Public Comments to Revised Article III of the
***Privacy of Consumer Financial and Health Information Regulation* (#672)**
Section 6—Access, Correction, and Deletion of Nonpublic Personal Information
Section 7—Sale of Nonpublic Personal Information
Section 8—Use and Disclosure of Sensitive Personal Information

TABLE OF CONTENTS

Regulator Comments 2

California Department of Insurance 2
Maine Bureau of Insurance 4
North Dakota Insurance Department 11
Pennsylvania Insurance Department 12
Virginia Bureau of Insurance 17

Industry Comments 23

ACLI 23
AHIP 30
APCIA 31
ATLA 39
Blue Cross Blue Shield Association 44
ByAllAccounts Data Aggregation Strategy & Governance 45
Committee of Annuity Insurers 46
Insured Retirement Institute (IRI) 55
NAMIC 57
NAVITUS Health Solutions 85
PIA 88
Privacy4Cars 94

Consumer Comments 96

Consumer Rep – Harry Ting 96

Regulator Comments

California Department of Insurance

This comment letter intends to provide high-level comments to steer discussion on the matters set forth in Article III. As noted in my prior comment letter, the definition of key terms will have major impact on the effect of the Act. While the Definitions section of the Chair Draft is not currently under consideration, the Department looks forward to providing input on that section. Additionally, the Department reserves its right to provide additional comments to this section (Article III – Consumer Requests), consistent with the changes ultimately adopted to the Definitions section of the Chair Draft.

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

One of the major shortcomings of Model 672 as a vehicle for drafting modern privacy legislation is the fact that Model 672 lacks many of the substantive features found in modern privacy laws. Perhaps for this reason, the Chair Draft document had invented entirely new substantive language for the consumer rights of access, correction, and deletion.

Unfortunately, the Chair Draft language is perfunctory and lacks many of the consumer protections contained in Model 670, Sections 8 and 9. Some twenty states have adopted Model 670, or some portion thereof, so it makes no sense to reinvent the wheel when it comes to the rights of access, correction, and deletion. The Working Group should start with the text of Sections 8 and 9 from Model 670, and use these as the basis for developing improved consumer rights. As currently drafted, the rights contained in Section 6 of the Chair Draft represent a diminishment of the rights that consumers have enjoyed for decades in Model 670 states. For example, Section 9 of Model 670 provides that, if a licensee refuses a consumer's request to correct, amend, or delete portions of a consumer's record, the consumer may file a statement setting forth the consumer's disagreement with the licensee's decision. The Chair Draft provides no protection in the event that the licensee ultimately refuses the consumer's request.

Rather than moving consumer protections backward, the Working Group should be making progress. Building off of the established framework of Model 670 will ensure the improvement of consumer rights, as well as promoting consistency for the many states which have followed Model 670 for years.

Section 7 – Sale of Nonpublic Personal Information

At its core, the insurance business is about risk transfer and indemnity. Insurers and producers are paid premium and earn commissions through provision of insurance services requested by the consumer. In contrast to "tech" industry consumers, who often receive free services, in return access to the consumer's information (and the ability to monetize the same), insurance consumers are not a product to be bought and sold. Insurance consumers are paying customers who are often required to obtain insurance

services (e.g.: mandated auto liability insurance, or homeowners' insurance required to secure a home loan).

During discussions with industry about personal information practices of licensees, no licensee or trade group would admit to selling consumer information. Consequently, Model 674 was drafted to include a prohibition against selling consumers' personal information.

Whether or not a consumer permits a licensee to sell the consumer's information bears no relation to the risk underwritten by the insurer, or the commission paid to the producer. Therefore, there is no good reason to permit the sale of insureds' information; allowing the possibility of data sales may lead to coercive or misleading practices which harm consumers.

Section 8 – Use and Disclosure of Sensitive Personal Information

While the definition of "Sensitive Personal Information" ("SPI") will ultimately determine the substantive impact of this section, most privacy laws reserve this designation for information about identification numbers, financial accounts, precise geolocation, religious or philosophical beliefs, racial or ethnic origin, genetic data, health information, and information about sex life and sexual orientation.

SPI relates to the core of a person's identity, and its improper use or disclosure may cause serious harm or embarrassment to the consumer.[1] Consequently, limits should accompany all aspects of the SPI lifecycle, including collection, use, and disclosure. While insurers may have legitimate need for this information for underwriting purposes, they should not be indiscriminately collecting or disclosing SPI for purposes unrelated to servicing a transaction requested by the consumer.

It bears noting that personal information safeguards are of limited use if they are presented to the consumer in a confusing or misleading manner. So-called "dark patterns" have been employed in interface design, either to confuse the consumer, or even to complicate the process of making privacy-protective choices. Consistent with modern privacy laws, the NAIC Privacy Model should prohibit the use of "dark patterns," in order to safeguard consumers' free and informed privacy decision-making.

[1] In one case, now over a decade old, Target's advertising algorithm outed a teenager's pregnancy to her father, by sending her mailers for baby products.

https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

Maine Bureau of Insurance

Comments on Draft Privacy Model, Article III

Bob Wake, Maine Bureau of Insurance

Corrected November 26, 2024

Markup: I have followed these comments with a markup of the relevant sections of the exposure draft. You have asked for comments in Word format, and I repeat the request I made in my previous comments, to return the favor and provide the Drafting Group with all exposure drafts in Word format. Articles II and III (Sections 5 through 8) are entirely new text, so they are reasonably legible when copied and pasted from the PDF, but after this round of comments, we will be moving on to sections where the discussion draft will be the existing text with revisions. Copying and pasting from a PDF does not preserve formatting, so it will result in a jumble where the underlined, deleted, and existing text all look the same. I started to submit my changes on a straight copy-and-paste from the PDF, without reformatting, but I decided that would be too passive-aggressive. But I have included a separate attachment showing that copy-and-paste work, up to the point when I decided to take the time to reformat my markup draft, as a further illustration why we need a Word version of the exposure drafts in order to provide meaningful feedback.

"Authorized" Request: This term is confusing. The intent seems to be to protect the consumer from a request that is made by an impostor, which is clearly an important concern, but the terminology suggests that the consumer needs some sort of authorization before a request can trigger the licensee's duty to respond. I think the term we're looking for here is "authenticated." Draft Model 674 had used the term "verifiable," but that adjective implies that whether the request is actually verified is at the licensee's discretion, while the purpose of this requirement is to protect the consumer, not to protect the licensee. If the request is submitted by some third party on the consumer's behalf, then there does need to be some sort of authorization, and we need to include that in the authentication process, but it is the representation, not the request, that needs to be authorized in those circumstances, either by the consumer or by applicable law.

Verification: I've pulled this out as a separate topic because it's an important and difficult one. The consumer needs to be protected both from unnecessary roadblocks in accessing personal information, and from impostors trying to access their personal information. If the consumer has an account with controlled access, I would expect this to be the normal method for authentication. Otherwise it gets messier. I've tried some language, but I think it needs further work.

Specific Information Requested: The current draft assumes that the consumer will specify with particularity which information the consumer wants to access. We should not require that, nor assume that it is the default scenario, because that makes it too easy for the licensee to treat information it doesn't want to provide as nonresponsive.

A "format specific to the consumer"? I'm not sure what this phrase was supposed to mean. It can't mean there needs to be a different format for each consumer, and it shouldn't mean that each consumer has the unrestricted right to specify a format of the consumer's choosing. (WordPro, anyone?) I don't think the licensee should be prohibited

from providing information in its native format as long as that format is reasonably accessible to the average consumer. PDF, at least in the current era, should also be acceptable, as long as digital originals are properly exported and scanning to graphic format is used only for hard-copy originals.

Deletion: Under FCRA and Model 670, there is no general right to request deletion of information. The right to correction or deletion under those laws has nothing to do with any "right to be forgotten" – they're alternative remedies for information that the consumer asserts to be inaccurate, and my understanding is that the licensee can decide which course is appropriate in the circumstances. Although I have misgivings about a more general right to delete accurate-but-unnecessary information, I'm inclined to think that to whatever extent we decide to mandate deletion, it should be a categorical duty rather than something triggered by a consumer request, as currently structured.

Placement: These three sections do not belong together. While Section 6 deals with various requests that consumers have the right to initiate, and the nature of those requests is similar, Sections 7 and 8 do not. "Opt-in" requirements for the sale of information or for uses and disclosure of sensitive information are limitations on what the licensee can do with the information. It is extremely unlikely that a licensee will receive an unsolicited request to "Please sell my information" or "Please disclose my sensitive information." It might make sense to have a general section on authentication and authorization that lives in Article III and applies in the same manner to both consumer-initiated requests and consent to licensee-initiated requests, but the requirement to obtain consent belongs in Article V as the draft Model is currently structured.

Parent or guardian: A parent's right to access their child's information should not be absolute, at least in the health insurance context in states where children have the right to access certain sensitive health care services without parental consent. I have proposed some optional language inspired by our law, at 24-A M.R.S. § 2208(1)(A)(2). This should only apply where the right is already created by other applicable law, and should not be construed as creating any new rights in situations where children's and parents' interests might be adverse.

Sensitive Personal Information: I don't think this is the time or place for that discussion, because it's part of a larger discussion of how Articles IV through VI are structured, but Article VI as currently drafted might not be the definitive list of permitted disclosures of sensitive personal information without affirmative "opt-in" consent. Why, for example, do joint marketing partners deserve access to sensitive information that shouldn't be used by **anyone** for marketing purposes unless and until the consumer has opted in?

MARKUP OF ARTICLE III. CONSUMER REQUESTS

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

A. Access to nonpublic personal information.

(1) Within 45 days ~~of~~ after an authorized request from a consumer or a consumer's authorized representative, a licensee shall disclose, ~~:(ii). Must be provided~~ in an ~~format specific to the consumer and~~ easily readable format.

(a) All n~~N~~onpublic personal information about ~~a~~ the consumer that is ~~requested by the consumer and~~maintained by the licensee or any contracted third-party service provider, with the exception of~~; that~~:

~~(i). Must include a list of all third-party service providers to in which the licensee~~

~~disclosed the consumer's nonpublic personal information; and~~

~~(ii). Must be provided in a format specific to the consumer and easily readable.~~

~~(2) In response to an authorized request from a consumer in (1) above, a licensee shall not disclose:~~

(i~~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, or unique biometric data.

~~(b)~~ The licensee may instead disclose in generic terms that it maintains this information and list out each type of nonpublic personal information about the consumer~~.~~;

(ii) Information that is voluminous and repetitive, if the duplicative information that has been withheld is described in a manner reasonably understandable by the consumer and the consumer is offered an opportunity to review the information for inconsistencies; or

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

(~~i~~b) ~~. Must include a~~A list of all third-party service providers to in which the licensee disclosed the consumer's nonpublic personal information;

B. Correction of nonpublic personal information.

(1) A consumer may request the correction of their nonpublic personal information.

Commented [RAW1]: Because the hyphen in the PDF was at the end of a line, Word mistook it for a conditional hyphen.

(2) An authorized request from a consumer under this subsection shall identify the specific information that the consumer wishes to correct and provide explanation of why the licensee's information is incorrect.

(3) After receiving an authorized request under this subsection, a licensee shall, within 30 days of receipt of the request, notify the consumer of:

(a) Correction of the information as requested by the consumer or deletion of the information in dispute; or

(b) Denial of the correction, the basis for refusal to correct the information as requested, and the consumer's ability to submit an appeal.

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

(a) The licensee believes the information is correct from clear documentation in its possession or

(b) The licensee received the information from a third-party, such as a healthcare provider, who has the responsibility or authority for determining the accuracy of the information.

C. Deletion of nonpublic personal information.

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

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

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

(b) The information may be necessary:

(i) To perform the contract or service request or benefiting the consumer; or

(ii) To comply with a legal obligation.

(c) 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 30 days, to delete with respect to information stored on an achieved or backup system until the archived or backup systems is deleted. A licensee must notify the consumer of such delay.

D. Request Procedures

(1) ~~Guidelines for responding to authorized requests e~~Except as otherwise provided in this Act, a licensee shall respond to requests submitted under this section 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) ~~(3) A child's~~ The parent or legal guardian ~~may submit a request under this section on behalf of the child regarding processing nonpublic personal information belonging to the child~~of a consumer who is a minor, ***[optional]*** *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.

~~shall respond to an authorized request received from a consumer under this section, unless fulfilling the request proves impossible due to the specific nonpublic personal information is not locatable or retrievable by the licensee.~~

(b) If a licensee if unable to verify that a request has been made or authorized by the consumer, the licensee shall not be required to consider the request ~~and may request that~~until the ~~consumer~~ person making the request provides additional information ~~necessary~~ sufficient to authenticate the consumer and the consumer's request.

(c) If a licensee declines to take action regarding the consumer's request, the licensee shall inform the consumer of the basis for declining to take action and any relevant instructions for how to appeal the decision pursuant to subparagraph (B)(3)(b) of this section.

(2) A consumer may make up to two requests per subsection in a 12-month period.

~~(3) A child's parent or legal guardian may submit a request under this section on behalf of the child regarding processing nonpublic personal information belonging to the child.~~

Section 7. Consent to Sale of Nonpublic Personal Information or to Use or Disclosure of Sensitive Personal Information

~~C. Affirmative Consent: t~~The consumer's affirmative ("opt-in") written consent to the sale of nonpublic personal information as required by Section [17*], or to the use or disclosure of sensitive personal information as required by Section [17**], must be:

A. ~~o~~Obtained separately from any other consent obtained from the consumer;

B. Authenticated in accordance with Section 6D; and~~.~~

C. Subject to revocation or modification at any time at the written request of the consumer or the consumer's authorized representative.

****

Section 17*~~7~~. Sale of Nonpublic Personal Information

A. A licensee shall not sell a consumer's nonpublic personal information, including for purposes of targeted advertising, unless the consumer has affirmatively opted in to the sale of their nonpublic personal information after receiving clear and conspicuous notice.

B. Before a consumer opts in to the sale of nonpublic personal information, a licensee shall provide a clear and conspicuous notice to the consumer, which includes:

(1~~a~~) A description of the categories of nonpublic personal information that the licensee intends to sell;

(2~~b~~) The purpose for which the nonpublic personal information will be sold; and

(3~~c~~) The consumer's right to ~~opt out of~~withhold consent to the sale of nonpublic personal information.

~~C. Affirmative Consent: the consumer's affirmative opt-in consent must be obtained separately from any other consent obtained from the consumer.~~

Section ~~8~~17. Use ~~and~~ or Disclosure of Sensitive Personal Information**

A. ~~A.~~ Licensees may utilize sensitive personal information only ~~for certain identified purposes and uses, including those purposes and uses identified in~~as expressly permitted or required by Article VI (Exceptions to Limits on Disclosures of Financial Information) or other provisions of this Act, or with the affirmative ("opt-in") consent of the consumer.~~:~~

~~B. A consumer shall have the right, at any time, to direct a licensee that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to the authorized purposes and uses;~~

~~C~~B. A licensee that seeks to disclose~~s~~ or process~~es~~ a consumer's sensitive personal information for purposes other than those specified in subsection A of this section shall provide a clear and conspicuous notice to the consumer, which includes:

(1~~a~~) A description of sensitive personal information that the licensee intends to disclose;

(2~~b~~) The purpose for which the sensitive personal information will be processed; and

(3~~c~~) The consumer's right to ~~opt-out of~~withhold consent to the processing of sensitive personal information for those purpose.

~~C. A consumer's affirmative opt-in consent must be obtained separately from any other consent obtained from the consumer.~~

North Dakota Insurance Department

North Dakota is of the opinion that the 45-day deadlines listed within Section 6 (6.A.1 and 6.C.1) should be consistent with the 30 days listed at 6.B.3.

We also feel the request denial language within 6.B.4 (a) is too broad and cedes substantial judgment to the licensee in determining what information is correct. We would like Section 6.B.4(a) struck out. . If parties are not agreeable to deletion of this sub-section, we would insist on, as a compromise, the reference to and inclusion of an appeals process similar to the DOI complaint process for request denials under this sub-section, to ensure licensees are not abusing the denial process and consumers needs are being met.

Considering the language within Section 6.D.1 (a), (b), and (c), we don't feel a restriction of two requests per 12-month period is necessary. We would like 6.D.2 struck out. We assert that a consumer's data is the consumer's, and that consumers should have reasonably unrestricted access to amend, delete, or correct any data possessed by a licensee and 6.D.2 unreasonably restricts that right.

We had no comments relating to Section 7 or Section 8.

Pennsylvania Insurance Department

ARTICLE III. CONSUMER REQUESTS

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

~~A. Access to nonpublic personal information.~~

~~(1) Within 45 days of an authorized request from a consumer, a licensee shall disclose:~~

~~(a) Nonpublic personal information about a consumer that is requested by the consumer and maintained by the licensee or any contracted third-party service provider; that:~~

~~(i) Must include a list of all third-party service providers to in which the licensee disclosed the consumer's nonpublic personal information; and~~

~~(ii) Must be provided in a format specific to the consumer and easily readable.~~

~~(2) In response to an authorized request from a consumer in (1) above, a licensee shall not disclose:~~

~~(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, or unique biometric data.~~

~~(b) The licensee may instead disclose in generic terms that it maintains this information and list out each type of nonpublic personal information about the consumer.~~

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

(1) Access to nonpublic personal information.

(a) A consumer may request a licensee provide a list of all third-party service providers to which the licensee disclosed the consumer's nonpublic personal information.

(b) A licensee's response to a request for access may not include 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, or unique biometric data.

~~B. Correction of nonpublic personal information.~~

Commented [FJ2]: If the term "authorized request" is used, it should be defined.

Commented [JF3]: Is the intent of this section to confine requests for access to third-party disclosures? Or to allow a consumer to request access for any purpose beyond the transaction sought by the consumer (or beyond the purposes set forth in Article VI?)

Commented [JF4]: If the intent of subsection (a) is just to provide a list of third party service providers, is this section necessary?

~~(1) A consumer may request the correction of their nonpublic personal information.~~

~~(2) An authorized request from a consumer under this subsection shall identify the specific information that the consumer wishes to correct and provide explanation of why the licensee's information is incorrect.~~

~~(3) After receiving an authorized request under this subsection, a licensee shall, within 30 days of receipt of the request, notify the consumer of:~~

~~(a) Correction of the information as requested by the consumer or deletion of the information in dispute; or~~

~~(b) Denial of the correction, the basis for refusal to correct the information as requested, and the consumer's ability to submit an appeal.~~

~~(4) A licensee may deny a request for correction if:~~

~~(a) The licensee believes the information is correct from clear documentation in its possession or~~

~~(b) The licensee received the information from a third-party, such as a healthcare provider, who has the responsibility or authority for determining the accuracy of the information.~~

(2) Correction of nonpublic personal information.

(a) A consumer seeking that a licensee correct nonpublic personal information in the possession of a licensee may file a request with the licensee:

(i) Identifying the specific information the consumer wishes to correct.

(ii) Providing an explanation of why the information is incorrect.

(b) Within 30 days of receipt of a request under this subsection, a licensee shall notify the consumer of:

(i) Correction of the nonpublic personal information as requested by the consumer.

