NAIC INSURANCE INFORMATION AND PRIVACY PROTECTION MODEL ACT

EXPOSURE DRAFT TOPICS – APRIL 15, 2020
WITH APRIL 29, 2020 COMMENTS ON SECTIONS 1-9
(and definitions from Model #668-IDSM) 8/22/21

Table of Contents

Preamble

COMMENTS: This paragraph needs a rewrite. In addition to being streamlined and put into active voice instead of passive voice, the following items merit discussion:

- Are the definitions correct/current? Do we need to overtly state we expect third party vendors, Insurtechs, TPAs, etc., to be included in the definition of 'insurance support organization.'
- The term 'fairness' – do we need to add the words 'transparency,' 'security' and 'confidence'? Add all of these terms? Better ones? We want to ensure the consumer and the company has "confidence" that the data/information is being used appropriately.
- Application of Provisions. Should this continue to apply to the same class of entities? The rights granted extend to "natural" persons. What about "legal" persons? [Note the definition of "person" includes both natural persons and legal entities.] Are there new 'rights' that have emerged that should be included? What about unrelated third-party recipients of data maintained by covered entities? Should there be a size threshold or category that captures entities that trade in data?

ACLI: Flag for later discussion.

~~The purpose of~~ this Act ~~is to~~ establishes standards for the collection, use and disclosure of information gathered ~~in connection~~ with insurance transactions by insurance ~~institutions,~~ agents or insurance support organizations; to maintain a balance between the need for information by those conducting the business of insurance and the public's need for fairness in insurance information practices, including the need to minimize intrusiveness; to establish a regulatory mechanism to enable natural persons to ascertain what information is being or has been collected about them in connection with insurance transactions and to have access to such information ~~for the purpose of~~ verify~~ing~~ or disput~~ing~~e its accuracy; to limit the disclosure of information collected in connection with insurance transactions; and to enable insurance applicants and policyholders to obtain the reasons for any adverse underwriting decision.

Section 1. Scope

A. The obligations by this Act shall apply to those insurance institutions, agents or insurance support organizations which, on or after the effective date of this Act:

(1) In the case of life, health and disability insurance:

(a) Collect, receive or maintain information in connection with insurance transactions which pertains to natural persons who are residents of this state, or

(b) Engage in insurance transactions with applicants, individuals or policyholders who are residents of this state, and

(2) In the case of property or casualty insurance:

(a) Collect, receive or maintain information in connection with insurance transactions involving policies, contracts or certificates of insurance delivered, issued for delivery or renewed in this state, or

(b) Engage in insurance transactions involving policies, contracts or certificates of insurance delivered, issued for delivery or renewed in this state.

COMMENTS:

- Do we need the distinction between LOBs? Can't we combine both A and B? Can we rewrite A above to simply state this act applies to all lines of business?

ACLI: Distinguish between lines of business (§1 A & B) – Flag for discussion later

MPL: **Agree** that language should be streamlined, and terminology revised.

- All of the definitions in the section need to be reviewed in light of other recently passed models, the CCPA, GDPR, FCRA, Data Security {#668} and other resource documents. We also need to ensure we are consistent throughout these two models currently under review. Should we include reference to legislation from Washington State that I understand is being touted as a possible future model? Its SB 6291

ACLI: Review of definitions and alignment with other laws – Yes, we agree

B. The rights granted by this Act shall extend to:

(1) In the case of life, health or disability insurance, the following persons who are residents of this state:

(a) Natural persons who are the subject of information collected, received or maintained in connection with insurance transactions, and

(b) Applicants, individuals or policyholders who engage in or seek to engage in insurance transactions, and

(2) In the case of property or casualty insurance, the following persons:

(a) Natural persons who are the subject of information collected, received or maintained in connection with insurance transactions involving policies, contracts or certificates of insurance delivered, issued for delivery or renewed in this state, and

(b) Applicants, individuals or policyholders who engage in or seek to engage in insurance transactions involving policies, contracts or certificates of insurance delivered, issued for delivery or renewed in this state.

C. For ~~purposes of~~ this section, a person shall be considered a resident of this state if the person's last known mailing address, as shown in the records of the insurance institution, agent or insurance support organization, is located in this state.

Comment: Is paragraph D necessary? Should we make it clear that there are two parts to the question? That is, the first is if there should be a carve out for the specific class of public records that deal with title to real property and the second is whether it should apply to any info collected from the public records.

ACLI: §1 D. – Not applicable

ATLA: **Section 1(D):** In terms of public records, the Act should mirror the scope of the CCPA and clearly exempt "publicly available information" as defined within CCPA as "information that is lawfully made available from federal, state, or local government records." We suggest striking 1(D) and adding the CCPA definition for publicly available information.

MPL: **D. Agree** that all publicly available information should be carved out.

