ▪ [open an account] or [deposit money] ▪ pay your bills] or [apply for a loan] ▪ [use your credit or debit card] [We also collect your personal information from other companies.] OR [We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.]
Why can't I limit all sharing?	Federal law gives you the right to limit only ▪ sharing for affiliates' everyday business purposes—information about your creditworthiness ▪ affiliates from using your information to market to you ▪ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing. [See below for more on your rights under state law.]
What happens when I limit sharing for an account I hold jointly with someone else?	[Your choices will apply to everyone on your account.] OR [Your choices will apply to everyone on your account - unless you tell us otherwise.]
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ▪ *[affiliate information]*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ▪ *[nonaffiliate information]*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ▪ *[joint marketing information]*
Other important information	
[insert other important information]	

© 2026 National Association of Insurance Commissioners

Version 4: Optional Mail-in Form

Mail-in Form	
Leave Blank OR [If you have a joint account, your choice(s) will apply to everyone on your account unless you mark below. ☐ Apply my choices only to me]	Mark any/all you want to limit: ☐ Do not share information about my creditworthiness with your affiliates for their everyday business purposes. ☐ Do not allow your affiliates to use my personal information to market to me. ☐ Do not share my personal information with nonaffiliates to market their products and services to me. **Name** **Address** **City, State, Zip** **[Account #]**
Mail To:	[Name of Licensee], [Address 1], [Address 2], [City], [ST] [ZIP]

© 2026 National Association of Insurance Commissioners