(ii) Deletion of the nonpublic personal information in dispute.

(iii) Denial of the consumer's request which must include the basis for refusal to correct the nonpublic personal information as requested

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

(i) The nonpublic personal information is accurate and complete.

Commented [FJ5]: Why do some provisions have a 30 day deadlines and some have 45? Should this be consistent?

(ii) The nonpublic personal information that is the subject of the request for correction was not created by the licensee unless the individual provides a reasonable basis to believe that the originator of the information is no longer available to act on the requested correction.

~~C. Deletion of nonpublic personal information.~~

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

Commented [JF6]: Should this be "direct" the third party to delete the information?

~~(2) The licensee shall not be required to delete nonpublic personal information if:~~

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

~~(b) The information may be necessary:~~

~~(i) To perform the contract or service request or benefiting the consumer; or~~

~~(ii) To comply with a legal obligation.~~

~~(c) 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 30 days, to delete with respect to information stored on an achieved or backup system until the archived or backup systems is deleted. A licensee must notify the consumer of such delay.~~

(3) Deletion of nonpublic personal information.

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

(b) The licensee shall not be required to delete nonpublic personal information if:

(i) The licensee is required by law or regulation to retain the information.

(ii) The information is necessary to perform the contract or service requested by or benefiting the consumer.

(iii) The information is necessary to comply with a legal obligation.

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

(c) A licensee may delay fulfilling a consumer's request for up to 30 days to delete information stored on an archived or backup system. A licensee must notify the consumer of such delay.

BD. Request and Response Procedures

(1) ~~Guidelines for responding to authorized requests except as otherwise provided in this Act,~~ Except as provided in paragraph (2) of this subsection, a licensee shall respond to requests submitted under this section within 45 calendar days. ~~in the following manner:~~

(2) A licensee is not required to respond to a request made under this section if:

(a) ~~A licensee shall respond to an authorized request received from a consumer under this section, unless fulfilling the request proves impossible due to the~~ The specific nonpublic personal information at issue is not locatable or retrievable by the licensee.

(b) ~~If a~~ The licensee is ~~if~~ unable to verify the ~~a~~ request after ~~, the licensee shall not be required to consider the request and may~~ requesting that the consumer provide additional information necessary to authenticate the identity of the consumer and authenticate the consumer's request.

~~(c)~~ (3) If a licensee declines to take action regarding the consumer's request, the licensee shall inform the consumer of the basis for declining to take action and ~~any relevan~~t instructions for how to request a review of the ~~appeal the~~ decision. ~~pursuant to subparagraph (B)(3)(b) of this section.~~

~~(2) A consumer may make up to two requests per subsection in a 12-month period.~~

~~(3) A child's parent or legal guardian may submit a request under this section on behalf of the child regarding processing nonpublic personal information belonging to the child.~~

Section 7. Sale of Nonpublic Personal Information

A. ~~A.~~ Before a~~A~~ licensee may ~~shall not~~ sell, including for purposes of targeted advertising, ~~a consumer's~~ nonpublic personal information~~, including for purposes of targeted advertising, that the licensee has~~ obtained from a consumer:

(1) A consumer must receive the clear and conspicuous notice that includes:

(a) A description of the categories of nonpublic personal information that the licensee intends to sell;
(b) The purpose for which the nonpublic personal information will be sold.

(2) The consumer must affirmatively opt in to the sale. ~~, unless the consumer has affirmatively opted in to the sale of their nonpublic personal information after receiving clear and conspicuous notice.~~

~~B. Before the a consumer opts in to the sale of nonpublic personal information, a licensee shall provide a clear and conspicuous notice to the consumer, which includes:~~

~~(a) A description of the categories of nonpublic personal information that the licensee intends to sell;~~

~~(b) The purpose for which the nonpublic personal information will be sold; and~~

~~(c) The consumer's right to opt out of the sale of nonpublic personal information.~~

~~A.~~B. ~~C. Affirmative Consent: the~~A consumer's affirmative opt-in consent pursuant to subsection A ~~A~~ must be obtained separately from any other consent obtained from the consumer.

Section 8. Use and Disclosure of Sensitive Personal Information

~~A. A.~~ A. ~~l~~Licensee~~s~~ may not utilize sensitive personal information other than for the ~~certain identified~~ purposes and uses~~, including those purposes and uses~~ identified in Article VI (Exceptions to Limits on Disclosures of Financial Information) unless the consumer has affirmatively opted in to the use or disclosure of their nonpublic personal information after receiving clear and conspicuous notice as provided by this section.~~;~~

B. A consumer shall have the right, at any time, to direct a licensee that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to the authorized purposes and uses identified in Article VI (Exceptions to Limits on Disclosures of Financial Information).~~;~~

C. Before a licensee may disclose or process ~~A licensee that discloses or processes~~ a consumer's sensitive personal information for purposes other than those specified in subsection A of this section, a licensee shall provide a ~~clear and conspicuous~~ notice to the consumer that~~, which~~ includes:

(1~~a~~) A description of sensitive personal information that the licensee intends to disclose or process;

(2~~b~~) The purpose for which the sensitive personal information will be disclosed or processed; and

(3~~c~~) A notice that the consumer must opt-in to provide affirmative consent before the consumer's sensitive personal information may be disclosed or processed. ~~The consumer's right to opt out of the processing of sensitive personal information for those purpose.~~

D~~C~~. A consumer's affirmative opt-in consent~~.~~ pursuant to paragraph (C)(3) must be obtained separately from any other consent obtained from the consumer.

Commented [JF7]: To be defined.

Commented [FJ8]: Question re: the "certain identified purposes and uses" and "including" language- Is this meant to be an exclusive list? If not, what would the other "certain" purposes be?

Virginia Bureau of Insurance

The Bureau offers its comments below for the Working Group's consideration along with the attached redline showing the Bureau's proposed revisions to incorporate its comments among other changes.

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

The Bureau generally supports the language of Section 6 and its affirmation of rights allowing consumers to request to access, correct, and delete nonpublic personal information possessed by licensees. To further enhance these rights, the Bureau provides two comments on this section. First, the language in (D)(1)(a) on request procedures around the impossibility of a request needs more clarity for licensees and regulators to understand when fulfilling a request is truly impossible. Second, the Bureau supports revising the text of (D)(2) to maintain the limit on requests to access and delete nonpublic personal information but to remove the cap on requests to correct nonpublic personal information. Consumers should not face any barriers in their requests to correct inaccurate nonpublic personal information.

Section 7 – Sale of Nonpublic Information

The Bureau supports the approach discussed in Section 7 that prohibits the sale of nonpublic personal information absent affirmative opt-in consent of the consumer. Consistent with this approach, the Bureau recommends removing the qualifier "that the licensee has obtained from a consumer" in subsection (A). Nonpublic personal information possessed by a licensee should be treated the same no matter the data source. Removing the qualifier in subsection (A) makes one clear bright-line rule for licensees to follow and will eliminate the need to maintain and demonstrate a data trail as it relates to the sale of nonpublic personal information. Additionally, the Bureau recommends revising the language in (B)(c) to state that the consumer has the right to refuse to opt in to the sale of their nonpublic personal information. The draft's current language about opting out is confusing.

Section 8 – Use and Disclosure of Sensitive Personal Information

The Bureau agrees with the framework set forth in Section 8 that there are certain purposes and uses for which a licensee can process sensitive personal information without needing to provide notice or seek consumer input. However, the Bureau believes that the text in Section 8 should better identify the purposes and uses in subsection A and that consumers should need to affirmatively opt in to allow processing of sensitive personal data outside of the identified purposes and uses. Affirmative opt-in consent to process sensitive personal information shows that this is a category of information that deserves heightened protection and is consistent with its treatment in several states, including Virginia,[1] that have adopted data protection laws.

As such, the Bureau's edits in the attached redline articulate the "identified purposes and

uses" in subsection A that are not identified in the draft language. The Bureau also revised the proposed opt-out language to incorporate an opt-in approach to the processing of sensitive personal information outside of processing permitted under subsection A.

Two other items to flag for the Working Group's consideration: (1) this section refers to "use and disclosure" of sensitive personal information but a better umbrella term may be "processing," and (2) the definition of "sensitive personal information" should be revisited in Section 4 to remove the link to "nonpublic personal financial information."

Redline version for Bureau

ARTICLE III. CONSUMER REQUESTS

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

A. Access to nonpublic personal information.

(1) Within 45 days of an authorized request from a consumer, a licensee shall disclose:

(a) Nonpublic personal information about a consumer that is requested by the consumer and maintained by the licensee or any contracted third-party service provider; that must:

(i) ~~Must~~ Include a list of all third-party service providers to in which the licensee disclosed the consumer's nonpublic personal information; and

(ii) ~~Must~~ Be provided in a format specific to the consumer and easily readable.

(2) In response to an authorized request from a consumer in (1) above, a licensee shall not disclose:

(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, or unique biometric data.

(b) The licensee may instead disclose in generic terms that it maintains this information and list out each type of nonpublic personal information about the consumer.

B. Correction of nonpublic personal information.

(1) A consumer may request the correction of their nonpublic personal information.

(2) An authorized request from a consumer under this subsection shall identify the specific information that the consumer wishes to correct and provide explanation of why the licensee's information is incorrect.

(3) After receiving an authorized request under this subsection, a licensee shall, within 30 days of receipt of the request, notify the consumer of:

(a) Correction of the information as requested by the consumer or deletion of the information in dispute; or

(b) Denial of the correction, the basis for refusal to correct the information as requested, and the consumer's ability to submit an appeal.

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

(a) The licensee reasonably believes the information is correct from clear documentation in its possession or

(b) The licensee received the information from a third-party, such as a healthcare provider, who has the responsibility or authority for determining the accuracy of the information.

C. Deletion of nonpublic personal information.

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

(2) The licensee ~~shall not be~~ 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:

(i) To perform the contract or service request ~~or~~ benefitting the consumer; or

(ii) To comply with a legal obligation.

(c) 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 30 days, to delete ~~with respect to~~ nonpublic personal information stored ~~on an achieved~~ on an archived or backup system until the archived or backup systems is deleted. A licensee must notify the consumer of such delay.

D. Request Procedures

(1) ~~Guidelines for responding to authorized requests~~ Except as otherwise provided in this Act, a licensee shall respond to requests submitted under this section in the following manner:

(a) A licensee shall respond to an authorized request received from a consumer under this section, unless fulfilling the request proves impossible due to the specific nonpublic personal information is not locatable or retrievable by the licensee.

(b) If a licensee if unable to verify a request, the licensee shall not be required to consider the request and may request that the consumer provide additional information necessary to authenticate the consumer and the consumer's request.

(c) If a licensee declines ~~to take action regarding~~ the consumer's request, the licensee shall inform the consumer of the basis for declining ~~to take action~~ the request and any relevant instructions for how to appeal the decision ~~pursuant to subparagraph~~ (B)(3)(b) of this section.

(2) A consumer may make up to two requests each for access or deletion ~~per subsection~~ in a 12-month period. There shall be no cap on the number of requests to correct nonpublic personal information.

(3) A child's parent or legal guardian may submit a request under this section on behalf of the child regarding processing nonpublic personal information belonging

Commented [DB1]: The language here is unclear. I would propose deleting the text "until the archived or backup systems is deleted" as the archived or backup system may not be deleted.

Commented [DB2]: The provision cited does not elaborate on the appeal procedures. Here might be the appropriate place to include the appeal procedures.

to the child.

Section 7. Sale of Nonpublic Personal Information

A. A licensee shall not sell a consumer's nonpublic personal information, including for purposes of targeted advertising~~, that the licensee has obtained from a consumer,~~ unless the consumer has affirmatively opted in to the sale of their nonpublic personal information after receiving clear and conspicuous notice.

B. Before a consumer opts in to the sale of nonpublic personal information, a licensee shall provide a clear and conspicuous notice to the consumer, which includes:

(a) A description of the categories of nonpublic personal information that the licensee intends to sell;

(b) The purpose for which the nonpublic personal information will be sold; and

(c) The consumer's right to ~~opt out of~~ refuse to opt in to the sale of nonpublic personal information.

C. ~~Affirmative Consent:~~ The consumer's affirmative opt-in consent must be obtained separately from any other consent obtained from the consumer.

Section 8. Use and Disclosure of Sensitive Personal Information

Commented [DB3]: Processing may be a better umbrella term than use and disclosure.

A. Licensees may process ~~utilize~~ sensitive personal information ~~for certain identified purposes and uses~~ as is reasonably necessary and proportionate to achieve the purposes for which the personal information was collected, including those purposes and uses identified in Article VI (Exceptions to Limits on Disclosures of ~~Financial~~ Nonpublic Personal Information);

B. ~~A consumer shall have the right, at any time, to direct a licensee that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to the authorized purposes and uses;~~ A licensee shall not process a consumer's sensitive personal information for purposes other than those specified in subsection A of this section, unless the consumer has affirmatively opted in to the processing of their sensitive personal

information after receiving clear and conspicuous notice.

C. Before a consumer opts in to the processing of their sensitive personal information for purposes other than those specified in subsection A of this section, a licensee ~~that discloses or processes a consumer's sensitive personal information for purposes other than those specified in subsection A of this section~~ shall provide a clear and conspicuous notice to the consumer, which includes:

(a) A description of the categories of sensitive personal information that the licensee intends to ~~disclose~~ process;

(b) The purpose for which the sensitive personal information will be processed; and

(c) The consumer's right to ~~opt out of~~ refuse to opt in to the processing of sensitive personal information for those purpose.

D. A consumer's affirmative opt-in consent must be obtained separately from any other consent obtained from the consumer.

Industry Comments

ACLI

Article III Section 6 Access, Correction, and Deletion of Nonpublic Personal Information

Section 6(A)(1) Comments

- Under the current Chair's Draft language 6(A)(1)(i), insurers are required to provide a list of nonaffiliated third parties who have access to nonpublic personal information. This requirement could be satisfied more efficiently via a list of the types or categories of third parties (rather than individual third parties) and could be included on a website disclosure, rather than on an individual basis.
- The list of individual third party service providers a licensee uses is not static, meaning a particularized point-in-time disclosure instead of a categorical disclosure results in potentially outdated or inaccurate information to the consumer. Consumers are familiar with categorical notices and are able to make more informed decisions about the use of their information compared to a potentially opaque third party's name. *Compare,* "adverting networks" and "ABC Solutions, LLC." The name alone of a third party means less to a consumer than the actual category of services that the provider offers. Instead of providing a list which could change and would not provide a substantial benefit to consumers, licensees should be able to provide categorical notices. Lastly, in terms of security, it is far better to have categorical notices rather than invite bad actors to target specific third party service providers that provide services across the industry, e.g., Crowdstrike.
- A(1)(a)(ii) states information must be provided "specific to the consumer." Rather than this language, which could be confusing and misinterpreted, we suggest the below changes, consistent with other privacy laws like the CCPA.
- Suggested Language: "Access to nonpublic personal information. (1) Within 45 days of an authorized request from a consumer, a licensee shall disclose: (a) Nonpublic personal information about a consumer that is requested by the consumer and maintained by the licensee or any contracted third-party service provider; on behalf of the licensee that: (i). Must include ~~a list of all~~ categories of third-party service providers to ~~in~~ which the licensee disclosed the consumer's nonpublic personal information; and (ii). Must be provided in a readily accessible format ~~specific to the consumer~~ and easily readable."

Section 6(B) Comments

- Changing the requirement from 30 days to 45 days is consistent with CCPA 7021, VCDPA 59.1-577, and the Rhode Island Data Transparency and Privacy Protection Act.
- Suggested Language: "Correction of nonpublic personal information. (1) A consumer may request the correction of their nonpublic personal information. (2) An authorized request from a consumer under this subsection shall identify the specific information that the consumer wishes to correct and provide explanation of why the licensee's information is incorrect. (3) After receiving an authorized request under this subsection, a licensee shall, within ~~30~~ 45 days of receipt of the request, notify the consumer of: (a) Correction of the information as requested by the consumer or deletion of the information in dispute; or (b) Denial of the correction, the basis for refusal to correct the information as requested, and the consumer's ability to submit an

appeal. (4) A licensee may deny a request for correction if: (a) The licensee believes the information is correct from clear documentation in its possession or (b) The licensee received the information from a third-party, such as a healthcare provider, who has the responsibility or authority for determining the accuracy of the information."

Section 6(C)(3) Comments

- We recommend standardizing this section with other consumer privacy laws like California, Colorado, Virginia, etc. Removing the 30-day time frame allows for adequate time to address the consumer's request, while allowing the licensee to notify the consumer of any delay.
  Further, the edits below are consistent with CCPA (Section 7022(d)) "If a business, service provider, or contractor stores any personal information on archived or backup systems, it may delay compliance with the consumer's request to delete, with respect to data stored on the archived or backup system, until the archived or backup system relating to that data is restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose." This language is rooted in an existing state comprehensive privacy law and addresses the concerns surrounding archived media.
- Suggested Language: A licensee may delay fulfilling a consumer's request ~~up to 30 days,~~ to delete with respect to data ~~information~~ stored on an achieved or backup system until the archived or backup ~~systems is deleted.~~ system relating to that data is restored to an active system or is next accessed or used by the licensee or third- party service provider. A licensee must notify the consumer of such delay.

Section 6(D) Comments

- This section includes an exemption that excuses the licensee from honoring a request where it is impossible to locate or retrieve the relevant data. "Impossible" is a very high bar which does not consider the variety of reasons that it would not be feasible to fulfill the request. Instead this should be revised to provide an exemption where data is not "reasonably feasible" locatable or retrievable. This is consistent with NYDFS 500.13.
- The suggested language below in D(1), is consistent with CCPA 791.08 and provides parameters for requests.
- For the safety of the consumer, we also recommend including language that a parent or guardian show proper documentation to validate they can make such request on behalf of the child.
- Suggested Language: "D. Request Procedures (1) Guidelines for responding to authorized requests except as otherwise provided in this Act, a licensee shall respond to requests, which are reasonably described by the individual and reasonably locatable and retrievable by the insurance institution submitted under this section in the following manner: (a) A licensee shall respond to an authorized request received from a consumer under this section, unless fulfilling the request proves ~~impossible~~ not reasonably feasible due to the specific nonpublic personal information ~~is not~~ not being locatable or retrievable by the licensee (b) If a licensee if unable to verify a request, the licensee shall not be required to consider the request and may request that the consumer provide additional information necessary to authenticate the consumer and the consumer's request. (c) If a licensee declines to take action regarding the consumer's request, the licensee shall inform the consumer of the basis for declining to take action and any relevant instructions for how to appeal the decision pursuant to subparagraph (B)(3)(b) of this section. (2) A consumer may make up to two requests per subsection in a 12-month period. (3) A child's

parent or legal guardian may submit a request under this section on behalf of the child with proper documentation regarding processing nonpublic personal information belonging to the child."

New Section 6(E) Comments

- Many states' existing consumer privacy laws afford the licensee a reasonable extension to respond to a consumer request to access, correct, or delete their information. ACLI recommends adding a similar extension to this model.
- Suggested Language: "E. The licensee may extend a response to a consumer's request under this section by 45 additional days when reasonably necessary, considering the complexity and number of the consumer's requests; provided the licensee informs the consumer of any such extension within the initial 45 day response period and of the reason for the extension."