D. Notwithstanding Subsections A and B above, this Act shall not apply to information collected from the public records of a governmental authority and maintained by an insurance institution or its representatives ~~for the purpose of insuring~~ to insure the title to real property ~~located~~ in this state.

Section 2. Definitions

As used in this Act:

COMMENT: Is it cleaner to update definitions through revisions to existing terms or through the addition of new terms? There is a need to update the scope of "personal information," we need to ensure it accurately reflect business practices of today and perhaps add definitions for such terms as "biometric information," "collects," "consumer profile," "sell," "third party," "general business practice" or others? Key term esp in section 4.B(4). May be similar definition available in unfair trade practice statutes. Why does "insurance transaction" seem to exclude commercial insurance? Consider adding in a couple others that might be helpful such as "facial recognition' service/template or similar, pseudonymous data," etc.

ACLI: Flag entire section for discussion later. If regulators are going to go through with this exercise, then taking a wholistic approach to the definitions is necessary.

MPL: **Agree** that all publicly available information should be carved out.

A. "Adverse underwriting decision" means:

COMMENT: For A - our preference is to use a definition from the Market Regulation Handbook. It is more concise and more accurate.

MPL: **A. Agree** with using Market Regulations Handbook definition.

(1) Any of the following actions ~~with respect to~~ regarding insurance transactions involving individually underwritten insurance coverage ~~which is individually underwritten~~:

(a) A declination of insurance coverage;

(b) A termination of insurance coverage;

(c) Failure of an agent to apply for insurance coverage with a specific insurance institution which the agent represents and which is requested by an applicant;

(d) In the case of a property or casualty insurance coverage:

(i) Placement by an insurance institution or agent of a risk with a residual market mechanism, an unauthorized insurer or an insurance institution which specializes in substandard risks; or

(ii) The charging of a higher rate based on ~~the basis of~~ information which differs from that which the applicant or policyholder furnished;

Drafting Note: The use of the term "substandard" in Section 2A(d)(i) ~~is intended to~~ should apply to those insurance institutions whose rates and market orientation are directed at risks other than preferred or standard risks. To facilitate compliance with this Act, Commissioners should develop ~~consider developing~~ a list of insurance institutions operating in their state which specialize in substandard risks and make it known to insurance institutions and agents.

(e) In the case of a life, health or disability insurance coverage, an offer to insure at higher than standard rates.

(2) Notwithstanding Paragragh (1) above, ~~the following~~ these actions shall not be considered adverse underwriting decisions but the insurance institution or agent responsible for their occurrence shall nevertheless provide the applicant or policyholder with the specific reason or reasons for their occurrence:

(a) The termination of an individual policy form on a class or statewide basis;

(b) A declination of insurance coverage solely because such coverage is not available on a class or statewide basis; or

(c) The rescission of a policy.

B. "Affiliate" or "affiliated" means a person that directly, or indirectly through one or more intermediaries, controls, is controlled by or is under common control with another person.

MPL: B-Z. Flag for discussion. All definitions for which there is not consensus between regulators, and stakeholders, should be discussed in order to ensure clarity for all parties.

C. "Agent" means [~~make reference~~ refer here to every appropriate statutory category of producer, including brokers, authorized to do business in the state. This is necessary because in many states different types of producers, or producers for certain types of insurance institutions are referred to by specific statutory terms in the insurance code.]

COMMENT: We want to ensure that the definitions capture third party vendors, Insurtechs, TPAs, etc. Not sure which definition is the best one to modify.

D. "Applicant" means a person who seeks to contract for insurance coverage other than a person seeking group insurance that is not individually underwritten.

E. "Authorized Individual" means an individual known to and screened by the Licensee and determined to be necessary and appropriate to have access to the Nonpublic Information held by the Licensee and its Information Systems. From NAIC Model #668 (Insurance Data Security Model Law-IDSM)

F. "Commissioner" means [insert the appropriate title and statutory reference for the principal insurance regulatory official of the State.] "Commissioner" means the chief insurance regulatory official of the state. From 668-IDSM)

G. "Consumer" means an individual, including but not limited to applicants, policyholders, insureds, beneficiaries, claimants, and certificate holders who is a resident of this State and whose Nonpublic Information is in a Licensee's possession, custody, or control. (From 668-IDSM)

H. “Consumer report” means a written, oral or other communication of information bearing on a natural person’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living ~~which is used or expected to be used in connection with~~ for an insurance transaction.

CDIA: Under Section 2, "Definitions" , on page 5 there are edits to the definition of “Consumer Report”. We recommend using the exact definition of a “Consumer Report” as defined in the Fair Credit Reporting Act (FCRA) Section 1681a or leaving this language as it currently stands

in Model Act #670 without any changes or edits. We believe there is a need for consistency with definitions in model acts and where they are already defined under the federal laws that CRAs are regulated by. Comparatively, there were no changes to the definition of "Consumer reporting agency" in the exposure draft for Model #670.