Article III Section 7 Sale of Nonpublic Personal Information

Section 7 Comments

- There are numerous issues with Section 7. First, "sale" is not defined. Second, there are provisions that conflict with the broader set of GLBA rights. Rather than revise the existing draft language, the suggested language accomplishes the same goal in a way that does not conflict with GLBA opt-out requirements. As opposed to providing a redline for this section, we recommend striking the section entirely and replacing it with the following language.
- Suggested Language: "Limits on Targeted Advertising Limitation on targeted advertising. A consumer has the right to opt-out of Targeted Advertising. Request procedures. (1) A licensee shall act on the request within 15 days of receipt. (2) 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. (3) A licensee is under no obligation to obtain additional data to execute the opt-out request. (4) A licensee may not solicit the consumer to change their opt-out selection for twelve months."

Article III Section 8 Use and Disclosure of Sensitive Personal Information

Section 8(A)-(B) Comments

- The scope of "authorized purposes" should be clarified. As drafted, it suggests there are additional authorized purposes beyond those specified in Article VI, but there is no indication of what those purposes might be. These should be clearly defined. Very few US privacy laws regulate companies' internal use of data that they already maintain. Instead, privacy laws (including the existing Model 672) regulate how the data is shared. Attempting to regulate internal use of data would be a significant change to existing law, and it would be very complex for insurers to identify all of the ways that they need to use data in order to process requested transactions and conduct business.
- Additionally, Article VI, was drafted to define authorized purposes for *disclosure* of personal information – *not use*. This language needs to be carefully reviewed and broadened to allow more flexibility for data usage needed to conduct business. Attempting to scope the exact purposes for which usage is required is highly impracticable, and may change over time.

Section 8(D) Comments

- Like Section 7 above, this section is inconsistent as to whether it is intended to be an opt-in requirement or opt-out. This should be clarified to be an opt-out requirement, consistent with other privacy laws like the CCPA.

- Further, exceptions to Section 8 should include those already listed as exceptions to the notice and opt-out regime in GLBA and the current Model 672.
- Suggested Language: "C. A consumer's affirmative ~~opt-in~~ opt-out consent must be obtained separately from any other consent obtained from the consumer."

Finally, as an organizational note, ACLI recommends that Sections 7 & 8 fit better within Article 5, if this language shifts back to an opt out.

ACLI Appendix A Article III Comments

ARTICLE III. CONSUMER REQUESTS

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

A. Access to nonpublic personal information.

(1) Within 45 days of an authorized request from a consumer, a licensee shall disclose:

(a) Nonpublic personal information about a consumer that is requested by the consumer and maintained by the licensee or any contracted third-party service provider on behalf of the licensee~~;~~ that:

(i). Must include ~~a list of all~~categories of third-party service providers to ~~in~~ which the licensee disclosed the consumer's nonpublic personal information; and

(ii). Must be provided in a readily accessible format ~~specific to the consumer~~ and easily readable.

(2) In response to an authorized request from a consumer in (1) above, a licensee shall not disclose:

(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, or unique biometric data.

(b) The licensee may instead disclose in generic terms that it maintains this information and list out each type of nonpublic personal information about the consumer.

B. Correction of nonpublic personal information.

(1) A consumer may request the correction of their nonpublic personal information.

(2) An authorized request from a consumer under this subsection shall identify the specific information that the consumer wishes to correct and provide explanation of why the licensee's information is incorrect.

(3) After receiving an authorized request under this subsection, a licensee shall, within ~~30~~ 45 days of receipt of the request, notify the consumer of:

(a) Correction of the information as requested by the consumer or deletion of the information in dispute; or

(b) Denial of the correction, the basis for refusal to correct the information as requested, and the consumer's ability to submit an appeal.

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

(a) The licensee believes the information is correct from clear documentation in its possession or

(b) The licensee received the information from a third-party, such as a healthcare provider, who has the responsibility or authority for determining the accuracy of the information.

C. Deletion of nonpublic personal information.

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

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

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

(b) The information may be necessary:

(i). To perform the contract or service request or benefiting the consumer; or

(ii). To comply with a legal obligation.

(c) 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 30 days~~, to delete with respect to ~~information~~ data stored on an achieved or backup system until the archived or backup ~~systems is deleted~~system relating to that data is restored to an active system or is next accessed or used by the licensee or third-party service provider. A licensee must notify the consumer of such delay.

D. Request Procedures

(1) Guidelines for responding to authorized requests except as otherwise provided in this Act, a licensee shall respond to requests, which are reasonably described by the

individual and reasonably locatable and retrievable by the insurance institution, submitted under this section in the following manner:

(a) A licensee shall respond to an authorized request received from a consumer under this section, unless fulfilling the request proves ~~impossible~~ not reasonably feasible due to the specific nonpublic personal information not being~~is not~~ locatable or retrievable by the licensee.

(b) If a licensee if unable to verify a request, the licensee shall not be required to consider the request and may request that the consumer provide additional information necessary to authenticate the consumer and the consumer's request.

(c) If a licensee declines to take action regarding the consumer's request, the licensee shall inform the consumer of the basis for declining to take action and any relevant instructions for how to appeal the decision pursuant to subparagraph (B)(3)(b) of this section.

(2) A consumer may make up to two requests per subsection in a 12-month period.

(3) A child's parent or legal guardian may submit a request under this section on behalf of the child with proper documentation regarding processing nonpublic personal information belonging to the child.

E. The licensee may extend a response to a consumer's request under this section by 45 additional days when reasonably necessary, considering the complexity and number of the consumer's requests; provided the licensee informs the consumer of any such extension within the initial 45 day response period and of the reason for the extension.

Section 7. ~~Sale of Nonpublic Personal Information~~Limits on Targeted Advertising

~~A. A licensee shall not sell a consumer's nonpublic personal information, including for purposes of targeted advertising, that the licensee has obtained from a consumer, unless the consumer has affirmatively opted in to the sale of their nonpublic personal information after receiving clear and conspicuous notice.~~

~~B. Before a consumer opts in to the sale of nonpublic personal information, a licensee shall provide a clear and conspicuous notice to the consumer, which includes:~~

~~(a) A description of the categories of nonpublic personal information that the licensee intends to sell;~~

~~(b) The purpose for which the nonpublic personal information will be sold; and~~

~~(c) The consumer's right to opt out of the sale of nonpublic personal information.~~

~~C. Affirmative Consent: the consumer's affirmative opt in consent must be obtained separately from any other consent obtained from the consumer.~~

A. Limitation on targeted advertising. A consumer has the right to opt-out of Targeted Advertising. Request procedures.

(1) A licensee shall act on the request within 15 days of receipt.

(2) 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.

(3) A licensee is under no obligation to obtain additional data to execute the opt-out request.

(4) A licensee may not solicit the consumer to change their opt-out selection for twelve months.

Section 8. Use and Disclosure of Sensitive Personal Information

A. Licensees may utilize sensitive personal information for certain identified purposes and uses, including those purposes and uses identified in Article VI (Exceptions to Limits on Disclosures of Financial Information);

B. A consumer shall have the right, at any time, to direct a licensee that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to the authorized purposes and uses;

C. A licensee that discloses or processes a consumer's sensitive personal information for purposes other than those specified in subsection A of this section shall provide a clear and conspicuous notice to the consumer, which includes:

(a) A description of sensitive personal information that the licensee intends to disclose;

(b) The purpose for which the sensitive personal information will be processed; and

(c) The consumer's right to opt out of the processing of sensitive personal information for those purpose.

D. A consumer's affirmative ~~opt in~~opt-out consent must be obtained separately from any other consent obtained from the consumer.

AHIP

- **Timeframe.** The time for correction in Article III, Section 6.B, presently shown as 30 days, should align with Sections 6.A and C of 45 days. Keeping these time limitations consistent will minimize confusion for consumers, industry, and regulators.

- **Definitions.** It would be beneficial to all parties to have the term "sale" or "sell" defined or clarified. To do so, language could be used which is similar to that found in the HIPAA Privacy Rule, Section 164.502(a)(5)(ii)(B)(1) which provides:

(B) For purposes of this paragraph, *sale of protected health information means*:
(1) Except as provided in paragraph (a)(5)(ii)(B)(2) of this section, a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information.

This language could be easily modified by replacing references to "protected health information" with "nonpublic personal information," and "covered entity or business associate" with "licensee." If needed, AHIP welcomes the opportunity to draft language that would accomplish this recommendation.

- **Form**. It would be beneficial if there was a single, uniform form or template for use by consumers to make requests for access, correction, and deletion. This might be handled by including a note in the Model that such a uniform form should be developed by regulation or bulletin.

APCIA

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

At the outset APCIA notes that the collection of consumer information is a necessity for both insurers and consumers. Without the information provided by consumers, our members would be unable to adequately or accurately underwrite or price the relevant coverage. Moreover, consumers both expect a high degree of personalization[2] and have concerns about the use of their data.[3] The take-away from these expectations is that all of us in the insurance industry must balance competing needs, desires, and fears. APCIA submits that plain language disclosure about what happens to information is the best means to achieve that end and not prescriptive rules that assume ill intent by any party.

Disclosure of "Nonpublic Personal Information" and Third Party Service Providers

Section 6A(1) requires licensees to disclose, within 45 days of a consumer's authorized request, the nonpublic personal information maintained by the licensee or third-party service providers and a customized list of all such providers. This obligation to create lists of third-party service providers is excessively burdensome and offers limited value to consumers. For instance, under the current Draft Model's broad definitions of "nonpublic personal information" and "third-party service providers," licensees would need to list out auto body shops, AWS, Microsoft (for email services), and numerous IT or back-end service providers, none of which will likely have information meaningful to the consumer. All companies, large and small, may have thousands of vendors. Determining which specific vendors received data for an individual consumer is impractical and resource intensive without yielding useful information to the consumer, particularly if the licensee is required to provide the information itself. Further, agreements with third party service providers often prohibit disclosure, especially in instances where the service being provided relates to fraud detections or assistance with litigation. Providing vendor lists would also create security risks by exposing sensitive operational details, effectively offering a roadmap to the company's network.

Given these concerns, APCIA recommends eliminating the revised definition of "nonpublic personal information" and rewriting Section 6A to require disclosure of categories of third- party recipients upon request, consistent with state laws like the CCPA/CPRA. This approach aligns with longstanding insurance norms, enhances consumer understanding by explaining why entities access personal information, and avoids imposing disproportionate costs on businesses. It also ensures meaningful transparency while avoiding excessive costs and risks to the industry.

Format Specific to the Consumer and Easily Readable

Section 6A(1)(a)(ii) requires a licensee to disclose requested information in a "format specific to the consumer and easily readable." Allowing each consumer to specify the format and individually determine what is easily readable would be extremely burdensome or impossible. To ensure feasibility, it would be more practical to enable companies to establish a repeatable process. APCIA recommends revising this provision to allow licensees to respond to data access requests in any reasonable electronic or hard copy format. We recommend looking to CCPA which allows for a "format that is easily understandable to the average consumer, and to the extent technically feasible, in a structured, commonly used, machine-readable format…".

Self-Help Tools

Section 6A(2) should allow a licensee to direct consumers to self-help tools, such as instructing them to log in to their accounts to view and print much of their nonpublic personal information. Similar provisions exist in state comprehensive privacy laws and could serve as a model. Additionally, the section should clarify that redaction of certain personal data is not required if the data is already available to the consumer in unredacted form (e.g., through their account). However, any documents created specifically in response to a data subject access request (DSAR) may need to exclude certain sensitive information for security and privacy purposes.

Routine Updates

As noted throughout these comments, the Draft Model currently includes a broad definition of nonpublic personal information. Section 6B(1) allows consumers to request corrections to their nonpublic personal information, but the broad definition of this term could lead to Section 6B(1) being used for routine updates, like mailing addresses or phone numbers— tasks better handled through customer service than as a regulatory requirement. To address this, APCIA recommends eliminating the revised definition of "nonpublic personal information." Section 6B(1) should be limited to the existing definition of nonpublic personal information found in the existing Model #672, focusing on data related to insurance purchases while excluding health information, or narrowed further to corrections of information used specifically in underwriting or claims coverage.

Denials

Section 6B(4) allows a licensee to deny a correction request if the information is deemed correct based on "clear documentation in its possession." Traditionally, the standard in privacy laws has been a "good faith basis to believe the information is accurate." The current Draft Model, however, seemingly provides only two reasons for denying correction requests, neither of which adequately addresses potential claims-handling scenarios. For example, consumers may "change their minds" about facts, sometimes after consulting an attorney, requiring the licensee to retain both versions for accurate records. Similarly, claimants may revise their statements from what was initially shared during the First Notice of Loss. Both versions are relevant and "correct" because they reflect statements actually made by the claimant, even if one is closer to the truth.

Relatedly, Section 6D(2) does limit a consumer to two requests per subsection in a 12-month period. While the drafted language is a step in the right direction, it needs further refinement. The Draft Model should include provisions allowing a licensee to refuse or limit excessive or repetitive requests, particularly those requiring unreasonable effort to redact, and to charge for duplicative or excessive demands. This approach aligns with similar rights provided under existing state comprehensive privacy laws.

Deletion of Nonpublic Personal Information Maintained by a Third Party

Section 6C(1) requires that within 45 days of an authorized request from a consumer, a licensee shall delete the nonpublic personal information about the consumer that is maintained by any third-party service provider on the licensee's behalf. This is unworkable as licensees cannot directly delete any information maintained by the third-party service provider. APCIA suggests that this provision be amended to clarify that the licensee is required to *request* that the third-party service provider delete the nonpublic personal information about the consumer that is maintained by that third-party service provider on the licensee's behalf.

Insufficient Exceptions to Deletion Requests

The list of exceptions to deletion requests included in section 6C(2) is missing many critical components typically found in privacy laws such as CCPA. While exceptions to comply with a legal obligation or to perform a service for the individual are included, missing exemptions include, for example, the ability to use nonpublic personal information solely for internal purposes, such as compliance with a company's record retention policy or schedule, or for reasons reasonably expected by the consumer. As written, a licensee would also not be able to use any nonpublic personal information in analytics after the insurance contract ended.

This isn't just operationally challenging for businesses, but also confusing for consumers who would potentially read this section as allowing them to request that a licensee delete all of their data. A significant amount of nonpublic personal information is required to be maintained under DOI regulations, at least until the statute of limitations expires. Given the limited circumstances that would legally allow for deletion, perhaps it would be better to clarify for which nonpublic personal information consumers could make such a request.

Similarly, there should be exceptions for access requests. For example, an insurance company should not be required to disclose the information it collects pursuant to fraud investigations or in calculating settlement offers.

Deletion of Back Ups

Section 6C(3) seems to require removal of individual consumer data from backups within a short period. Although providing for a short delay, this requirement is extremely onerous and would require a record management system outside of traditional operations. The vast majority of privacy laws, including CCPA, have excluded data in archives and back up tapes from the right to deletion because of this complexity. APCIA recommends the requirement align with established practices, allowing licensees to retain data on backup media until those systems are overwritten, deleted, or destroyed in accordance with the licensee's existing information security and records management protocols.

Appeal Process

Section 6D provides a right of appeal when a request is rebuffed, but, unlike the state comprehensive privacy laws that this appears to be based on, there is no timeframe or other outline of the appeal process requirements. APCIA recommends that the Working Group look to the Virginia Consumer Data Protections Act, which establishes an explicit appeal process if a business denies a consumer's requests. This includes, among other things, providing the consumer clear instructions on how to submit an appeal and timeframes for the appeals.

Request by Guardian/Parent

Section 6D(3) should be amended as follows: "A KNOWN child's parent or legal guardian may submit a request under this section WITH PROPER DOCUMENTATION on behalf of the child regarding processing nonpublic personal information belonging to the child. The purpose of these edits are to ensure that the actions taken on behalf of a child are done so by those that have authority to do so.

Response Times

APCIA recommends several changes relating to the response times found throughout Section 6. First, access, correction and deletion should all have the same 45-day time period to respond. It isn't clear why correction – the process that requires factual investigation- should have a shorter period of 30 days. Additionally, for request procedures, there needs to be an option to request additional time to investigate and respond, preferably like that found in the California Consumer Privacy Act (CCPA) which allows a business to request one 45-day extension, "when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period." We also encourage the Working Group to clarify that all timeframes are business days. Without this clarification it could reduce an already difficult timeframe to meet, particularly when using a third-party administrator. Finally, the sections should also clarify that the 45 days to respond starts only after the request is authorized and after the licensee has verified the identity of the person making the request. Verification can take up to 10 days if the ID verifications questions are not fully completed by the individual making the request.

Lookback Period

As written, Section 6 of the Draft Model does not contain a defined lookback period for any of the rights, which would indicate that a licensee would potentially have to provide any and all nonpublic personal information ever held on that consumer, which would include prior IP addresses or purchasing histories under the draft definition of "nonpublic personal information." This is especially challenging for the right to access, including the requirement to disclose for which third parties' licensees have disclosed nonpublic personal information. Insurers may not have these full historical records. APCIA strongly recommends incorporating a lookback period consistent with the CCPA, such as "the preceding 12 months," to ensure practicality and alignment with existing standards.

Requests By Consumer

Throughout Section 6, the Draft Model references "nonpublic personal information about a consumer that is *requested by the consumer*." This language is confusing as it implies that each request could be uniquely customized for the requesting consumer. Under the CCPA, entities can provide consumers with options (e.g., marketing information, claims information) while also allowing them to select "all personal information." Adopting a similar approach here could provide clarity and flexibility while maintaining consumer choice.

Section 7. Sale of Nonpublic Personal Information

Definition of Sale

As addressed previously and further into these comments, APCIA respectfully requests that in addition to the Article III text that the Working Group consider discussing definitions that are foundational to the requirements and expectations in this section. For Section 7 comments and recommendations are dependent on what the drafters deem to be a sale. This is largely because some states define "sale" as an exchange for money, while others define it as an exchange for anything of value. APCIA encourages a definition that follows from a traditional understanding of sale, which requires the exchange of money and is not tied to services being provided.

Targeted Advertising

As mentioned above, the Draft Model currently has no definition of the term "sale." While the definition section is not the focus of this exposure, we would advocate for a definition that follows from a traditional understanding of sale, which requires the exchange of money and is not tied to services being provided. That said, without further clarity around the definition of "sale," our comments on Section 7 reflect what we perceive to be included within the definition, such as "targeted advertising." Including "targeted advertising" within the definition of a "sale" introduces significant confusion, as it is inconsistent with traditional understandings of what constitutes a sale.