I. "Consumer reporting agency" means a person who:

(1) Regularly engages, in whole or in part, in the practice of assembling or preparing consumer reports for a monetary fee;

(2) Obtains information primarily from sources other than insurance institutions; and

(3) Furnishes consumer reports to other persons.

J. "Control," including the terms "controlled by" or "under common control with," means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of voting securities, by contract other than a commercial contract for goods or nonmanagement services, or otherwise, unless the power ~~is the result of~~ results from an official position with or corporate office held by the person.

COMMENT: Why is paragraph H needed? Is it consistent with the definition of "control" used today?

K. "Declination of insurance coverage" means a denial, in whole or in part, by an insurance institution or agent of requested insurance coverage.

COMMENT: All of the parts of definition J need discussion; need to look to other resource documents, too. Some of the points to consider: does J2 include dependents? Does J5 include a beneficiary?

L. "Individual" means a natural person who:

(1) In the case of property or casualty insurance, is a past, present or proposed named insured or certificateholder(s);

(2) In the case of life, health or disability insurance, is a past, present or proposed principal insured or certificateholder;

(3) Is a past, present or proposed policyowner;

(4) Is a past or present applicant;

(5) Is a past or present claimant; or

(6) Derived, derives or is proposed to derive insurance coverage under an insurance policy or certificate subject to this Act.

M. "Institutional source" means any person or governmental entity that provides information about an individual to an agent, insurance institution or insurance support organization, other than:

(1) An agent;

(2) The individual who is the subject of the information; or

(3) A natural person acting in a personal capacity rather than in a business or professional capacity.

COMMENT: Is paragraph K needed? Is it correct anymore?

N. "Insurance institution" means any corporation, association, partnership, reciprocal exchange, inter-insurer, Lloyd's insurer, fraternal benefit society or other person engaged in the business of insurance, including health maintenance organizations, medical service plans and hospital service plans as defined in [insert the ~~applicable~~ section of the State insurance code which defines health maintenance organizations or medical or hospital service plans.] "Insurance institution" shall not include agents or insurance support organizations.

COMMENT: discuss definitions. We don't agree with the last sentence.

O. "Insurance support organization" means:

(1) Any person who regularly engages, in whole or in part, in the practice of assembling or collecting information about natural persons ~~for the primary purpose of providing~~ primarily to provide the information to an insurance institution or agent for insurance transactions, including:

(a) The furnishing of consumer reports or investigative consumer reports to an insurance institution or agent for use in connection with an insurance transaction, or

(b) The collection of personal information from insurance institutions, agents or other insurance support organizations ~~for the purpose of detecting or preventing~~ to detect or prevent fraud, material misrepresentation or material nondisclosure in connection with insurance underwriting or insurance claim activity.

(2) Notwithstanding Paragraph (1) above, ~~the following~~ these persons shall not be considered "insurance support organizations" for ~~purposes of~~ this Act: agents, government institutions, insurance institutions, medical care institutions and medical professionals.

COMMENT: Discuss definition M; refer to other resource documents.

P. "Insurance transaction" means any transaction involving insurance primarily for personal, family or household needs rather than business or professional needs which entails:

COMMENTS: Discuss definition N; need to refer to other resource documents.

- The personal/business distinction is a gap in privacy protections which is common to GLBA-derived statutes; essentially all protections arise from an "insurance transaction" and, thus, PII gathered in connection with commercial coverages is excluded. This problem is recurrent in many states' statutes.
- Personal information can be collected in connection with a large range of commercial policies and, in many cases, the data subject may be giving up their PII as part of a job function and may not have a choice about which insurer to use or what data they are willing to submit.
- Workers' Comp is the most significant example, (research shows states disagree about whether W/C was intended to be covered under GLBA and derivative statutes), however, others include "key person," business continuity policies, E&O Liability Coverage, etc.

(1) The determination of an individual's eligibility for an insurance coverage, [benefit or payment]; or

COMMENTS:

- Do we need to add "benefit or payment" after the word "coverage"?
- One of the areas where CCPA grants more consumer rights than existing statutes is that it grants rights to "non-consumers," *e.g.*, people who browse a website, but do not buy anything. It

appears that the Model would protect consumers who request a quote, but do not ultimately purchase coverage, however, we may want to discuss information which insurers collect via website visits, tracking cookies, web "beacons," etc. {Issue – Google's recent announcement that they are phasing out support for third-party cookies.}

(2) The servicing of an insurance application, policy, contract or certificate.