Targeted advertising encompasses a variety of practices, including cross-context behavioral advertising (e.g., generating ads for a user on a social media platform based on their visit to a website), demographic-based ads displayed on social media, retargeting ads after a user leaves a website mid-process, or even sending physical postcards to individuals on a purchased mailing list. In most instances, privacy laws have not considered these activities a "sale" of personal information. As long as the platform or medium displaying the ad uses data solely for ad placement and not for any other purpose, it is inaccurate to characterize this as a sale of personal information—no more so than when a body shop receives claimant contact information to complete vehicle repairs. The reason some privacy laws, such as the CCPA, consider the specific activity of "cross-context behavioral advertising" a sale (as opposed to other targeted advertising) is because social media companies not only provide a service to advertisers by placing ads based on cookies created when visiting websites, but also use the personal information for their own purposes (i.e., to create profiles of individuals). If social media companies used personal information solely for ad placement, it would not be considered a "sale," they would be "service providers" performing services at the direction of their client. To more appropriately address targeted advertising, which is typically not considered a "sale," APCIA recommends focusing on an opt-out structure, to align with the CCPA. Under this structure, for example, when a user visits a website, they would be presented with a privacy notice and may choose to opt-out of third party cookies or select which third-party cookies may be deployed.

Opt In/Opt Out

Section 7 of the Draft Model requires a consumer to "affirmatively opt in to the sale of their nonpublic personal information after receiving clear and conspicuous notice." While protecting consumer privacy is essential, requiring opt-in consent for the sale of nonpublic personal information diminishes the consumer experience and creates significant operational challenges or impracticalities, particularly so without a clear definition of "sale." Businesses often interact with consumers anonymously (e.g., website visitors), making prior consent impractical and requiring intrusive identification methods. Frequent opt-in prompts added friction, frustrating consumers and deterring engagement while limiting personalization and valuable interactions. Implementing and managing opt-in systems across various platforms and jurisdictions is complex and costly, ultimately impacting consumers through higher prices or reduced services.

This issue is not unique to the insurance industry; it has been considered and addressed internationally and the resolution has been to take an opt-out approach. That approach, requiring clear disclosures and opt-out mechanisms, protects privacy without compromising convenience or efficiency. If insurance companies move to an opt-in standard, it would make our industry an outlier and handicap our industry without any indication of providing consumers any meaningful benefit. At a time when regulators are concerned about disparities in consumers' access to coverage, this

would be a setback. Even the CCPA, a very robust comprehensive privacy law, does not require an opt-in standard.

Exceptions

First and foremost, we urge the Working Group to eliminate the opt-in approach found in Section 7. Without elimination, the APCIA recommends the Working Group consider adding exceptions for standard insurance activities, e.g., referring applicants for coverage to another insurance carrier in exchange for a referral fee. This task could also be achieved by a narrowly tailored definition of "sale" focused on exchanges for monetary consideration.

Section 8. Use and Disclosure of Sensitive Personal Information

Identified/Authorized Purposes and Uses

Section 8 addresses the use and disclosure of sensitive personal information but lacks clarity in defining "authorized purposes and uses" and "identified purposes and uses." This vagueness makes it challenging to provide substantive feedback.

Specifically, Section 8A allows licensees to use sensitive personal information for "certain identified purposes and uses, including those identified in Article VI." The term "including" implies the existence of additional purposes and uses beyond those listed in Article VI. However, the Draft Model does not specify what these additional purposes and uses are, leaving their scope ambiguous.

Further complicating matters, referencing Article VI as a source of "identified purposes" is confusing. Article VI of the Draft Model, which encompasses Sections 19, 20, and 21, outlines exceptions to opt-out requirements based on conditions unrelated to sensitive personal information. It isn't clear how reading Article VI tells a licensee or a consumer when sensitive personal information can be used and for what purpose. For example, Section 19 provides that, in certain circumstances, the opt-out requirements found in Section 12 and 16 don't apply if licensees provide nonpublic personal information to a nonaffiliated third party to perform services for the licensee, including joint marketing. However, it is unclear how this provision connects to the "purposes and uses" referenced in Section 8. As currently drafted, this lack of clarity undermines the ability to interpret how sensitive personal information can or should be handled under the Draft Model.

Internal Use of Data

Section 8 imposes limitations on a licensee's use of sensitive personal data. Few U.S. privacy laws impose restrictions on how companies use data internally once it is collected. Instead, privacy laws (including the existing Model 672) regulate how the data is shared. Attempting to regulate internal use of data would be a significant change to existing law, and it would be very complex for insurers to identify all of the potential ways that they may need to use data in order to process requested transactions and conduct business. A rigid framework governing internal data use could inadvertently stifle innovation, increase operational costs, and create compliance burdens without providing meaningful benefits to consumers.

Opt In/Opt Out

As with Section 7, APCIA recommends an opt-out approach apply to Section 8. That approach, requiring clear disclosures and opt-out mechanisms, protects privacy without compromising convenience or efficiency.

Additional Considerations

Section 4. Definitions

APCIA members have several concerns with the definitions of terms found or missing in Section 4, with many of those concerns being interrelated with the provisions of Draft Model Article III. While we understand the decision to review definitions towards the end of drafting, we respectfully suggest that certain key definitions need to be discussed at the onset of Article III discussions. Specifically, the comments and recommendations above are dependent on what the drafters deem to be a sale, how broadly nonpublic personal information is defined, and how targeted advertising is understood.

As noted earlier in these comments, the definition of "nonpublic personal information" is crucial and as currently defined in the Draft Model includes any information that is linked or reasonably linked to an identified or identifiable natural person. As this is a huge movement away from the traditional GLBA classifications and definitions of nonpublic personal (or personal health) information, it deserves a closer review, specifically of all the provisions that reference different classes of personal data to ensure regulatory intent is still reflected. APCIA recommends eliminating the revised definition of "nonpublic personal information," and instead reverting to the definition of nonpublic personal information found in the existing Model #672.

APCIA recommends that the Working Group include a definition for the undefined term "sale" that follows from a traditional understanding of sale, which requires the exchange of money and is not tied to services being provided.

For "targeted advertising," APCIA recommends the following definition:

"Targeted advertising" means displaying online advertisements to a consumer where the advertisement is selected based upon data that is linked or reasonably linkable to an identified or identifiable natural person obtained from that consumer's activities across nonaffiliated websites or online applications over time to predict such consumer's preferences or interests.

"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 personal data solely for measuring or reporting advertising performance, reach, or frequency.

These concerns are not all encompassing, and only represent some of the definitional questions raised while reviewing Article III. Additional issues impacting definitions throughout the Draft Model will likely be identified as drafting evolves.

Conclusion

Privacy is an important matter, and an insurance-specific approach must reconcile with the context of the industry, align with the broader landscape for financial institutions nationally, and consider certain state and federal requirements. Any privacy model law ultimately developed by the NAIC must be practical, reasonable, and workable. It must ensure that its provisions are integrated and work well together and achieve the intended objective of protecting consumers while allowing licensees to meet their business obligations.

ATLA

The American Land Title Association (ALTA), representing the real estate settlement services, abstract, and title insurance industry, appreciates the opportunity to provide the following comments on the updates to Model 672.

In addition to the redlines below, there are a few general observations we would like to make as the workgroup continues this process. First, where appropriate and relevant to the insurance industry, concepts from more recent state privacy laws, such as the California Consumer Protection Act (CCPA), Colorado Privacy Act (CPA), the Virginia Consumer Data Protection Act (VCDPA), should be incorporated into the model law. A model bill that is consistent with existing data privacy laws promotes compliance and provides consistency among consumer privacy rights across geography and industry. Additionally, alignment with current state privacy laws creates consistencies across definitions, expectations for use of data for transactional and marketing purposes, notice requirements, third-party oversight, small business exemptions, and exemptions for publicly available data.

The small business exemptions and exemption of publicly available data are key to the title insurance industry. 90% of the title industry is comprised of small businesses, which states have exempted from compliance with data privacy laws based on recognition of the challenges and costs associated with implementation. Similar consideration under this model act would create consistency for small businesses that have less negotiating power compared to large licensees and limited resources to expend on the significant costs associated with compliance.

Additionally, state data privacy laws have universally exempted the use of publicly available data from their scope. The title insurance industry extensively uses public records maintained by government agencies, including court, tax, and land records, to facilitate real estate transactions and to insure these transactions. Without a publicly available data exemption, the model would unintendedly – and significantly – harm beneficial uses of this data. The title insurance industry's ability to maintain copies of land records within title plants would be severely hampered, jeopardizing continued operation in the many states that require ownership of complete and accurate title plants to conduct title insurance business. More broadly, any limitation of access to or use of publicly available data would negatively impact the industry's ability to issue title insurance policies, which are required by lenders in any financed real estate transaction. To mitigate these foreseeable harms, we suggest the following change to the definition of Nonpublic personal information:

Nonpublic personal information does not include publicly available information, de-identified information, aggregated data, and pseudonymous data.

Additionally, the model should define "publicly available" as other states have done in their privacy laws:

"Publicly available" means: information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media; or

information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.

Within the redline below, we provide edits and direct feedback to language within Section 6 – 8 as shown.

ARTICLE III. CONSUMER REQUESTS

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

A. Access to nonpublic personal information.

(1) Within 45 days of an authorized request from a consumer, a licensee shall disclose:

(a) Nonpublic personal information about a consumer that is requested by the consumer and maintained by the licensee or collected and maintained by the licensee from any contracted third-party service provider; that:

(i). Must include a list of all third-party service providers to whom the licensee disclosed the consumer's nonpublic personal information; and

(ii). Must be provided in a format specific to the consumer and easily readable.

(2) In response to an authorized request from a consumer in (1) above, a licensee shall not disclose:

(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, or unique biometric data. The licensee may instead disclose in generic terms that it maintains this information and list out each type of nonpublic personal information about the consumer.

B. Correction of nonpublic personal information.

(1) A consumer may request the correction of their nonpublic personal information.

(2) An authorized request from a consumer under this subsection shall identify the specific information that the consumer wishes to correct and provide explanation of why the licensee's information is incorrect.

Commented [EB9]: Will this be a defined term?

Commented [EB10]: With out this, if a licensee or insurer uses a credit bureau's services to validate the identity of the consumer, would the licensee have the obligation to disclose to the consumer all information that the credit bureau has? CCPA's right to know is limited to information "collected and maintain[ed]" by the business.

(3) *After receiving an authorized request under this subsection, a licensee shall, within ~~30~~ 45 days of receipt of the request, notify the consumer of:*

(a) *Correction of the information as requested by the consumer or deletion of the information in dispute; or*

(b) *Denial of the correction, the basis for refusal to correct the information as requested, and*
the consumer's ability to submit an appeal.

The time period to provide the required information, to correct inaccurate personal information, or to delete personal information may be extended once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.

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

(a) *The licensee believes the existing information is correct from clear documentation in its possession; or*

(b) *The licensee received the information from a third-party, such as a healthcare provider, who has the responsibility or authority for determining the accuracy of the information.*

(c) *The Licensee determines that the contested personal information is more likely than not accurate based on the totality of the circumstances. (1) Considering the totality of the circumstances includes, but is not limited to, considering: (A) The nature of the personal information (e.g., whether it is objective, subjective, unstructured, sensitive, etc.). (B) How the business obtained the contested information. (C) Documentation relating to the accuracy of the information whether provided by the consumer, the business, or another source. Requirements regarding documentation are set forth in subsection (d).*

C. *Deletion of nonpublic personal information.*

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

(2) *The licensee shall not be required to delete nonpublic personal information if:*

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

(b) *The information may be necessary:*

Commented [EB11]: This should be consistent with other privacy laws, which allow 45 days and an extra 45 days if necessary

Commented [EB12]: A concept from CCPA

Commented [EB13]: Edit the list to include CCPA relevant items (below)

Commented [EB14R13]: (d) A business, or a service provider or contractor acting pursuant to its contract with the business, another service provider, or another contractor, shall not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the business, service provider, or contractor to maintain the consumer's personal information in order to:
(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated by the consumer within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.
(2) Help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes.
(3) Debug to identify and repair errors that impair existing intended functionality.
(4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.
(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.
(6) Engage in public or peer-reviewed scientific, historical, or statistical research that conforms or adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the ability to complete such research, if the consumer has provided informed consent.
(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business and compatible with the context in which the consumer provided the information.
(8) Comply with a legal obligation.

(i). To perform the contract or service request or benefiting the consumer; or

(ii). To comply with legal obligation.

(c) 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 30 days, to delete with respect to information stored on an achieved or backup system until the archived or backup system is deleted. A licensee must notify the consumer of such delay.~~

D. Request Procedures

(1) Guidelines for responding to authorized requests except as otherwise provided in this Act, a licensee shall respond to requests submitted under this section in the following manner:

(a) A licensee shall respond to an authorized request received from a consumer under this section, unless fulfilling the request proves impossible due to the specific nonpublic personal information is not locatable or retrievable by the licensee.

(b) If a licensee if unable to verify a request, the licensee shall not be required to consider the request and may request that the consumer provide additional information necessary to authenticate the consumer and the consumer's request.

(c) If a licensee declines or is exempt from ~~to~~ taking action regarding the consumer's request, the licensee shall inform the consumer of the basis for declining to take action and any relevant instructions for how to appeal the decision pursuant to subparagraph (B)(3)(b) of this section.

(2) A consumer may make up to two requests per subsection in a 12-month period.

(3) A child's parent or legal guardian may submit a request under this section on behalf of the child regarding processing nonpublic personal information belonging to the child.

Section 7. Sale of Nonpublic Personal Information

A. A licensee shall not sell a consumer's nonpublic personal information that the licensee has obtained from a consumer, including for purposes of targeted advertising, unless the consumer has affirmatively opted in to the sale of their nonpublic personal information after receiving clear and conspicuous notice.

Commented [EB15]: CCPA specifically excludes backups from the deletion requirements. It might be impossible to identify information in bulk archived records to delete.

Commented [EB16]: Need to fill in the relevant section(s)

Commented [EB17]: Do we need to include legal representative for adults who can't represent themselves?

Commented [EB18]: This term needs to be defined. Consider CCPA.

Commented [EB19R18]: (1) "Sell," "selling," "sale," or "sold,'' means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.

B. *Before a consumer opts in to the sale of nonpublic personal information, a licensee shall provide a clear and conspicuous notice to the consumer, which includes:*

(a) *A description of the categories of nonpublic personal information that the licensee intends to sell;*

(b) *The purpose(s) for which the nonpublic personal information will be sold; and*

(c) *The consumer's right to opt out of the sale of nonpublic personal information.*

C. *Affirmative Consent: the consumer's affirmative opt-in consent must be obtained separately from any other consent obtained from the consumer.*

Commented [EB20]: Please clarify: Does this need to be obtained on a separate document, or at a separate time?

Section 8. Use and Disclosure of Sensitive Personal Information

A. *Licensees may utilize sensitive personal information for certain identified purposes and uses, including those purposes and uses identified in Article VI (Exceptions to Limits on Disclosures of Financial Information);*

B. *A consumer shall have the right, at any time, to direct a licensee that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to the authorized purposes and uses;*

C. *A licensee that discloses or processes a consumer's sensitive personal information for purposes other than those specified in subsection A of this section shall provide a clear and conspicuous notice to the consumer, which includes:*

(a) *A description of the sensitive personal information that the licensee intends to disclose;*

(b) *The purpose for which the sensitive personal information will be processed; and*

(c) *The consumer's right to opt out of the processing of sensitive personal information for those purpose(s).*

Commented [EB21]: Transaction based use should be expressly exempt.

C. A consumer's affirmative opt-in consent must be obtained separately from any other consent obtained from the consumer.

Blue Cross Blue Sheild Association

Effective privacy protections are foundational to the work of BCBS companies. To support Plan efforts and the aims of this Working Group, we recommend continued focus on solutions that protect patient information while also preventing undue complexity in requirements. This helps ensure companies can implement consistent, robust practices. Navigating separate and distinct requirements across types of data, lines of business and markets can diffuse resources and reduce the effectiveness of the protections for the members we serve. With this in mind, we offer the following recommendations:

- **Align Section 6A and Section 6(D) to the Health Insurance Portability and Accountability Act (HIPAA) by exempting HIPAA covered entities from the requirements.** Section 6A, as drafted, requires an accounting of disclosures broader than the HIPAA disclosure accounting requirement. Disclosures for health care operations, among other purposes, are exempt from an accounting of disclosure under HIPAA. To align with this existing standard, we recommend exempting HIPAA-covered entities from these requirements. This would promote consistency and avoid a potential conflict with Section 25 of the model regulation which exempts HIPAA-covered entities, staging that a HIPAA covered entity that "maintains nonpublic personal information in the same manner as protected health information, shall be deemed to comply with the requirements of this Act." Similarly, we recommend revising Section 6(D) to be consistent with the access requirements in the HIPAA Privacy Rule by exempting HIPAA-covered entities.
- **If retained, clarify the language in Section 6A(ii) regarding how nonpublic personal information should be shared with the consumer requesting such information to state that it "must be provided in paper or electronic form, as requested by the consumer".** Section 6A(ii) notes that nonpublic personal information about a consumer that is requested by the consumer and maintained by the licensee or any contracted third-party service provider, "must be provided in a format specific to the consumer and easily readable". To clarify expectations of? the normal mechanisms for the sharing of information, we recommend the model regulation language instead state that the information "must be provided in paper or electronic form, as requested by the consumer." This language should provide consistency in expectations between the licensee or any contracted third-party service provider and the patient, preventing confusion or unnecessary complexity.
- **Clarify Section 7(C) and 8(C) regarding patient consent that "separately" can be defined as a separate document with its own signature.** The current language is ambiguous and could lead to overinterpretation on what constitutes "separately." While we appreciate the need for ensuring the consumer understands they are consenting to the release of their information, this should be balanced with encouraging the responsible sharing of information. Consent should be obtained in a manner that is clear to the consumer and would not be easily selected or confused with other consent requests but should not necessitate a wholly separate interaction which would impose burden on the consumer and might inhibit the sharing of information which the consumer would have otherwise supported.

ByAllAccounts Data Aggregation Strategy & Governance

Section 8 specifically, and the model regulation in general, does not address the data portability consideration of privacy sufficiently within accepted principles. In particular, the right of the data subject to direct the data controller to share their data with a third-party. This proscriptive approach harms consumers seeking to obtain positive financial outcomes via competent independent financial advice. Is this an issue with which the Working Group is will to engage as part of this model regulation?

Committee of Annuity Insurers

OVERVIEW

The CAI recognizes and appreciates the Working Group's ongoing efforts to enhance privacy protections for consumers through a revised version of Model 672, an established and time-tested framework. While there remains a range of important and complex issues to work through in the Chair's Draft, we are confident that the current process will ultimately yield a revised privacy model law that significantly enhances consumer privacy protections while being workable and pragmatic for licensees.

As requested, our comments below focus on issues raised by Article III of the Chair's Draft. However, there are also related issues raised by Article III that necessarily impact other sections of the Chair's Draft, such as the definitions section. Accordingly, we are also commenting on other sections of the Chair's Draft to the extent relevant to issues raised by Article III. As the Working Group proceeds through the comment and drafting process, we urge the Working Group to keep an eye toward ensuring the revised draft ultimately works as a whole.

Overall Article III introduces concepts from other recent state comprehensive privacy laws that are familiar, but we respectfully submit that Article III will greatly benefit from additional work to clarify its policy goals and the intended meaning of several core concepts. This lack of clarity necessarily affects the nature and extent of the comments we can proffer at this juncture, since we cannot fully comment on proposals that are not yet clear in their intended meaning or purpose. For example and as discussed further below, Section 7 of the Chair's Draft proposes to limit the "sale" of Nonpublic Personal Information ("NPI"), but it does not define what the "sale" of NPI means. Some existing privacy frameworks, like the California Consumer Privacy Act ("CCPA"), define the term "sale" much more broadly than any plain English understanding of the term, while others are more aligned with the plain meaning of the term. Whether the terms of proposed Section 7 are appropriate or untenable will entirely depend on this definition. Currently, there is no indication in the Chair's Draft what a "sale" is intended to cover, making it difficult for the CAI to provide thorough feedback to the Working Group without engaging in assumption and supposition. The same dynamic applies to several other areas of newly proposed Article III. Accordingly, our comments highlight where additional clarity is needed, and provide feedback based on our current understanding of the intent of the Chair's Draft where possible. However, further opportunity for comment on these sections will be needed once the proposed provisions as identified below are clarified.

COMMENTS

Section 6 – Access, Correction, and Deletion of Nonpublic Information

1. **Requirements to "Verify" and "Authorize" consumer requests need to be clarified and defined.**

Section 6 of the Chair's Draft requires that licensees respond to "authorized" requests. However, there is no definition or indication as to what constitutes such an "authorized" request. Subsection 6.D also anticipates that in some instances a licensee will not be able to "verify" a request, but it is not clear what the standard of verification is or if a "verified" request and an "authorized" request are intended to refer to the same kind of request authentication process. This important concept should be clarified to set a clear expectation and meaning for licensees. Accordingly, the language of "authorize vs verify" should be made consistent and defined.

Section 6 should be revised to use the term "authenticate" to refer to the process of verifying the legitimacy of consumer rights requests received by licensees. "Authentication" should be defined to require verification of an individual's identity through reasonable means. This approach would be consistent with the approach taken in a majority of states that have recently adopted comprehensive privacy laws and provides a flexible and workable standard without being overly prescriptive.

CAI Recommendation. Section 6 should be revised to use the term "authenticate" to refer to the process of verifying the legitimacy of received consumer rights requests. The term "authenticate" should be defined in Section 4 as follows:

"Authenticate" means to verify through reasonable means that the consumer who is entitled to exercise the consumer's rights under Section 6 is the same consumer exercising those consumer rights with respect to the nonpublic personal information at issue.

2. **Licensees should not be required to provide consumers with a list of all third-party service providers to which information has been disclosed.**

As currently drafted, proposed Subsection 6.A.(1)(a)(i) would require licensees to include "a list of all third-party service providers to which the licensee disclosed the consumer's nonpublic personal information". If enacted, this obligation would be burdensome, complex, and serve little apparent consumer protection purpose. From a practical perspective, it would 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. Therefore, to determine if a particular consumer's data was sent to that vendor, the licensee would need 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 data about a particular consumer. For all this complexity and challenge, 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 or counterparty 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. Additionally, as drafted, 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. Accordingly, this requirement would be extremely burdensome and costly for licensees to comply with, while providing little apparent benefit to consumers.

Additionally, if the goal of this requirement is to provide greater transparency to consumers about how a licensee may use and disclose their NPI to enable informed consumer choice in selecting an insurer, disclosing this information in response to an access request would be too late. Rather, transparent disclosures in the initial privacy notice would be a better fit. Because any such disclosure would be forward looking, it similarly would not be possible for licensees to identify exactly which service providers would receive a particular consumer's NPI. Rather, licensees could describe the types of third party service providers NPI is generally shared with, which would provide consumers with a plain language and understandable indication of how their NPI may be disclosed to service providers.

CAI Recommendation. Proposed Section 6.A.(1)(a)(i) should be deleted. If the disclosure requirement is retained, it should be limited to disclosure in the initial privacy notice of the general types of third-party service providers with whom the licensee generally shares NPI.

3. Licensees should be required only to provide NPI in a reasonably accessible format when responding to access requests.

As currently drafted, Section 6.A.(1)(a)(ii) states that a licensee must provide responses to access requests in a "format specific to the consumer". It is unclear what this language is intended to require. It could be read to mean that the licensee must provide the NPI in whatever format the requesting consumer may specify. If so, this would be a burdensome and unnecessary obligation. There are innumerable potential mechanisms and formats through which a consumer could request their NPI, including hard copy, placing an onerous burden on licensees to cater to the varied requests of consumers. We are aware of no other privacy regime that places this requirement on regulated entities. Rather, this provision should be amended to take an approach consistent with most state comprehensive privacy laws, which only require that a copy of digital data be provided in a readily usable format.

CAI Recommendation. Existing Subsection 6.A.(1)(a)(ii) should be deleted and replaced with a requirement that NPI data only need be provided in a readily usable format, as follows:

(ii) If the nonpublic personal information is available in a digital format, it must be provided in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another party without hindrance.

4. Exemptions to 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. For example, it is not currently clear that NPI could be retained to protect the physical safety of an individual, protect against security incidents, or engage in peer-reviewed research. 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 research, safety, security, and anti-fraud efforts. Additionally, other provisions of the Chair's Draft beyond the right to delete could similarly prevent licensees from performing these important functions if appropriate exemptions are not specified, including Sections 7 and 8. Accordingly, a broader list of exemptions should be added to Article VI of the Chair's Draft to broadly protect appropriate and necessary uses of NPI under a revised Model 672. This approach, and the below proposed language, would again be consistent with the approach and language adopted by most states that have adopted comprehensive privacy laws.

CAI Recommendation. Section 6.C.(2) should be deleted and a new section should be added to Article VI as follows:

Section [X]. Other Limitations and Exceptions

A. This Act may not be construed to restrict a licensee's ability to:
(1) comply with federal, state, or local laws, rules, or regulations;
(2) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other governmental authorities;
(3) investigate, establish, exercise, prepare for, or defend legal claims;
(4) provide a product or service or process a transaction specifically requested by a consumer, perform a contract to which the consumer is a party, or take steps at the request of the consumer before entering into a contract;
(5) take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual;
(6) prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity;
(7) preserve the integrity or security of systems to investigate, report, or prosecute those responsible for breaches of system security;
(8) engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or similar independent oversight entity that determines:
(a) if the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the licensee;
(b) whether the expected benefits of the research outweigh the privacy risks; and
(c) if the licensee has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification; or
(9) assist another licensee or other third party with any of the requirements under this subsection.

B. This Act may not be construed to prevent a licensee from providing Nonpublic Personal Information concerning a consumer to a person covered by an evidentiary privilege under the laws of this state as part of a privileged communication.

C. This Act may not be construed as imposing a requirement on licensees that adversely affects the rights or freedoms of any person, including the right of free speech.

D. This Act may not be construed as requiring a licensee, third party, or consumer to disclose a trade secret.

E. The requirements imposed on licensees under this Act may not restrict a licensee's ability to collect, use, or retain data to:
(1) conduct internal research to develop, improve, or repair products, services, or technology;
(2) identify and repair technical errors that impair existing or intended functionality; or
(3) perform internal operations that:
(a) are reasonably aligned with the expectations of the consumer;
(b) are reasonably anticipated based on the consumer's existing relationship with the licensee; or
(c) are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

F. A requirement imposed on a licensee under this Act does not apply if compliance with the requirement by the licensee would violate an evidentiary privilege under the laws of this state.

5. Data should not have to be deleted from backup systems until the data is next accessed in the ordinary course

Subsection 6.C.(3) also allows deletion to be delayed by up to 30 days where the data is stored on archived or backup systems. However, some backup and archive systems (e.g. tape archives) are rarely accessed. So, mandating deletion within 60 days would in practice 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. Instead, Subsection 6.C.(3) should allow licensees to delete data from backup or archive systems within 60 days or whenever the system is next accessed in the ordinary course, whichever is longer. Doing so would still protect consumers whose data is not deleted within the 60 days, 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 the operational burden placed on licensees and would be consistent with the approach taken by other privacy laws, including the CCPA.

Additionally, in some circumstances systems may not be able to be deleted because of the nature of the system (e.g. WORM compliant systems established to comply with SEC regulations). Accordingly, an exemption should also be made where deletion is not technically feasible.

CAI Recommendations. Subsection 6.C.(3) should be revised as follows:

(3) A licensee may delay fulfilling a consumer's request ~~up to 30 days,~~ to delete with respect to information stored on an achieved or backup system by up to 30 days or until the archived or backup system~~s~~ is ~~deleted~~ next accessed, whichever is greater. A licensee must notify the consumer of such delay.

Additionally, Subsection 6.C.(1) should be revised as follows to allow for when deletion may not be technically feasible:

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

6. Licensees should be exempted from honoring requests where doing so would involve disproportionate effort.

Similarly, Subsection 6.D.(1)(a) also includes an exemption that excuses licensees from responding to authorized consumer requests where "fulfilling the request proves impossible due to the specific nonpublic personal information is not locatable or retrievable by the licensee." We appreciate and support 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. However, "impossible" sets a very high standard to qualify for this exception, which would be difficult to implement and assess in practice. For example, if honoring a consumer request would likely require hundreds of hours of manually reviewing hardcopy documents, would that be "impossible" to honor or merely extremely difficult? As drafted, the standard would require licensees to expend every resource to honor a request until it can determine that honoring the request is fully impossible. This "impossible" standard would also be beyond the approach taken by other modern privacy frameworks. For example, the CCPA allows businesses to decline to honor consumer requests where doing so would "be impossible or 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.

CAI Recommendation. Subsection 6.D.(1)(a) should be revised as follows:

(a) A licensee shall respond to an authorized request received from a consumer under this section, unless fulfilling the request ~~proves~~ would be impossible or would involve disproportionate effort. ~~due to the specific nonpublic personal information is not locatable or retrievable by the licensee.~~

Section 7 – Limit on Sale of NPI

1. The definition of a "sale" of NPI must be defined.

Currently, the Chair's Draft does not define what constitutes the "sale" or "selling" of NPI. Accordingly, we do not know what the intended scope of application of the limits of Section 7 would be under the Chair's Draft. Therefore, we cannot identify what issues and additional considerations may be raised by the proposed language since any such issues are necessarily dependent on the definition of a "sale" of NPI. Other existing modern privacy frameworks have diverged on the scope of what constitutes the "sale" of personal information, and so there is not a single common understanding of the term's meaning. Some frameworks, such as the CCPA, define the term extremely broadly such that almost any disclosure of NPI

to a third party could constitute a ”sale” of information. Others, like the comprehensive privacy laws adopted in Virginia and other states, define the term more narrowly as disclosing personal data for monetary consideration. Necessarily, the broader the term “sale” is defined, the more potential interpretative issues will arise. Accordingly, the term "sale" should be defined in the Chair’s Draft to reflect the more common, and widely adopted, definition of a “sale” as the disclosure of NPI for monetary consideration.

Please note that depending on how the Working Group proposed to define a “sale” of NPI, there may be considerable additional issues and concerns that arise with respect to Section 7.

CAI Recommendation. A “sale” of NPI should be defined in Section 4 as follows:

“Sale” or “selling” of nonpublic personal information means the exchange of nonpublic personal information for monetary consideration by the licensee to a non-affiliated third party. “Sale” or “selling” nonpublic personal information does not include:

(1) The disclosure of nonpublic personal information to a service provider that processes the nonpublic personal information on behalf of the licensee;

(2) The disclosure of nonpublic personal information to a third party for purposes of providing a product or service requested by the consumer or as otherwise permitted under Article VI of this Act;

(3) The disclosure or transfer of nonpublic personal information to an affiliate of the licensee;

(4) The disclosure of information that the consumer (i) intentionally made available to the general public via a channel of mass media and (ii) did not restrict to a specific audience; or

(5) The disclosure or transfer of personal data to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the licensee’s assets.

2. Section 7 must be revised to clarify whether it is an opt-in or an opt-out requirement.

As currently drafted, Section 7 refers to both the requirement to obtain affirmative “opt-in” consent from a consumer prior to selling their NPI, as well as referencing the “right to opt out of the sale of nonpublic personal information” in Subsection 7.B.(d). Accordingly, it is currently unclear whether the limitation on selling NPI under Section 7 is intended to be an opt-in requirement, or to be an opt-out right. Section 7 must be amended to clearly indicate whether this section requires affirmative opt- in consent or is providing an opt-out right. We firmly believe that an opt-out approach provides the appropriate balance between empowering consumers to have control over their NPI and the need for licensees to make informed decisions in specific circumstances regarding how to best leverage consumer data to better and more efficiently serve their customers. Indeed, the opt-out approach is the most widely adopted approach to placing limits on the sale of personal information, including under the CCPA and other adopted state comprehensive privacy laws. It has also served the insurance industry well to date under the time tested opt-out requirement already included in Model 672. The Working Group should not deviate from that broad consensus just for the insurance industry when there is no clear reason or need for doing so.

CAI Recommendation. Section 7 should be revised as follows:

> *A. A licensee shall not sell a consumer's nonpublic personal information unless the licensee has provided the consumer with notice and a reasonable opportunity to opt-out consistent with Section 16 of this Act. ~~, including for purposes of targeted advertising, that the licensee has obtained from a consumer, unless the consumer has affirmatively opted in to the sale of their nonpublic personal information after receiving clear and conspicuous notice.~~*
>
> *B. ~~Before a consumer opts in to the sale of nonpublic personal information, a licensee shall provide a clear and conspicuous notice to the consumer, which includes:~~*
> *~~(a) A description of the categories of nonpublic personal information that the licensee intends to sell;~~*
> *~~(b) The purpose for which the nonpublic personal information will be sold; and~~*
> *~~(c) The consumer's right to opt out of the sale of nonpublic personal information.~~*
>
> *C. ~~Affirmative Consent: the consumer's affirmative opt-in consent must be obtained separately from any other consent obtained from the consumer.~~*

Section 8 – Limit on Use and Disclosure of Sensitive Personal Information ("SPI")

1. Section 8 should be revised to clarify the core concepts of the proposal, including whether it is opt-in or opt-out, its scope, and its notice requirement.

As currently drafted, Section 8 is unclear in a number of its core concepts, including whether it is opt-in requirement or opt-out right, its scope of application, and how and when the notice requirement applies. With so much uncertainty as to the intended effect of the proposed language, we are unable to provide detailed feedback on the proposal or provide specific suggested language at this juncture. Accordingly, we have focused our comments on identifying those areas in need of clarification.

Like Section 7 above, Section 8 is inconsistent as to whether it is intended to be an opt-in requirement or an opt-out right. Much of the section seems focused on providing an opt-out right, but Subsection 8.C. specifically references "A consumer's affirmative opt-in consent." Section 8 must be clarified to specify which approach is intended. As discussed above with respect to Section 7, we believe an opt-out approach best balances the interests of consumers and of licensees and would be consistent with the approach adopted in most recently adopted state privacy frameworks.

Additionally, Section 8 is not currently clear on the intended scope of the consumer's right to limit the use and disclosure of SPI. While it references the right of a consumer to limit the use of SPI to "certain identified purposes and uses", those purposes and uses are not clearly defined. They are stated to "include" those purposes and uses identified in Article VI, but there is no definition regarding what other purposes or uses may be permissible. Additionally, Article VI specifically addresses the purposes and uses for which NPI may be disclosed to nonaffiliated third parties, which could be read to mean the right to limit the use and disclosure of SPI specifically applies only when SPI is disclosed to third parties. The intended scope of the right to limit the uses and disclosure of SPI should be clarified so that all stakeholders may provide appropriate feedback.

Finally, the notice requirement referenced in Section 8 is unclear. Section 8 states that licensees that disclose or process SPI for purposes other than those "certain identified purposes and uses" are required to provide a notice to the consumer, but it does not indicate when or how such notice is required to be made. The intended nature and timing of this notice needs to be clarified. We suggest that this notice could be incorporated into the initial notice requirements set forth in Section 9, which would take advantage of the established notice timing and delivery requirements already established in Model 672. This approach would also be consistent with the approach taken by other states in recently adopted state privacy laws, including the CCPA.

CAI Recommendation. Section 8 should be revised both to clarify the intended nature (opt-in vs. opt-out) and scope of the proposed right to limit the use and disclosure of SPI, and to clarify the associated notice requirement.

Insured Retirement Institute (IRI)

1) **Section 6(A)(1):** We request that the Working Group consider the following recommendations:
    a. Increase the timeline to disclose to allow for adequate time to gather the needed information to respond to the request.
    b. Adjust 6(A)(1)(a) as follows: "Nonpublic personal information about a consumer that is requested by the consumer and maintained by the licensee or any contracted third-party service provider on behalf of the licensee; that…".
    c. Align 6(A)(1)(a)(i) with other notification requirements that allow for "categories" of third parties to be identified. Our members have significant concerns with a requirement to disclose a list of all specific third parties that have consumer nonpublic personal information for security and competition reasons. We strongly recommend that the rule allow for disclosure of *categories* of third parties.
    d. Remove the requirement in 6(A)(1)(a)(ii) that the disclosure must be in a format "specific to the consumer." It is unclear what this means and would be impractical from a compliance standpoint to implement.
2) **Section 6(B)(3):** Increase the time to notify a consumer of corrections or denial of corrections to allow for adequate time to address a request.
3) **Section 6(C):** 45 days is likely too short of a timeframe to delete nonpublic personal information about a consumer, due to the variety of different systems that some insurers may have. Also, when it comes to archived or backup systems, even an additional 30 days on top of the original 45, is likely not enough time due to the challenges with deleting physical backup tapes. We strongly recommend that the Working Group reconsider these timeframes to make this section workable, to standardize with other privacy laws, and to allow insurers for adequate time to complete these requests. It may also be appropriate to provide an exception to deletion requirements for archived media that is not reasonably accessible.
4) **Section 6(D)(1)(a):** Adjust this provision as follows: "A licensee shall respond to an authorized request received from a consumer under this section, unless fulfilling the request proves impossible due to the specific nonpublic personal information is not locatable or retrievable by the licensee without disproportionate effort."

5) Section 7:

a. Our members strongly support an "opt-out" approach, which is the current standard in the industry (and is also the standard in the existing Model #672). An "opt-in" approach, as the current draft contemplates, deviates significantly from U.S. privacy laws and would place insurers in a different position than other GLBA-regulated entities, such as banks. We strongly urge the Working Group to adjust the language in the section to align with an "opt-out" approach.

b. While our members support an "opt-out" approach for selling and for targeted advertising, there should be clarity between the two terms. We suggest that this Section add "or use[d] for targeted advertising" whenever a sale of nonpublic personal information is referenced, so that it is clear the section applies to both uses.

c. In addition to changing this section to an "opt-out" approach, we recommend that an additional subsection be added to Section D to clarify what constitutes an exception to selling nonpublic

personal information and that there not be instances where a consumer may not opt out, and we'd suggest language along the lines of the following:

D. A licensee does not sell nonpublic personal information when:
(a) A consumer uses or directs the business to intentionally:
(i) Disclose personal information.
(ii) Interact with one or more third parties.
(b) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information for the purposes of alerting persons that the consumer has opted out of the sale of the consumer's personal information or limited the use of the consumer's sensitive personal information.
(c) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with this title. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer.

6) **Section 8:** Our members have significant concerns about the workability of this section. It does not appear to align with the other provisions of Model #672, which have exceptions to opt-out requirements. There are situations where it is not feasible operationally to allow customers to opt out of sharing when it would inhibit an insurer's ability to conduct business. We recommend that this section be removed or revamped to
better align with existing privacy regimes.