COMMENTS: need a definition of "servicing"

Q. "Investigative consumer report" means a consumer report or portion thereof in which information about a natural person's character, general reputation, personal characteristics or mode of living is obtained through personal interviews with the person's neighbors, friends, associates, acquaintances or others who may know of such information ~~have knowledge concerning such items of information.~~

R. "Licensee" means any Person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this State or a Licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction. (From 668-IDSM)

COMMENTS: needs a lot of discussion. Terms are too subjective; need to ensure this definition tracks current business practices. Disclosures needed for personal interviews? Reliability of personal interviews? What elements are "allowed" to be discussed and collected? Proxy for prohibited elements? Relevance?

S. "Medical-care institution" means any facility or institution that is licensed to provide health care services to natural persons, including but not limited to: health-maintenance organizations home-health agencies, hospitals, medical clinics, public health agencies, rehabilitation agencies and skilled nursing facilities.

T. "Medical professional" means any person licensed or certified to provide health care services to natural persons, including but not limited to, a chiropractor, clinical dietician, clinical psychologist, dentist, nurse, occupational therapist, optometrist, pharmacist, physical therapist, physician, podiatrist, psychiatric social worker or speech therapist.

U. "Medical record information" means personal information which:

(1) Relates to an individual's physical or mental condition, medical history or medical treatment; and

(2) Is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent or legal guardian.

V. "Nonpublic Information" means information that is not Publicly Available Information and is:

(1) Business related information of a Licensee the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Licensee;

(2) Any information concerning a Consumer which because of name, number, personal mark, or other identifier can be used to identify such Consumer, in combination with any one or more of the following data elements:

(a) Social Security number,

(b) Driver's license number or non-driver identification card number,

(c) Account number, credit or debit card number,

(d) Any security code, access code or password that would permit access to a Consumer's financial account, or

(e) Biometric records;

(3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a Consumer and that relates to

(a) The past, present or future physical, mental or behavioral health or condition of any Consumer or a member of the Consumer's family,

(b) The provision of health care to any Consumer, or

(c) Payment for the provision of health care to any Consumer. (From 668-IDSM)

COMMENT: compare to Electronic Health Record-EHR definitions

W. "Person" means any natural person, corporation, association, partnership or other legal entity. "Person" means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association. (From 668-IDSM)

COMMENT: needs discussion. See Comments in Preamble.

X. "Personal information" means any ~~individually~~ identifiable information gathered ~~in connection with~~ as part of an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health or any other personal characteristics. "Personal information" includes an individual's name and address and "medical record information" but does not include "privileged information".

COMMENTS: needs a lot of discussion.

- CCPA specifies that, in addition to "traditional" PII, consumers also have rights in "consumer profile" information which companies have compiled using information about the consumer. It is ambiguous as to whether this section covers that type of information. On the one hand, businesses have worked to develop that information; on the other hand, it pertains to the consumer and could prove detrimental to the consumer if incorrect.

- Additionally, we should consider the extent to which companies create profiles purely for underwriting-related reasons, versus for marketing (or sale) purposes. [Example - recent Maryland denial of a company's rating algorithm which (allegedly) identified consumers who overpaid for coverage and targeted them for rate increases, while giving reductions to other consumers.]

Y. "Policyholder" means any person who:

(1) In the case of individual property or casualty insurance, is a present named insured;

(2) In the case of individual life, health or disability insurance, is a present policyowner; or

(3) In the case of individually underwritten group insurance ~~which is individually underwritten~~, is a present group certificateholder.

COMMENT: confirm the LOB distinctions are needed

Z. "Pretext interview" means an interview whereby a person, in an attempt to obtain information about a natural person, performs one or more of ~~the following~~ these acts:

(1) Pretends to be someone he or she is not;

(2) Pretends to represent a person he or she is not ~~in fact~~ representing;

(3) Misrepresents the true purpose of the interview; or

(4) Refuses to identify himself or herself upon request.

AA. "Privileged information" means any ~~individually~~ personally identifiable information that:

(1) Relates to a claim for insurance benefits or a civil or criminal proceeding involving an individual; and

(2) Is collected ~~in connection~~ with or in reasonable anticipation of a claim for insurance benefits or civil or criminal proceeding involving an individual; provided, ~~however,~~ the information otherwise meeting the requirements of this subsection shall nevertheless be considered "personal information" under this Act if it is disclosed in violation of Section 13 of this Act.

BB. "Publicly Available Information" means any information that a Licensee has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

For the purposes of this definition, a Licensee has a reasonable basis to believe that information is lawfully made available to the general public if the Licensee has taken steps to determine:

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

(2) Whether a Consumer can direct that the information not be made available to the general public and, if so, that such Consumer has not done so. (From 668-IDSM)

COMMENT: discussion and updating needed

Drafting Note: The phrase "in reasonable anticipation of a claim" contemplates that the insurance institution has knowledge of a loss but has not received formal notice of the claim.