NAMIC

On behalf of the National Association of Mutual Insurance Companies (NAMIC) members, thank you for the opportunity to provide these comments on the exposure draft dated August 5, 2024 (draft). Consistent with the direction of the Working Group, this input focuses on the aspects of the draft relating to Article III of the exposure draft (and given the accelerated timeframe, they are in bullet form).

NAMIC members very much appreciate the efforts of the Privacy Protections (H) Working Group (PPWG or Working Group) and the ability to provide input. This part of broader feedback, and we look forward to continuing to share members' concerns and suggestions as the process continues.

Before getting to more substantive remarks, there are some preliminary considerations.

First, with respect to **definitions**, while we understand that there is an interest in taking the effort one section at a time, it is extremely difficult to remark on the provisions without knowing what they actually mean and including them as a part of the corresponding conversation. Many of the definitions are seriously problematic and impact the substantive provisions negatively. To some extent, these comments assume that the definitions are going to be addressed to find reasonable solutions.

Second, these comments do not reflect full vetting and we ask for an opportunity to amend them going forward through the process. While we understand the preference for an abbreviated **timeframe**, this the compressed timeframe is a new approach (contrary to previous representations of the expected process and of limiting review to the specified sections), and with the fewer days overlapping with the Fall National Meeting the time available for response efforts are even more compressed. Because of this, the suggestions offered here may be more tentative in nature and we ask for the ability to revise them as additional insights and input are offered by members. Respectfully, the red-lines shared here should be understood as being a quick effort but they should not be considered to be a full and comprehensive indication of all concerns and suggestions. We look forward to continuing to share input as this process continues.

ACCESS REQUESTS & DISCLOSURES
Draft Article III: Section 6A

Timeframe
§6A(1)

To address the more detailed nature of the requests process, please consider the notes below.

PLACEMENT: The basic number of days to respond to an authorized [verifiable] consumer request is better contained within subsection (D) of this Section 6 dealing with Request Procedures. Please also see the corresponding suggestions for correction and deletion provisions.

ADDITIONAL NUANCES: By placing the number of days (45 days as the general rule) in the Request Procedures, there is space and a structure to expand on some of the necessary logistics for unusual situations. For example, there may be times that an insurer will need additional time to authenticate the identity of a consumer.

COUNTING DAYS: Consider inserting "business" before days throughout.

TRIGGER & AUTHENTICATION/VERIFICATION: As a practical matter, the time period should not begin to run until the licensee is able to verify the identity of the consumer (otherwise there may be a situation where the consumer does not provide the necessary information to verify the identity until day 44, leaving the licensee with only one day to fulfill the request). This should be clear through definitions (whether of an "authorized request" or a "verifiable request" [or Virginia uses "authenticate"] (and then using the corresponding working throughout)) or included in the substantive provisions. Again, as a technical item, it may be that referencing subsection 6D's request procedures could be a way to efficiently address the mechanics governing requests.

Technical working suggestion to cross reference applicable timing/procedures:

(1) ~~Within 45~~ ~~business~~ ~~days~~ ~~of~~ A~~n~~ ~~authorized~~ verifiable consumer request ~~from a consumer~~, a licensee shall follow request procedures in accordance with Subsection D of this section and disclose:

If it is decided not to reference Subsection D, we would then urge that the issues suggested to be resolved there be handled in this subsection.

ACCESS REQUESTS & DISCLOSURES
Draft Article III: Section 6A

TPSP Info to Consumers – Content
§6A(1)(a)(i)

Requiring categories of TPSPs rather than a list enumerating all of them would be a better approach, for reasons including those sketched briefly below.

OVERWHELMING: A list of all a licensee's TPSPs could be extensive and not meaningful to a consumer. Indeed, it may invite confusion about a complex industry.

OUTDATED: The TPSPs that are used may be changing and the request response is at a point in time. For information provided to remain accurate (evergreen), categories should be used instead.

NOT GOING BEYOND CCPA OR GDPR: Categories are the norm for those jurisdictions that have this requirement today.

SECURITY THREATS: 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/systems or for scanning multiple licensees' approaches to create a cyber roadmap for exploiting a vulnerability by targeting critical service providers (potentially causing occurrences similar to the Crowdstrike outage).

PROPRIETARY & TRADE SECRET INFORMATION – POTENTIAL COMPETITION IMPACTS: Through accessing an extensive list of vendors, competitors may be able to see what specific tasks are handled in-house and which are outsourced. They may also be able to piece together aspects of others' strategic approaches and partnerships. This does not benefit the marketplace.

CONTRACT NEGOTIATION & POTENTIAL PRICING IMPACTS: If a vendor accesses the list of vendors, they might learn a licensee's dependencies and use this information as leverage in contract negotiations (possibly including by increasing fees).

BURDENSOME & COSTLY LEVEL OF DETAIL: Providing this list could be burdensome as sharing may vary and it would take time and resources to research the PII of an individual. Not only would it be impractical, but it may be contrary to public policy such as where specific third parties have been engaged for investigations relating to a particular consumer, etc.

UNBOUNDED: There should be some clear indication of the reasonable time period to which the obligation would apply, such as going back a year (as done in California).

INTERNAL CONSISTENCY: The general privacy notice information in Sec. 11 of the Chair's draft refers to "categories."

Working suggested revision to address challenges with TPSP-related disclosure:

Must include the categories of ~~a list of all~~ third-party service providers to ~~in~~ which the licensee disclosed the consumer's nonpublic personal information in the preceding 12 months;

ACCESS REQUESTS & DISCLOSURES
Draft Article III: Section 6A

TPSP Info to Consumers - Format
§6A(1)(a)(ii)

The format-related provisions should be modified for reasons including those sketched briefly below.

INTERPRETATION: Aid Compliance & Avoid Confusion: What does "format specific to the consumer" mean? What will easily readable mean? There needs to be clarity and additional detail, if this requirement is to remain.

STATE EXAMPLE: The lead-in phrase used in CCPA 1798.130 is "in a form that is readily accessible."

PAPER NOT DEFAULT METHOD: There needs to be modernization here (with potential for paper upon request (and this has possible efficiency and environmental benefits as well) with a default as providing the information electronically. Further, depending on what kinds of information is required electronic may better allow for authenticating requests.

Working suggested revision to address workability of TPSP-related disclosure format:

Must be provided in a format that is ~~specific to the consumer and~~ easily readable to a reasonable consumer and in a form that is readily accessible.

ACCESS REQUESTS & DISCLOSURES
Draft Article III: Section 6A

TPSP Info to Consumers – Content Avoid Disclosing (High Risk Info)
§6A(2)(a)

The provision relating to information not to be disclosed should be expanded for reasons including those sketched briefly below.

CONSISTENCY: Some other laws also include an exception to allow for avoiding disclosure of information that could create a high risk of identity theft.

CONSUMER PROTECTION: It may be that there could be other information (now or over time) that may put the consumer at risk, such as a risk of identity theft. The model could account for this potentiality.

Working suggested revision to address workability of TPSP-related disclosure format:

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, or unique biometric data. Upon a determination that other information could create a high risk of identity theft, a licensee need not disclose such information.

ACCESS REQUESTS & DISCLOSURES
Draft Article III: Section 6A

Exceptions - Omitted
§6A

REVIEW NEEDED – REFERENCE EXCEPTIONS: As an overall matter, careful review should be done of what exceptions under what is now Article IV under the Chair's Draft (8/5/24) should be permitted for the provisions that will be added. For example, it may be that what the draft reflects as Sec. 21A should be expanded and referenced within the new access-related subsection. Those exceptions refer to things like fraud prevention, protecting confidentiality/security, risk control, and resolving disputes. As we continue to review, there may be other exceptions to consider as well.

Working suggested revision to reference exceptions:

(3) Notwithstanding any other provision, the requirements under subsection A of this section do not apply when a licensee shares or receives nonpublic personal information about a consumer pursuant to an exception described in Section 21(A).

CORRECTION REQUESTS
Draft Article III: Section 6B

Scope
§6B(1)(a)

MATERIAL IMPACT: The corrections should relate only to items that will be material.

PURPOSE OF CORRECTION MECHANISM: This mechanism may not be the best avenue for updating basic information and should not be used for usual administrative updates, etc.

Working suggested revision to address scope of correction requests:

A consumer may request the correction of their nonpublic personal information that is material to the processing of a claim or the binding of a policy.

CORRECTION REQUESTS
Draft Article III: Section 6B

Timeframe
§6B(3)

To address the timeline and the more detailed nature of the process around the requests, please consider the notes below.

NUMBER OF DAYS & INTERNAL CONSISTENCY: The time provided should be 45 days rather than 30.

CONSISTENCY WITH OTHER STATE LAWS: Generally speaking, the timeframe of 45 days seems for consistent with what is seen in other consumer privacy laws, such as what we understand is in some of the state comprehensive laws (California, Colorado, Virginia, etc.). Again, the consistency may be useful with consumer expectations.

TRIGGER & AUTHENTICATION/VERIFICATION: As a practical matter, the time period should not begin to run until the licensee is able to verify the identity of the consumer (otherwise there may be a situation where the consumer does not provide the necessary information to verify the identity until day 44, leaving the licensee with only one day to fulfill the request). This should be clear through definitions (whether of an "authorized request" or a "verifiable request" [or Virginia uses "authenticate"] (and then using the corresponding working throughout)) or included in the substantive provisions. Again, as a technical item, it may be that referencing subsection 6D's request procedures could be a way to efficiently address the mechanics governing requests.

EASE OF UNDERSTANDING & ADMINISTRATION: Having the same timeframe for all three kinds of newly added requests may be easier for consumers to understand (avoiding confusion) and for licensees to administer.

PLACEMENT: The basic number of days to respond to an authorized request is better contained within subsection (D) of this Section 6 dealing with Request Procedures. Please also see the corresponding suggestions for access and deletion provisions.

ADDITIONAL NUANCES: By placing the number of days in the Request Procedures, there is space and a structure to expand on some of the necessary logistics for unusual situations. For example, there may be times that an insurer will need additional time to authenticate the identity of a consumer.

Working suggested revision to timing of correction requests:

After receiving an ~~authorized~~ verifiable consumer request under this subsection, a licensee shall, within 45 ~~30~~ business days of receipt of the request, notify the consumer of: …

CORRECTION REQUESTS
Draft Article III: Section 6B

Correction Denial
§6B(4)

To ensure a more reasonable scope, kindly consider the notes below.

LITIGATION: The wording should be considered through the lens of fraud investigations, pending claims, and potential/actual litigation.

IMPACTFUL: Some suggest that the correction should only be required if material as to the specific product or service and that there should not be an obligation to correct things that have no impact.

Working suggested revision to scope of request response:

A licensee may deny a request for correction if:
(a) The licensee believes the information is correct ~~from clear documentation in its possession~~; ~~or~~
(b) The licensee received the information from a third-party, such as a healthcare provider, who has the responsibility or authority for determining the accuracy of the information.
(#) The correction would not have an impact the consumer's specific product, service, or price or would not have a material impact.

DELETION REQUESTS
Draft Article III: Section 6C

General Rule & TPSPs
§6C(1)

COMPLIANCE & PRACTICALITY: Technically, a licensee cannot delete information that is not in its control. Where there is a TPSP requirement, it should relate to a request.

STATE CONSISTENCY: The deletion section of CCPA references notifying third parties "to delete the consumer's personal information unless this proves impossible or involves disproportionate effort."

Working suggested revision to deletion requests general rule:

Within 45 business days of an ~~authorized~~ verifiable consumer request ~~from a consumer~~, a licensee shall delete the nonpublic personal information about a consumer that is maintained by the licensee and notify ~~or any~~ third-party service providers to delete that consumer personal information from their records ~~on the licensee's behalf~~.

Again, with respect to the timeframe, this subsection could reference the corresponding procedures in subsection 6D.

DELETION REQUESTS
Draft Article III: Section 6C

Exceptions to Deletion-on-Demand
§6C(2)

PERMANENCE & UNINTENDED CONSEQUENCES - COVERAGE: Once information is deleted, it's gone and will be unable to access. As noted during the Fall National Meeting, there are times such information may help consumers by providing coverage, etc.; absence of such information may mean that benefit cannot later be accessed. But these are not the only potential consequences, if valid data retention is cut too deeply, there may be other complications as well.

UNINTENDED CONSEQUENCES – REGULATORY: It is not fully clear whether the draft anticipates market conduct type purposes.

UNINTENDED CONSEQUENCES – ADMINISTRATIVE: There are also administrative reasons why the exceptions may be too narrow as drafted. For example, it is essential to be able to use information for functions like: facilitating fraud detection and prevention, accurately pricing and underwriting products and services, record retention policies; and maintaining the stability of licensee systems.

MANAGING OPERATIONAL IMPLICATIONS: As structured, this could be difficult to administer. For example, it could have implications for even basic tasks like reconciling payments.

CONSISTENCY WITH OTHER LAWS: As we understand it, other laws, such as CCPA in 11 CCR 7022(f), provide for an exception in certain instances, such as where there is an exception (including a business purpose exception) and other practical reasons. This is a very sensible approach (which should be incorporated).

ALTERNATIVES TO DELETION: There could also be alternatives to deletion, such as keeping, but de-identifying or aggregating the information so it is not personally identifiable. This would be similar to CCPA which recognizes these options as suitable alternatives to deletion. For example, Sec. 1798.145(a)(6).

DELETION SCOPE – INFORMATION FROM THE CONSUMER: The ability to request deletion focuses on information received "from" the consumer (not all information about the consumer) under CCPA.

CONTEXT OF INSURANCE: While focusing on privacy requirements, the model still should reflect and respect the context of the insurance relationships and products.

SEE EXCEPTIONS NOTE: Reasons to allow an exception in the context of deletion are broader than for access (see notes above). A simple way to provide for a placeholder around the exceptions might be something like the following:

Working suggested revision to reference exceptions for deletion on demand:

… (2)(d) An exception described in Sections 19, 20, or 21 applies.

INCORPORATING EXCEPTIONS: Rather than cross referencing the exceptions section, it may be possible to incorporate additional necessary exceptions directly into subsection 6C. This may be more difficult; preliminary notes follow:

Working suggested revision address reasonable exceptions to deletion-on-demand:

Notwithstanding subsection (1) of this section, the licensee shall not be required to delete nonpublic personal information if:

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

(#) The licensee did not collect the information from the consumer;

(b) The information may be necessary to:

- (i) ~~To p~~Perform the contract or service request ~~or~~ benefitting the consumer;~~ or~~
- (ii) ~~To c~~Comply with a legal obligation, including: federal, state, or local laws; compliance with a court order or subpoena to provide information; compliance with civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities; cooperate with law enforcement agencies concerning conduct or activity that the licensee, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law; comply with a government agency request for emergency access to a consumer's nonpublic personal information if a natural person is at risk or danger of death or serious physical injury provided that the request is both approved by a high-ranking agency officer for such emergency access and based on the agency's good faith determination that it has a lawful basis to access the information on a nonemergency basis;
- (iii) Help to ensure security and integrity to the extent the use of nonpublic personal information is reasonably necessary and proportionate for those purposes;
- (iv) Debug, identify, and repair errors that impair existing intended functionality;
- (v) Engage in public or peer-reviewed scientific, historical, or statistical research;
- (vi) Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the licensee and compatible with the context in which the consumer provided the information

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

…

DELETION REQUESTS
Draft Article III: Section 6C

Backup or Archive System Deletion - Process
§6C(3)

To address the timeline and the more detailed nature of the process around the requests, please consider the notes below.

NUMBER OF DAYS & INTERNAL CONSISTENCY: The additional time provided should be 45 days rather than 30 because it may be cumbersome to delete one individual's records from an archive.

CONSISTENCY WITH OTHER STATE LAWS: The timeframe of a 45 day extension seems for consistent with what is seen in other consumer privacy laws. For example, see Virgina (VCDPA § 59.1-577), which provides as follows:

> *A controller shall respond to the consumer without undue delay, but in all cases within 45 days of receipt of the request submitted pursuant to the methods described in subsection A. The response period may be extended once by 45 additional days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of any such extension within the initial 45-day response period, together with the reason for the extension.*

EXCEPTION: It could be that there should be an allowance to simply leave the information if the system is not expected to become live again.

Working suggested revision address reasonable handling of back-up/archive systems:

Notwithstanding subsection (1) of this section, a licensee may delay fulfilling a consumer's request ~~up to~~ 45 ~~30 days,~~ to delete with respect to information stored on an archived or backup system until (#) 45 business days after the archived or backup system is restored to production; or (#) the archived or backup system is deleted ~~the archived or backup systems is deleted~~. A licensee must notify the consumer of such delay.

REQUEST PROCEDURES
Draft Article III: Section 6D

Timeframe
§6D(1)&(1)(a)

To address the more detailed nature of the process around the requests, please see the notes below.

AVOIDS REPETITION: The number of days does not need to be referenced each time in the more substantive requirements in subsections A-C. See corresponding comments in other sections.

ADDITIONAL LOGISTICS DETAILS: Incorporating the days into this subsection could allow for more space to articulate additional details for situations in which additional time may be needed.

CONSISTENT WITH STATE LAWS: An approach that allows for an extension in limited circumstances is consistent with the state comprehensive laws as well as with California. Further, CCPA recognizing some measure of burden.

RECOGNIZE UNUSUAL BURDEN: There may be times when there may be a disproportionate effort and these situations should be accounted for in the model wording.

AUTHENTICATION/VERIFICATION: See comments above.

TECHNICAL: The lead-in language could be removed/revised to aid reading.

Working to incorporating the 45 day procedure and expanding to account for necessary delay

(1) ~~Guidelines for responding to authorized requests except as otherwise provided in this Act,~~ A licensee shall handle a ~~respond to~~ verifiable consumer request~~s~~ submitted in accordance with ~~under~~ this section in the following manner:

(a) A licensee shall respond to an ~~authorized~~ verifiable consumer request within 45 business days ~~received from a consumer under this section~~, unless fulfilling the request proves impossible due to the specific nonpublic personal information is not locatable or retrievable by the licensee without disproportionate effort.

(#) Notwithstanding the requirement in subsection (1)(a) of this section, the response period may be extended once by 45 additional days when reasonably necessary, taking into account any concerns about the identity of the consumer and the complexity and number of the consumer's requests, so long as the licensee informs the consumer of any such extension within the initial 45 day response period, together with the reason for the extension.

(#) If a licensee ~~if~~ is unable to verify a request, the licensee shall not be required to consider the request and may request that the consumer provide additional information necessary to authenticate the consumer and the consumer's request.

REQUEST PROCEDURES
Draft Article III: Section 6D

Reconciling Required Response and Declined Request
§6D(1)(c)

To address the more detailed nature of the process around the requests, please see the notes below.

FACIAL CONFLICT: As drafted, (a) would mandate a response while (c) contemplates declining to take action. It seems that this could be reconciled by a simple revision.

COMPLIANCE & CLARITY: Before finalizing the model, such items should be reconciled to avoid confusion.