CC. "Residual market mechanism" means an association, organization or other entity defined or described in

Sections(s) [insert those sections of the state insurance code authorizing the establishment of a FAIR Plan, assigned risk plan, reinsurance facility, joint underwriting association, etc.]

DD. "State" means [adopting state]. (From 668-IDSM)

COMMENT: Is paragraph X needed?

Drafting Note: Those states having a reinsurance facility may want to exclude it from this definition if the state's policy is not to disclose to insureds the fact that they have been reinsured in the facility.

EE. "Termination of insurance coverage" or "termination of an insurance policy" means either a cancellation or nonrenewal of an insurance policy, in whole or in part, for any reason other than failing ~~the failure~~ to pay a premium as required by the policy.

A. "Third-Party Service Provider" means a Person, not otherwise defined as a Licensee, that contracts with a Licensee to maintain, process, store or otherwise is permitted access to Nonpublic Information through its provision of services to the Licensee. (From 668-IDSM)

FF. "Unauthorized insurer" means an insurance institution ~~that has~~ not ~~been~~ granted a certificate of authority by the Commissioner to transact the business of insurance in this state.

Drafting Note: Each state must ensure ~~make sure that~~ this definition ~~is consistent with~~ follows its surplus lines laws.

Section 3. Pretext Interviews

No insurance institution, agent or insurance support organization shall use or authorize the use of pretext interviews to obtain information in connection with an insurance transaction; provided, however, a pretext interview may ~~be undertaken to~~ obtain information from a person or institution that does not have a generally or statutorily recognized privileged relationship with the person about whom the information relates ~~for the purpose of investigating~~ to investigate a claim where, based upon specific information available for review by the Commissioner, there is a reasonable basis for suspecting criminal activity, fraud, material misrepresentation or material nondisclosure in connection with the claim.

COMMENT: we need to compare this definition to other ant-fraud definitions and other resource documents.

ACLI: Compare to other anti-fraud definitions – Flag for discussion later

Drafting Note: Some states may desire to eliminate the exception in this section and ~~thereby~~ prohibit pretext interviews in all instances. Other states may desire to broaden the exception so ~~that~~ pretext interviews can be utilized in underwriting and rating situations ~~as well as~~ and claim situations. States may either expand or limit the prohibition against pretext interviews suggested in this section to accommodate their individual needs and circumstances. Deviation from the standard developed here should not ~~seriously~~ undermine efforts to achieve uniform rules for insurance information practices throughout the ~~various~~ states.

COMMENT: attention needs to be given to not "harming" the consumer and their 'right' to privacy.

Section 4. Notice of Insurance Information Practices

A. An insurance institution or agent shall provide a notice of information practices to all applicants or policyholders in connection with insurance transactions as provided below:

(1) In the case of an application for insurance, a notice shall be provided no later than:

(a) At the time of the delivery of the insurance policy or certificate when personal information is collected only from the applicant or from public records; or

COMMENT: shouldn't the notice be provided at the time of application? It seems like (b) below could be a stand-alone requirement?

ACLI: Notice at time of application – Flag for discussion later

ATLA: **Section 4:** Given the prevalence of interstate commerce, notification requirements should provide consistency. For example, as applicable, delivery of the privacy notice should be consistent with GLBA and the CFPB's Reg P requirements.

MPL: **Flag for discussion**-Based on the number and variety of comments received for this section, the entiresection should be thoroughly discussed.

(b) At the time the collection of personal information is initiated when personal information is collected from a source other than the applicant or public records;

(2) In the case of a policy renewal, a notice shall be provided ~~no later than~~ by the policy renewal date, except that no notice shall be required in connection with a policy renewal if:

(a) Personal information is collected only from the policyholder or from public records; or

(b) A notice meeting the requirements of this section has been given within the previous twenty-four (24) months; or

COMMENT: 24 months seems like a long period of time?

ACLI: Elimination of exemption for annual notice if notice has been given in past 24-months – No, we disagree to any changes to this provision

(3) In the case of a policy reinstatement or change in insurance benefits, a notice shall be provided ~~no later~~ thanby the time a request for a policy reinstatement or change in insurance benefits is received by the insurance institution, except that no notice shall be required if personal information is collected only from the policyholder or from public records.

B. The notice required by Subsection A above shall be in writing and shall state:

COMMENT: this section needs updating, *i.e.,* needs to overtly state, in order to clarify that simply referencing a report or scoring model from an insurance support organization does not adequately satisfy disclosure of "sources" of information.

ACLI: Disclosure of sources of information – Flag for discussion later

(1) Whether personal information may be collected from persons other than the individual or individuals proposed for coverage;

(2) The types of personal information that may be collected and the ~~types of~~ sources and investigative techniques that may be used to collect such information;

COMMENT: this requirement [B(2)] needs a great deal more emphasis in any notice.

ACLI: Flag for discussion later

(3) The types of consumer data that institutional sources may utilize to supply personal information pursuant to Subsection B(2), including but not limited to:
a. Social Media Activity
b. Web Traffic or Search Data
c. Geo-Location Information
d. Satellite Imagery
e. Consumer Purchasing/Subscription History
f. Cell Phone Application Activity Data
g. Genetic Genealogy Information

COMMENT: all of the elements listed in (3) above need discussion and updating. We need to refine this list to contain those data types most pertinent {and relevant} to insurance consumers and insurance companies.

ACLI: Flag for discussion later

(4) The ~~types of~~ disclosures identified in Subsections B, C, D, E, F, I, K, L and N of Section 13 of this Act and the circumstances under which such disclosures may be made without prior authorization; provided, however, only those circumstances need be described which occur with such frequency as to indicate a general business practice;

COMMENT: this provision needs to be discussed and then streamlined Not particularly user friendly with all the subsection references. Too much cross-referencing.

ACLI: Flag for discussion later

(5) A description of the rights established under Sections 8 and 9 of this Act and the manner in which such rights may be exercised; and

(6) That information obtained from a report prepared by an insurance support organization may be retained by the insurance support organization and disclosed to other persons.

COMMENT: provision (6) needs to be discussed; what does "disclosed to other persons" entail?

ACLI: Flag for discussion later

(7) Clear and concise notice as to how a consumer can restrict the use and/or disclosure of any of their information

COMMENT: we would like to add something like (7) above; CCPA and GDPR requirements.

ACLI: Flag for discussion later

C. In lieu of the notice prescribed in Subsection B, the insurance institution or agent may provide an abbreviated notice informing the applicant or policyholder that:

COMMENT: we suggest that a full notice be required at least at policy inception, if not at some longer interval, *e.g.*, every 5 years.

ACLI: No, we disagree with changes to this provision

(1) Personal information may be collected from persons other than the individual or individuals proposed for coverage;

(2) Such information as well as other personal or privileged information subsequently collected by the insurance institution or agent may in certain circumstances be disclosed to third parties without authorization;

COMMENT: a lot more focus is needed on this provision; discussion item

(3) A right of access and correction existsregarding ~~with respect to~~ all personal information collected; and

(4) The notice prescribed in Subsection B will be furnished to the applicant or policyholder upon request.

D. The obligations imposed by this section upon an insurance institution or agent may be satisfied by another insurance institution or agent authorized to act on its behalf.

COMMENTS:

- We suggest deleting paragraph D above.
- The notice requirements in the Model need to be modernized.

ACLI: Flag for further discussion

- We need to address electronic notices and not just written ones.

ACLI: Flag for further discussion

- The current requirements read more as a simple 'notice' and not consent to collect and use. Shouldn't it be the latter?

ACLI: No, we disagree

- Upon renewal, should the notice be required to be sent to the policyholder if there have been any changes in the types of information collected or other changes in the collection, use or disclosure of the personal information?

ACLI: Flag for further discussion

- The notice should/must include a statement as to the specific purposes for collecting the personal information and the intended use of the information.

ACLI: Flag for further discussion

- Should the provision allowing disclosure without prior authorization when not frequent enough to constitute a "general business practice" be amended?

ACLI: No, we disagree with changes to this provision

- Should we eliminate the abbreviated notice? We could consolidate these provisions into a single comprehensive notice. The abbreviated notice seems out-of-step with today's information collection and usage practices. For example, the disclosure of information to third parties without any authorization. This provision, as written, seems to put the onus on the policyholder to request information in the expanded notice. Shouldn't this comment be integrated into comment under C. on prior page?

ACLI: No, we disagree with the elimination of this provision

We need to discuss the interplay between the notice and the disclosure authorization form?

ACLI: No, we disagree with changes to this provision

Drafting Note: If permitted under Section 4A, an insurance institution or agent may include the notice in the insurance policy or certificate.

Section 5. Marketing and Research Surveys

An insurance institution or agent shall clearly specify those questions designed to obtain information solely for marketing or research purposes from an individual in connection with an insurance transaction.

COMMENT: we need to ensure we cover how GDPR and CCPA specifically address marketing usage.

ACLI: Flag for further discussion

Section 6. Content of Disclosure Authorization Forms [Specific categories of personal information. Business purpose for collecting information. Categories of third parties with whom data is shared and for what purpose.

ACLI: Flag for further discussion

COMMENTS:

- We need to examine the need for re-use and re-disclosure of information to third parties.
- Do state insurance regulators review and approve the Disclosure Authorization Forms? When is the latter provided to the insured?

ACLI: No, we disagree

MPL: **Disagree** with requiring covered entities to seek approval of Disclosure AuthorizationForms from state insurance regulators.