CALIFORNIA EXAMPLE: It appears that the California law addresses this through a "notwithstanding" approach.

> *Working suggestion to expand with additional consistent language*
>
> (#) Notwithstanding subparagraph (D)(1)(a) of this section or a licensee's general obligation to respond to authorized requests under this Section, if a licensee declines to take action regarding the consumer's request, the licensee shall inform the consumer of the basis for declining to take action and any relevant instructions for how to appeal the decision pursuant to subparagraph (B)(3)(b) of this section.

PLACEMENT & CONFUSION: Are the requirements referenced at the end of this provision and contained in "subparagraph (B)(3)(b)" intended to apply beyond corrections requests? If so, consider whether the appeal or review process belongs in subsection 6(D) relating to request procedures.

REQUEST PROCEDURES
Draft Article III: Section 6D

Request Pertaining to Minor
§6D(3)

STATE EXAMPLE: The Virginia Consumer Data Protection Act references a "known"" parent or legal guardian in Sec. 59.1-577(A) as well as an "authenticated consumer request" consistent with the idea that the licensee does not need to turn over information about a minor if no documentation is offered to indicate the nature of the relationship between an individual and the child.

AUTHENTICATED/VERIFIABLE/AUTHORIZED: California seems to structure its provisions around a "verifiable consumer request" and Virginia seems to structure their comprehensive privacy law around an "authenticated consumer request." For consistency and understanding, consider inserting one of these words in place of "authorized" (and then potentially defining that term or inserting a provision within subsection 6D to clarify intent).

TECHNICAL: Please consider revising "belonging" to "pertaining."

Working suggestion on requests relating to a child
A known child's parent or legal guardian may submit an authorized request under this section on behalf of the child regarding processing nonpublic personal information pertaining ~~belonging~~ to the child.

DEFAULT FRAMEWORK FOR CONSUMER OPTIONS [OPT IN VS OPT OUT]
Draft Article III: Section 7 & 8

Including an opt-in within the model is extremely problematic – with respect to any aspect of the model – for numerous reasons, including some provided below. Please see early 2023 comments and remarks for further details.

OUTLIER – NO US LAW HAS OPT-IN: We are unaware of any law in the United States that takes an opt-in approach.

OUTLIER – NO OTHER INDUSTRY: The insurance industry should not be held to the most restrictive approach. An opt-in would not only mean that licensees would have a legal/regulatory regime that deviates substantially from all other businesses, but it may put insurers at a relative disadvantage to other GLBA regulated entities. And for integrated financial institutions this could make business even more challenging.

CONFUSION: If insurance options differ from other industries in a state, consumers may become confused about the

UNWORKABLE: While overall problematic, any application to targeted advertising on an opt-in basis is untenable. This does not work as a default rule for providing information about products and services with a policyholder or someone who comes to a site for the purpose learning about a licensees products and services. Further, there must be certain exchanges for value given their importance of facilitating business purposes. (Consider loss costs, for example.)

EXISTING FRAMEWORK: Licensees have already built processes and systems to work with an opt-out framework.

EXPANSION THREAT: Having an opt-in for some topics may seem like an invitation in the future roll-out for some in some states to seek to move more aspects under that framework.

DISRUPTING THE CONSUMER EXPERIENCE: Separate asks (and forms) for consent (as contained in Sec. 7(C) may impact the user experience and be impractical to get at a different time from providing other options.

CONSUMER PROTECTION: An opt-in provides no greater consumer protection, rather it changes the default rule.

Crucial revision so all options take an opt-out approach

Any reference to opting in (and affirmative consent in these sections) should be revised to reflect opting out

SALE, TARGETED ADVERTISING, AND SPI
Draft Article III: Section 7 & 8

Placement & Structure

To connect with the rest of the model, please consider the notes and suggestions below:

CONSUMER REQUESTS VS. CONSUMER OPTIONS: The access, correction, and deletion requests are distinct and very different from the other aspects of the model dealing with making informed choices about how data may be shared. It makes sense for those requests to stand alone.

NEW VS. TOPICAL: Just because the sale and SPI provisions are also new does not mean that they belong with the Section 6 provisions under Article III. Rather, sale and SPI get at idea of limiting certain kinds of disclosure and this is something the model already does. (See current Chair's Draft section 16 for example.) Consider whether the sale/SPI provisions could be integrated into Article V (with exceptions and other provisions corresponding appropriately).

VISUALIZING OPTIONS: It seems that the construct under consideration is to give the consumer choice (and we strongly advocate that it should be on an opt out basis) around the following with respect to disclosure to a nonaffiliated third party:

- Nonpublic personal information generally (and for third party marketing) [in MDL-672];
- Nonpublic personal information for the purposes of targeted advertising (not first party);
- Nonpublic personal information for the purposes of sale (where it's really sale that's limited and not a valid business purpose); and
- Sensitive nonpublic personal information [as a particular subset of NPPI].

BRAINSTORMING: Building from existing framework and the wording that is in the Chair's Draft Section 16A(1), could something be done along these lines? Given the time constraints, these ideas are not fully vetted. And this simply shows an example for SPI as an illustration to share the idea and it does not repeat wording by expanding it out each of the bullets shown above.

Working suggested approach to integrate with model

Conditions for disclosure of sensitive personal information. Except as otherwise authorized in this Act, a licensee may not directly or through any affiliate, disclose any sensitive personal information about a consumer to a nonaffiliated third party unless:

(a) An exception applies under Article VI; or

(b) All the following conditions are met:

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

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

(iii) 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

(iv) The consumer does not opt out.

[Corresponding Section numbers and references/wording would need to be reviewed throughout.]

TARGETED ADVERTISING AS SEPARATE FROM SALE
Draft Article III: Section 7 --> New

To address the complexity of targeted advertising, if it is going to be included, we strongly urge that it be handled separately from sale and not mixed together as in the current draft.

ONFLATING ISSUES: There are important nuances to both advertising and sale topics and keeping them together could get very complicated. These are separate concepts, justifying separate provisions.

INTERPRETATION & COMPLIANCE: For licensees to better understand and comply with obligations, it would be helpful for targeted advertising to be handled separately from sale.

DIFFERENTIATING TYPES OF TARGETED ADVERTIZING & GLBA: Restrictions should be limited to third party advertising (outside of joint marketing with another financial institution). This kind of approach is consistent with the structure of the principles underlying the Gramm-Leach-Bliley Act and the Model 672. While online ads were not prevalent at the time that law/model was developed, applying the marketing ideas to be consistent as the technology has evolved makes sense.

OVERBROAD – CROSS CONTEXTUAL BEHAVIORAL ADVERTISING: A consumer may find it objectionable for an online business to follow the consumer from site to site. However, this is very different from a situation in which a consumer who *intentionally* interacts with a licensee's site later receives a targeted ad with a reminder or additional information/advertisement. By default, unless a consumer has indicated a preference otherwise, he/she should be able to benefit from this information.

TARGETED ADVERTIZING & COVERAGE GAPS: By allowing first party advertising (and joint marketing), a licensee may educate consumers about important products and services.

GENERAL MARKETING EXPENSES OR UNINTENDED CONSEQUENCES: It could be that reducing targeted advertising means that some individual licensees decide that they may allocate more resources to [what may be more costly and less effective] mass marketing. Conversely, it could mean that some individual licensees decide not to expand their general marketing so that conceivably certain markets may not have access to this marketing. Comments from 2023 offer additional context.

STATE APPROACH: Virginia's Consumer Data Protection Act offers an example of "targeted advertising" as a stand-alone provision (as well as a starting general definition). It also takes an opt-out approach (with opt-outs discussed below). See https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/

CONNECTION WITH GLBA: The focus of GLBA was on largely nonaffiliate marketing (outside of a joint marketing agreement). Targeted advertising seems a technological evolution of a type of online marketing and should be considered in the context of how it fits into the overall principles and structure of MDL-672. The limitation should not be with a licensee dealing with a consumer on its own site, such as via the use of first-part cookies, but rather as the consumer moves to other sites, where information from third party cookies is used to display advertising.

BRAINSTORMING: Building from the notes under Placement & Structure

> *Working suggested approach to integrate with model (see **BRAINSTORMING** above)*
>
> Conditions for disclosure of targeted advertising. 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: …

PRACTICAL TOPICS & TARGETED ADVERTISING: The language that was shared with the proof of concept 672-Plus effort included some rough wording relating to targeted advertising provisions that got at some topics that members raised. For context, though regulators are likely aware of how this works, it seems to be that an opt-out of targeted advertising is geared toward applicable cookies with respect to a specific browser on a specific device (e.g. an opt out using Chrome on my Windows laptop won't affect targeted advertising appearing on my Mac). Please see the excerpts that follow in terms of logistics and mechanics.

A. Limitation on targeted advertising. A consumer has the right to opt-out of Targeted Advertising.

B. Request procedures.

(1) A licensee shall act on the request within 15 days of receipt.

(2) 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.

(3) A licensee is under no obligation to obtain additional data to execute the opt-out request .

(4) A licensee may not solicit the consumer to change their opt-out selection for twelve months.

I. Targeted advertising opt out. A licensee may comply with the targeted advertising opt-out requirement by:

(2) Providing either a cookie banner or a link on the footer of their website homepage that allows a consumer to opt-out of targeted advertising; or

~~(2)~~(3) Using another method, if such approach can effectively identify a person and remove them from targeted advertising.

SCOPE & DEFINITION: Building off the connection to GLBA point raised above, as the drafting group considers this topic, the idea of limiting the restriction to those that are third party in nature seems a reasonable lens. A definition with this level of detail as to what is and is not included will aid implementation, compliance, and enforcement. As you consider the definition (and we encourage a sooner), we suggest the following:

"Targeted advertising" means displaying online advertisements to a consumer where the advertisement is selected based upon data that is linked or reasonably linkable to an identified or identifiable natural person obtained from that consumer's activities across nonaffiliated websites or online applications over time to predict such consumer's preferences or interests.

"Targeted advertising" does not include:
Online advertisements based on activities within a Licensee's own websites or online applications;
Online advertisements based on the context of a consumer's current search query, visit to a website, or online application;
Online advertisements directed to a consumer in response to the consumer's request for information or feedback; or
Processing personal data solely for measuring or reporting advertising performance, reach, or frequency.

SALE
Draft Article III: Section 7

Drafted in an overbroad way – whether with an opt-in (please see important points discussed above) or based on the unlimited scope (discussed below) – fixing this section is essential for a workable draft.

SCOPE & NECESSARY BUSINESS PURPOSES: Details matter and therefore the definitions and exceptions relating to this section cannot be thought of as ancillary. Any oversimplified interpretation of an exchange for value as a "sale" could miss some important business functions that must occur. For example, transmitting a consumer's personal information to a service provider in order to service a product or to prevent fraud should not be a sale, even though it could conceivably be interpreted by some as an exchange of personal information for some value. Also, consider how loss costs are developed, for example. We encourage the drafting regulators not to leave matters relating to precluding important business functions as matters to resolve later. An additional way to deal with some of these realities may be to integrate them into the substantive provisions with "notwithstanding" or otherwise creating an exception.

SCOPE & SEPARATING TARGETED ADVERTISING: See recommendation elsewhere in comments.

INTEGRATING WITH THE EXISTING MODEL: Please review the structure and way that the current model deals with limitations, notices, etc. (Also, see the **BRAINSTORMING** note above.)

Working suggestion for crucial revision for workable sale provision

A. A licensee shall not sell a consumer's nonpublic personal information~~, including for purposes of targeted advertising,~~ that the licensee has obtained from a consumer, unless:
(#) The licensee has provided the consumer an initial notice as required under [Sec.];
(#) The licensee has provided the consumer an opt out notice as required under Sec. [ ];
(#) The licensee has given the consumer a reasonable opportunity, before it sells the information, to opt out of the sale; and
(#) The consumer has not ~~affirmatively~~ opted out ~~in to the sale of their nonpublic personal information after receiving clear and conspicuous notice~~.

~~B.~~ Before a consumer opts out of ~~in to~~ the sale of nonpublic personal information, a licensee shall provide ~~clear and conspicuous~~ notice to the consumer consistent with Section 12 *[current model Section 8, which may need to be made more widely applicable],* ~~which includes:~~
~~(#) A description of the categories of nonpublic personal information that the licensee intends to sell;~~
~~(#) The purpose for which the nonpublic personal information will be sold; and~~
~~(#) The consumer's~~ ability ~~right to opt out of the sale of nonpublic personal information~~.

C. Notwithstanding any other provision, the selling nonpublic personal information subject to the limitation or opt out requirement does not occur when:
(#) The disclosure is to a third party for the purpose of or in support of providing a product or service requested by the consumer.

(#) A licensee provides or receives information to or receives anything of value an insurance support organization, statistical agent, or reinsurer;
(#) A licensee provides information to an affiliate or to a financial institution with which the licensee performs joint marketing;
(#) The business transfers to a third party the 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
(#) A consumer uses or directs the business to (i) disclose personal information; or (ii) interact with one or more third parties including but not limited to referrals to other licensees.

~~D. Affirmative Consent: the consumer's affirmative opt in consent must be obtained separately from any other consent obtained from the consumer.~~

SCOPE & DEFINITION: Because of the importance of getting the scope right to the workability of the provision, our current thought for a definition is shared below. Whether to include the "does not sell" kind of approach in the definition may depend on whether the carve out is added to the provision containing the selling limitation (as shown the working draft example above).

"**Sell**" or "**selling**" means the exchange of personal information to a third party for monetary or other valuable consideration.

A licensee does not sell 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 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 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 personal information; or (ii) interact with one or more third parties including but not limited to referrals to other licensees.

SENSITIVE PERSONAL INFORMATION
Draft Article III: Section 8

Kindly see the notes about integrating the provisions into Article V. With respect to Section 8B of the Chair's Draft, here are additional thoughts. Please avoid focusing the requirement on an undefined term and consider the ability to leverage the broader structure of the model by relying on the established exceptions.

UNDEFINED TERMS: The model does not define ***"authorized purposes and uses"*** or ***"identified purposes."*** Conceptually, it seems to be getting at the business purpose discussed with the PPWG in 2023 (and a definition provided). It could be more efficient to link to Article VI exceptions.

BIGGER PICTURE: Is the point that there should be a specific opportunity to opt-out of SPI disclosure outside of specific business purposes (that is subject to the exceptions)? If so, consider whether the model already has a structure for this that could be broadened. Please see current Article III (and Article V under the current Chair's Draft).

FACIAL CONFLICT – POTENTIAL INTERPRETATIONS: As drafted, it may be that (a) could be read to conflict with (c). Clarity is important for setting expectations and compliance. The way C reads a notice must be provided to a consumer if SPI is going to be used in a way that differs from how it is used in A.

MOVING THE REQUIREMENT & LEVERAGING WORKING MECHANISM: Consider the feasibility of moving this provision to connect with rest of the provisions would dovetail, including the limitations on redisclosure and reuse as well as the well thought out exceptions contained in the draft's Article VI.

PLACEMENT OF THE EXCEPTIONS & ABILITY TO OPT OUT: Having the exceptions in (A) and then the ability to opt out in (B) appears to nullify the ability to rely on those exceptions.

*This is just a working draft idea - please see **BRAINSTORMING** above*

~~A. Licensees may utilize sensitive personal information for identified purposes and uses, including those purposes and uses identified in Article VI (Exceptions to Limits on Disclosure of Financial Information);~~

A. Subject to the limits in Subsection B, a consumer may opt out of a licensee's disclosure of sensitive personal information except where such information is necessary to perform the services or to provide the goods reasonably expected by a reasonable average customer ~~shall have the right, at any time, to direct a licensee that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to the authorized purposes and uses~~.

B. This section does not apply if the licensee disclosure of sensitive personal information as permitted under Article VI *[exceptions].*

~~C.~~ A licensee that discloses ~~or process~~ a consumer's sensitive personal information for purposes other than those specified in subsection B ~~A~~ of this section shall provide ~~a clear~~

~~and conspicuous~~ notice to the consumer consistent with Section 12 *[current model Section 8, which may need to be made more widely applicable]* ~~which includes:~~

~~(#) A description of sensitive personal information that the licensee intends to disclose;~~

~~(#) The purpose for which the sensitive personal information will be processed; and~~

~~(#) The consumer's right to opt out of the processing of sensitive personal information for those purposes.~~

D. ~~A consumer's affirmative opt-in consent must be obtained separately from any other consent obtained from the consumer~~.

OTHER DEFINITIONS
Section 4

Several definitions were incorporated into the comments above. As the PPWG drafting process continues, it may be that the substantive requirements in Article III are impacted by the definitions and/or have implications for other sections.

For example, consider the change to the definition of **"nonpublic personal information"** (NPPI) (numbered as V in the discussion draft). Given how the definition now reads and the reference to (or intended reference to) NPPI within the TPSP section, the contractual provisions might technically be read to sweep in publicly available information. The reasonable wording pointing to "**publicly available**" is within the definition of "nonpublic personal financial information" of the existing Model #672 and which is not imbedded in the NPPI definition in this draft. It is essential that "nonpublic personal information" not encompass publicly available information. These kinds of practical technical issues are extremely important to consider.

While we heard that definitions are not part of the current review, because they are essential to the input and assumptions we are sharing, we are inserting several in these comments and we look forward to having conversations about them as the process continues.

* * * * *

Please understand that the input shared here is based on current input and that review and thought on these matters will continue and therefore feedback may evolve over time. On behalf of members, thank you for this opportunity.

NAVITUS Health Solutions

ARTICLE III. CONSUMER REQUESTS

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

A. Access to nonpublic personal information.

(1)Within 45 days of an authorized request from a consumer, a licensee shall disclose:

Nonpublic personal information about a consumer that is requested by the consumer and maintained by the licensee or any contracted third-party service provider; that:

(i). Must include a list of all third-party service providers to in which the licensee disclosed the consumer's nonpublic personal information; and

(ii). Must be provided in a format specific to the consumer and easily readable.

(2)In response to an authorized request from a consumer in (1) above, disclose:

(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, or unique biometric data.

(b) The licensee may instead disclose in generic terms that it maintains this information and list out each type of nonpublic personal information about the consumer.

Commented [KR1]: Curious as to why we would not disclose any of the listed information to a consumer, if this information were their own(?)

Additionally, (b) does not seem reasonable to deidentify when it's the person's own personal information that we are releasing to them.

B. Correction of nonpublic personal information.

(1)A consumer may request the correction of their nonpublic personal information.

(2)An authorized request from a consumer under this subsection shall identify the specific information that the consumer wishes to correct and provide explanation of why the licensee's information is incorrect.

(3)After receiving an authorized request under this subsection, a licensee shall, within 30 days of receipt of the request, notify the consumer of:

(a) Correction of the information as requested by the consumer or deletion of the information

in dispute; or

(b) Denial of the correction, the basis for refusal to correct the information as requested, and the consumer's ability to submit an appeal.

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

(a) The licensee believes the information is correct from clear documentation in its possession or

(b) The licensee received the information from a third-party, such as a healthcare provider, who has the responsibility or authority for determining the accuracy of the information.

C. Deletion of nonpublic personal information.

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

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

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

(b) The information may be necessary:

(i). To perform the contract or service request or benefiting the consumer; or

(ii). To comply with a legal obligation.