- Regarding Model #670 – it allows the disclosure of information for marketing purposes using opt-out. We would prefer seeing this written as an opt-in option. The section describing this form is consistent with an "opt-out" posture regarding marketing disclosures, consistent with Section 13(K). More consumer protection is provided by an "opt-in" posture, which is consistent with GDPR.

ACLI: No, we disagree

MPL: **Disagree** with recommendation to adopt an "opt in" posture for marketing disclosures.

Notwithstanding any other provision of law of this state, no insurance institution, agent or insurance support organization may utilize as its disclosure authorization form in connection with insurance transactions a form or statement which authorizes the disclosure of personal or privileged information about an individual to the insurance institution, agent or insurance support organization unless the form or statement:

A. Is written in plain language;

B. Is dated;

C. Specifies the ~~types of~~ persons authorized to disclose information about the individual;

D. Specifies the nature of the information authorized to be disclosed;

E. Names the insurance institution or agent and identifies by generic reference representatives of the insurance institution to whom the individual is authorizing information to be disclosed;

F. Specifies the purposes for which the information is collected;

COMMENTS:

- This sentence says "collected" but should it be "disclosed"?

ACLI: No, we disagree

- Perhaps this provision should refer back to the categories specified in Section 13? Consistent with GDPR practices, we may want to specify that the form must be "granular" with respect to disclosure purposes, *i.e.*, allow the insured to consent to disclosure for purposes of servicing the policy, while withholding consent for marketing disclosures.

ACLI: No, we disagree

G. Specifies the length of time such authorization shall remain valid, which shall be no longer than:

(1) In the case of authorizations signed for the purpose of collecting information in connection with an application for an insurance policy, a policy reinstatement or a request for change in policy benefits:

(a) Thirty (30) months from the date the authorization is signed if the application or request involves life, health or disability insurance;

(b) One (1) year from the date the authorization is signed if the application or request involves property or casualty insurance;

COMMENT: timeframes seem lengthy?

ACLI: No, we disagree with changing timeframes.

(2) In the case of authorizations signed for the purpose of collecting information in connection with a claim for benefits under an insurance policy,

(a) The term of coverage of the policy if the claim is for a health insurance benefit;

(b) The duration of the claim if the claim is not for a health insurance benefit; and

H. Advises the individual or a person authorized to act on behalf of the individual that the individual or the individual's authorized representative may ~~is entitled to~~ receive a copy of the authorization form.

Drafting Note: The standard established by this section for disclosure authorization forms should ~~is intended to~~ supersede any existing requirements a state may have adopted even if such requirements are more specific or applicable to particular authorizations such as medical information authorizations. This section is intended to be the exclusive statutory standard for all authorization forms utilized by insurance institutions, agents or insurance support organizations. This section does not preclude the inclusion of a disclosure authorization in an application form nor invalidate any disclosure authorizations in effect before ~~prior to~~ the effective date of this Act. Nor does this section preclude an insurance institution, agent or insurance support organization from obtaining, besides ~~in addition to~~ its own authorization form which complies with this section, an additional authorization form required by the person from whom disclosure is sought.

COMMENT: this drafting note needs greater prominence, perhaps made as a stand alone item

ACLI: No, we disagree

MPL: **Agree** that drafting note should be more prominent so as to highlight supremacy of thisact over all other state data privacy requirements applicable to insurers.

Section 7. Investigative Consumer Reports

A. No insurance institution, agent or insurance support organization may prepare or request an investigative consumer report about an individual in connection with an insurance transaction involving an application for insurance, a policy renewal, a policy reinstatement or a change in insurance benefits unless the insurance institution or agent informs the individual:

(1) That he or she may request to be interviewed in connection with the preparation of the investigative consumer report; and

(2) That upon a request under ~~pursuant to~~ Section 8, he or she may ~~is entitled to~~ receive a copy of the investigative consumer report.

B. If an investigative consumer report is to be prepared by an insurance institution or agent, the insurance institution or agent shall institute reasonable procedures to conduct a personal interview requested by an individual.

C. If an investigative consumer report is to be prepared by an insurance support organization, the insurance institution or agent desiring such report shall inform the insurance support organization whether a personal interview has been requested by the individual. ~~The insurance support organization shall institute reasonable procedures to conduct such interviews, if requested.~~

COMMENT: Section 7 needs a lot of discussion. Also, the last sentence of C. needs clarification. There should not be an *option* to have reasonable procedures.

ACLI: Flag for discussion

Section 8. Access to Recorded Personal Information

A. If any individual, after proper identification, submits a written request to an insurance institution, agent or insurance support organization for access to recorded personal information about the individual ~~which is~~ reasonably described by the individual and reasonably locatable and retrievable by the insurance institution, agent or insurance support organization, the insurance institution, agent or insurance support organization shall within thirty (30) business days from the date such request is received:

(1) Inform the individual of the nature and substance of such recorded personal information in writing, by telephone or by other ~~oral~~ communication, whichever the insurance institution, agent or insurance support organization prefers;

COMMENT: we need to discuss the term "recorded information." Also, for the last clause, this should be a required method and not a preference.