(c) 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 30 days, to delete with respect to information stored on an achieved or backup system until the archived or backup systems is deleted. A licensee must notify the consumer of such

delay

Commented [KR2]: Is the 30 day timeframe to delete any backups of information, doable?

D. Request Procedures

(1)Guidelines for responding to authorized requests except as otherwise provided in this Act, a licensee shall respond to requests submitted under this section in the following manner:

(a) A licensee shall respond to an authorized request received from a consumer under this section, unless

fulfilling the request proves impossible due to the specific nonpublic personal information is not locatable or retrievable by the licensee.

(b) If a licensee if unable to verify a request, the licensee shall not be required to consider the request and may request that the consumer provide additional information necessary to authenticate the consumer and the consumer's request.

(c) If a licensee declines to take action regarding the consumer's request, the licensee shall inform the consumer of the basis for declining to take action and any relevant instructions for how to appeal the decision pursuant to subparagraph (B)(3)(b) of this section.

(2)A consumer may make up to two requests per subsection in a 12-month period.

(3)A child's parent or legal guardian may submit a request under this section on behalf of the child regarding processing nonpublic personal information belonging to the child.

PIA

Clean Version of Revisions to Section 5 of Chair Draft Dated 8/5/2024
(tracks indicate PIA recommendations)

Section 5. Third-Party Service Provider Arrangements

A. Contract Requirements.
Commensurate with the size and complexity of the licensee, a~~A~~ licensee that discloses a consumer's nonpublic personal information (NPI) 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~~NPI 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 at the licensee's direction, to delete, destroy, de- identify or return all ~~nonpublic personal information~~NPI to the licensee when requested; or to delete ~~nonpublic personal information~~NPI after it is no longer necessary either to fulfill a legal requirement or to meet the record retention requirements of the licensee or third- party service provider and notify the licensee of that action;

(3) Requires the third-party service provider to notify the licensee if it can no longer comply with its obligations under this contract regarding privacy and the handling and safeguarding of ~~nonpublic personal information~~NPI and provides the licensee with a right to terminate the contract in that case;

~~(4) Requires that any contract between a third-party service provider and a subcontractor of the third-party service provider, 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)~~(4) 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)~~(5) Requires the third-party service provider to implement and maintain reasonable administrative, technical, and physical data security practices to protect the ~~nonpublic personal information~~NPI ~~data~~ from unauthorized access, destruction, use, modification, or disclosure; and

~~(7)~~(6) 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~~ NPI to a third-party service provider remains fully responsible for compliance with this Act and the handling of ~~nonpublic personal information~~NPI.

Article III, Sections 6-8 of Chair Draft Dated 8/5/2024

(tracks indicate PIA recommendations)

ARTICLE III. CONSUMER REQUESTS

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

A. Access to ~~nonpublic personal information~~NPI.

(1) Within 45 days of an authorized request from a consumer, a licensee shall disclose:

(a) ~~Nonpublic personal information~~NPI about a consumer that is requested by the consumer and maintained by the licensee or any contracted third-party service provider; that:

(i). ~~Must i~~Includes a list of all third-party service providers to ~~in~~ which the licensee disclosed the consumer's ~~nonpublic personal information~~NPI; and

(ii). ~~Must be~~ Is provided in a format specific to the consumer and easily readable.

(2) In response to an authorized request from a consumer in (1) above, a licensee shall not disclose:

(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/or answers, or unique biometric data.

(b) The licensee may instead disclose in generic terms that it maintains this information and list out each type of ~~nonpublic personal information~~NPI about the consumer.

B. Correction of ~~nonpublic personal information~~NPI.

(1) A consumer may request the correction of their ~~nonpublic personal information~~NPI.

(2) An authorized request from a consumer under this subsection shall identify the specific information that the consumer wishes to correct and provide an explanation of why or how the licensee's information is incorrect.

(3) After receiving an authorized request under this subsection, a licensee shall, within 30 days of receipt of the request, take one of the following steps and then notify the consumer of same:

(a) Correct~~ion of~~ the information as requested by the consumer or delete~~ion of~~ the information in dispute; or

(b) Deny~~ial of~~ the correction, provide the basis for the licensee's refusal to correct the information as requested, and describe the consumer's ability to submit an appeal.

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

(a) The licensee believes the information is correct, based on ~~from~~ clear documentation in its possession or

(b) The licensee received the information from a third -party, such as a healthcare provider, who has the responsibility for or authority ~~for~~ to determine~~ing~~ the accuracy of the information.

C. Deletion of ~~nonpublic personal information~~NPI.

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

(2) The licensee shall not be required to delete ~~nonpublic personal information~~NPI if any of these three (3) circumstances is present:

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

(b) The information may be necessary:

(i). To perform the contract or service request ~~or~~ benefiting the consumer; or

(ii). To comply with a legal obligation.

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

(4) A licensee may delay fulfilling a consumer's request for up to 30 days, to delete with respect to information stored on an achieved or backup system until the archived or backup system~~s~~ is deleted. A licensee must notify the consumer of such a delay.

D. Request Procedures. Guidelines for responding to authorized requests, except as otherwise provided in this Act:~~,~~ A~~a~~ licensee shall respond to requests submitted under this section in the following manner:

(1) A licensee shall respond to an authorized request received from a consumer under this section, unless fulfilling the request ~~proves~~would be impossible ~~due to~~ because the specific ~~nonpublic personal information~~NPI is not locatable or retrievable by the licensee.~~Guidelines for responding to authorized requests except as otherwise provided in this Act, a licensee shall respond to requests submitted under this section in the following manner:~~

(2) If a licensee is~~f~~ unable to verify a request, the licensee shall not be required to consider the request and may request that the consumer provide additional information necessary to authenticate the consumer and their ~~consumer's~~ request.

~~(1)~~(3) If a licensee declines to ~~take action~~ act on ~~regarding~~ the consumer's request, the licensee shall inform the consumer of the basis for declining to ~~take action~~ act and provide any relevant instructions for ~~how to~~ appealing the decision, pursuant to subparagraph (B)(3)(b) of this section.

(a) ~~A licensee shall respond to an authorized request received from a consumer under this section, unless fulfilling the request proves impossible due to the specific nonpublic personal information is not locatable or retrievable by the licensee.~~

(b) ~~If a licensee if unable to verify a request, the licensee shall not be required to consider the request and may request that the consumer provide additional information necessary to authenticate the consumer and the consumer's request.~~

(c) ~~If a licensee declines to take action regarding the consumer's request, the licensee shall inform the consumer of the basis for declining to take action and any relevant instructions for how to appeal the decision pursuant to subparagraph (B)(3)(b) of this section.~~

~~(2)~~(4) A consumer may make up to two requests ~~per subsection~~ in a 12-month period.

~~(3)~~(5) A child's parent or legal guardian may submit a request under this section on behalf of the child regarding ~~processing~~ use and maintenance of ~~nonpublic personal information~~NPI belonging to the child.

Section 7. Sale of ~~Nonpublic Personal Information~~NPI

A. A licensee shall not sell a consumer's ~~nonpublic personal information~~NPI, including for purposes of targeted advertising, that the licensee has obtained from a consumer, unless the consumer has ~~affirmatively~~ opted in to the sale of their ~~nonpublic personal information~~NPI after receiving clear and conspicuous notice of the licensee's intent to sell it.

B. Before ~~a consumer opts in to the sale of~~ selling a consumer's ~~nonpublic personal information~~NPI, a licensee shall provide a clear and conspicuous notice to the consumer, which includes:

(a) A description of the category/ies of ~~nonpublic personal information~~NPI that the licensee intends to sell;

(b) The purpose(s) for which the ~~nonpublic personal information~~NPI ~~will~~ may be sold; and

(c) The consumer's right to opt out of the sale of ~~nonpublic personal information~~NPI.

C. ~~Affirmative Consent~~Opportunity to opt out: T~~t~~he licensee must offer the consumer~~'s~~ the opportunity to opt out ~~affirmative opt-in consent~~ of the sale of all or some of their NPI after notifying the consumer of its intent to sell the consumer's NPI.

[Drafting Note: States should insert here the procedure by which consumers may request access to, or correction or deletion of, their NPI, or the means by which the consumer may opt out, if not addressed elsewhere in revised #672.]

- The consumer must notify the licensee of their intention to opt out ~~must be obtained~~ separately from any other consent obtained from the consumer.

Section 8. Use and Disclosure of Sensitive Personal Information

A. Licensees may utilize sensitive personal information for certain identified purposes and uses, including those purposes and uses identified in Article VI (Exceptions to Limits on Disclosures of Financial Information);

B. A consumer shall have the right, at any time, to direct a licensee that collects sensitive personal information about the consumer to limit its use of ~~the consumer's sensitive personal~~ that information to the authorized purposes and uses;

C. A licensee that discloses or processes a consumer's sensitive personal information for purposes other than those specified in subsection A of this section shall first provide a clear and conspicuous notice to the consumer, which includes:

(a) A description of sensitive personal information that the licensee intends to disclose;

(b) The purpose(s) for which the sensitive personal information will be ~~processed~~disclosed; and

(c) The consumer's right to opt out of the processing of sensitive personal information for those purposes.

C. A consumer's affirmative opt-in consent for the use of their sensitive personal information must be obtained separately from any other consent obtained from the consumer.

Privacy4Cars (link does not open document)

Thank you for the opportunity to provide comments on Article III, Sections 6, 7, and 8 of Model #672. We are writing to provide constructive feedback regarding personal data protections for Rhode Island residents, with a specific focus on data practices of the automotive sector. While data privacy regulations often concentrate on digital and online environments, vehicles represent an increasingly significant and frequently overlooked source of personal data collection and use.

Currently, many automotive businesses lack comprehensive protocols for handling personal data collected through vehicles. Specifically, our research indicates that very few automotive companies have robust processes for:

- Deleting driver and passenger personal data stored within vehicles
- Responding to consumer requests to opt out of personal data selling, sharing, and use
- Providing transparent mechanisms for personal data management and control related to the vehicle and connected/related services

We respectfully recommend that the proposed regulation explicitly address vehicle-specific personal data considerations, including:

- Including types of personal data collected in automotive contexts
- Mechanisms for personal data deletion
- Clear opt-out procedures
- Transparent personal data collection/use/selling/sharing disclosure summaries

Please review our proposed updates here: https://docs.google.com/document/d/1uXKi-FyZHMGnS9VGIvfLMu9ZQcx5Zh5blyw0QVfqnY4/edit?usp=sharing . Please let us know if you cannot open this document and need this in a different format. We tried to save this as a Word document, but lost the comments and your team asked for redlines (we highlighted additions in yellow color).

Here is a detailed summary of our proposed changes by section:

- Section 4. - Definitions
  - Added "Authorized Agent"
  - Added to the definition of "nonpublic personal information" to include:
    - neural data
    - contents of messages (e.g., emails, texts, chats) unless it's directed to the business
    - Racial, ethnic, citizenship, immigration, religious, philosophical, union membership data
    - health, sex life, sexual orientation data
    - genetic data, health, pregnancy status data
  - Added "Sell" definition which includes personal data sharing
- Article III: Consumer Requests. Section 6
  - added references to authorized agents everywhere a request from a consumer is mentioned

- added sensitive data types as not being returned in an access request (ie pregnancy health, sex life, sexual orientation, etc)
- Section C -- deletion of nonpublic personal information -- added " – including stored locally within vehicles,"
- Section C - 3 - added "including vehicles' local storage"

- Article III: Sale of nonpublic personal information. Section 7
  - added "or share" to mention of "sell" (also explicitly added a definition for in the definitions sections)
- Article IV: Privacy and Opt Out Notices for Nonpublic Personal Information
  - Added a new section "G. For vehicles that collect personal data, transparent disclosures must be made to consumers in a privacy label format with a link or a QR code to the larger Privacy Notice."
  - ^same for annual privacy notice

By incorporating these vehicle-specific data protection measures, the regulation can provide more comprehensive and meaningful privacy safeguards and choices for Rhode Island residents regarding their personal data.

Consumer Comments

Consumer Rep – Harry Ting

ARTICLE III. CONSUMER REQUESTS
REVISIONS FROM NAIC CONSUMER REPRESENTATIVES

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

A. Access to nonpublic personal information.

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

[COMMENT: We have replaced "authorized" with "authenticated" throughout this Article. It is a more appropriate term. Authentication needs to be defined in the Definitions section.]

(a) Disclose to the consumer all of their nonpublic personal information ~~about a consumer that is requested by the consumer and~~ maintained by the licensee or any contracted third-party service provider~~; that~~ and:

(b). ~~Must~~ Include in the disclosure a list of all third parties to ~~in~~ which the licensee has disclosed the consumer's nonpublic personal information; and

(c). The disclosure must be ~~provided~~ in a format ~~specific to~~ accessible by the consumer and ~~easily readable~~ written in a manner that follows the Federal Plain Language Guidelines.

(2) In response to an ~~authorized~~ authenticated request from a consumer in (1) above, a licensee ~~shall not disclose~~:

(a) ~~A~~ Shall not disclose 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, or unique biometric data.

(b) ~~The licensee~~ May instead disclose in generic terms ~~that it maintains this~~ the types of information it maintains by ~~and~~ listing ~~out~~ each type of nonpublic personal information it has about the consumer.

[COMMENT: We are concerned that Section A(2) compromises the ability of consumers to identify fraudulent use of their identifiers. For example, if a hacker set up fraudulent accounts in a consumer's name using the consumer's identifiers, the Model Act needs to provide consumers the ability to unearth such situations.]

B. Correction of nonpublic personal information.

(1) A consumer may request the correction of their nonpublic personal information maintained by a licensee or a contracted third-party service provider.

(2) An ~~authorized~~ authenticated request from a consumer under this subsection shall identify the specific information that the consumer wishes to correct and provide an explanation of why the ~~licensee's~~ information is incorrect.

(3) After receiving an ~~authorized~~ authenticated request ~~under this subsection~~, a licensee shall, within 30 days of receipt of the request, notify the consumer of:

(a) Correction or deletion of the information ~~as requested by the consumer or deletion of the information in dispute~~; or

(b) Denial of the ~~correction~~ request, the basis for ~~refusal to correct the information as requested~~ the denial, ~~and~~ information about how the consumer~~'s~~ can ~~ability to submit an~~ appeal the denial, and an explanation of how the appeal will be reviewed and consumer will be notified of the decision.

(4) A licensee may deny a request for correction of a consumer's nonpublic information if:

(a) The licensee ~~believes~~ can document that the information is correct~~; from clear documentation in its possession~~ or

(b) ~~The licensee received the information from~~ A third party, such as a healthcare provider, ~~who~~ has the responsibility or authority for determining the accuracy of the information. In this case, the licensee must include in the response to the consumer the identity of the third party and information on how to contact the third party to request correction of the information.

C. Deletion of nonpublic personal information.

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

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

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

(b) The information ~~may be~~ is necessary:
(i). To perform ~~the~~ a contract or service request ~~or benefiting the consumer~~; or

(ii). To comply with a legal obligation.

(c) 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 to delete nonpublic personal information by up to 30 days, ~~to delete with respect to information stored on an achieved or backup system until the archived or backup systems is deleted. A licensee must notify the consumer of such delay~~ if the information is stored on an archived or backup system and additional time is required to fulfill the request. A licensee must notify the consumer of such delay. During this delay, the licensee may not share that information with any third party.

(4) If, after an authenticated request by a consumer to delete the consumer's nonpublic information, a licensee or third party service provider is unable to locate or retrieve that information within the timeframe set forth in Section 6(C), the licensee or third party service provider must immediately take the following steps:

(a) Notify the consumer of the inability to comply with the request; and

(b) Notify the state regulator of the inability to comply with the request.

[COMMENT: There should be consequences if a licensee or third party service provider frequently is unable to comply with authenticated consumer requests. The licensee or third party service provider should be required to submit a plan of correction and/or be subject to a fine.]

D. Request Procedures

(1) ~~Guidelines for responding to authorized requests~~ Except as otherwise provided in this Act, a licensee shall respond to requests submitted under this section ~~in the following manner~~:

(a) A licensee shall respond to an ~~authorized~~ authenticated request received from a consumer under this section, unless fulfilling the request proves impossible ~~due to~~ because the specific nonpublic personal information is not locatable or retrievable by the licensee.

(2) A consumer may make up to ~~two~~ six requests ~~per subsection~~ for access, correction, or deletion of their nonpublic personal information to a licensee or their contracted third party service provider in a 12-month period.

(3) A child's parent or an individual's legal guardian or someone with a power of attorney over a consumer's business or health affairs may submit a request under this section on their behalf ~~of the child~~ regarding their nonpublic

personal information ~~belonging to the child~~. All conditions stated in this subsection shall apply to such requests.

E. Request Denials

(1) If a licensee if unable to authenticate a request, the licensee shall not be required to consider the request and may ask the consumer for additional information necessary to authenticate the consumer and the consumer's request.

(2) If a licensee declines to act on the consumer's request, the licensee shall inform the consumer of the basis for the refusal and provide instructions on how to appeal the decision pursuant to subparagraph (B)(3)(b) of this section.

ection 7. Sale of Nonpublic Personal Information

A licensee and any contracted third party service providers shall not sell a consumer's nonpublic personal information obtained from that consumer, including for purposes of targeted advertising~~, that the licensee has obtained from a consumer, unless the consumer has affirmatively opted in to the sale of their nonpublic personal information after receiving clear and conspicuous notice~~.

A. ~~Before a consumer opts in to the sale of nonpublic personal information, a licensee shall provide a clear and conspicuous notice to the consumer, which includes:~~

(a) ~~A description of the categories of nonpublic personal information that the licensee intends to sell;~~

(b) ~~The purpose for which the nonpublic personal information will be sold; and~~

(c) ~~The consumer's right to opt out of the sale of nonpublic personal information.~~

B. ~~Affirmative Consent: the consumer's affirmative opt in consent must be obtained separately from any other consent obtained from the consumer.~~

Section 8. Use and Disclosure of Sensitive Personal Information

A. ~~Licensees may utilize sensitive personal information for certain identified purposes and uses, including those purposes and uses identified in Article VI (Exceptions to Limits on Disclosures of Financial Information);~~

B. ~~A consumer shall have the right, at any time, to direct a licensee that collects sensitive personal information about the consumer to limit its use of the consumer's sensitive personal information to the authorized purposes and uses;~~

C. ~~A licensee that discloses or processes a consumer's sensitive personal information for purposes other than those specified in subsection A of this section shall provide a clear and conspicuous notice to the consumer, which includes:~~

(a) ~~A description of sensitive personal information that the licensee intends to disclose;~~

(b) ~~The purpose for which the sensitive personal information will be processed; and~~

(c) ~~The consumer's right to opt out of the processing of sensitive personal information for those purpose.~~

~~C. A consumer's affirmative opt-in consent must be obtained separately from any other consent obtained from the consumer.~~

[COMMENT: Per our Consumer Representatives' Privacy Principles, sensitive personal information should only be used to fulfill a consumer's business with licensees or to fulfill legal obligations. Any other disclosure should require explicit permission of the consumer that specifies the sensitive personal information to be disclosed and the purpose for which it will be used.]