ACLI: The terminology and concepts in Section 8 are antiquated. Regulators have identified many areas related to electronic communication and records that may need to be addressed – Flag for further discussion

MPL: Flag for discussion - **A.** The term *recorded personal information* should be updated, perhaps by using more updated terminology such as *protected personal information.*

(2) Permit the individual to see and copy~~, in person,~~ such recorded personal information pertaining to him or her or to obtain a copy of such recorded personal information by mail, whichever the individual prefers, unless such recorded personal information is in coded form, in which case an accurate translation in plain language shall be provided in writing;

COMMENT: this should be updated to include right of access by electronic means, *e.g.,*e-mail. However, we should also think about means to limit inadvertent or improper electronic disclosures.

ATLA: **Section 8: (A)(1&2)** To prevent fraud and provide consumer protection from potential harm, the requirement to provide a copy of personal information should be limited as described in CCPA's draft regulations (entity should never provide full SSN, bank account number, etc., upon request).

(3) Disclose to the individual the identity, if recorded, of those persons to whom the insurance institution, agent or insurance support organization has disclosed such personal information within two (2) years before ~~prior to~~ such request, and if the identity is not recorded, the names of those insurance institutions, agents, insurance support organizations or other persons to whom such information is normally disclosed; and

ATLA: Section 8: **(A)(3)** There needs to be an exception to this requirement where the entity has been instructed by law enforcement or court order not to disclose that the information was shared

(4) Provide the individual with a summary of the procedures by which he or she may request correction, amendment or deletion of recorded personal information.

COMMENT: if the term "recorded" is not deleted in this section then we need to ensure the definition includes all types of data/information.

B. Any personal information provided under ~~pursuant to~~ Subsection A above shall identify the source of the information ~~if such source is an institutional source~~.

MPL: Flag for discussion - **C-G.** The number and nature of comments suggest a thorough vetting of this section is necessary.

C. Medical-record information supplied by a medical care institution or medical professional and requested under Subsection A, together with the identity of the medical professional or medical care institution which provided such information, shall be supplied either directly to the individual or to a medical professional designated by the individual and licensed to provide medical care regarding ~~with respect to~~ the condition to which the information relates, whichever the insurance institution, agent or insurance support organization prefers. If it elects to disclose the information to a medical professional designated by the individual, the insurance institution, agent or insurance support organization shall notify the individual, at the time of the disclosure, that it has informed ~~provided the information to~~ the medical professional.

COMMENT: we must review current EHR requirements; there needs to be a more streamlined definition.

D. Except for personal information provided under Section 10, an insurance institution, agent or insurance support organization may charge a reasonable fee to cover the costs incurred in providing a copy of recorded personal information to individuals.

COMMENT: discuss; the company has already requested and obtained the information of their own volition. Why should the consumer be charged? Check CCPA/GDPR.

ACLI: Flag for discussion

E. The obligations imposed by this section upon an insurance institution or agent may be satisfied by another insurance institution or agent authorized to act on its behalf. Regarding ~~With respect to~~ the copying and disclosure of recorded personal information pursuant to a request under Subsection A, an insurance institution, agent or insurance support organization may arrange ~~make arrangements~~ with an insurance support organization or a consumer reporting agency to copy and disclose recorded personal information on its behalf.

COMMENT: What is the purpose of this provision?

F. The rights granted to individuals in this section shall extend to all natural persons to the extent information about them is [used], collected and maintained by an insurance institution, agent or insurance support organization in connection with an insurance transaction. The rights granted to all natural persons by this subsection shall not extend to information about them that relates to and is collected in connection with or in reasonable anticipation of a claim or civil or criminal proceeding involving them.

COMMENT: we need to compare the last sentence to the definitions from anti-fraud.

G. For purposes of this section, the term "insurance support organization" does not include "consumer reporting agency" except to the extent this section imposes more stringent requirements on a consumer reporting agency than other state or federal law.

COMMENTS:

- Any and all third party vendors, InsurTechs, TPAs, etc., need to be included in this act.

ACLI: Flag for discussion

CDIA: There are comments calling for “any and all third-party vendors, InsurTechs, TPAs, etc., need to be included in this act” in Section 8 (specifically page 17) relating to access to recorded personal information. We cannot speak for other third-party vendors or the newer “Insurtechs” that have entered the marketplace since 1992 when Model Act #670 was implemented. However, CRAs and their products, most notably Credit Based Insurance Scores, are already heavily regulated at the federal level. CRAs and the personal information they have on consumers are already heavily regulated under the FCRA, Gramm-Leach-Bliley

Act (GLBA), Drivers Privacy Protection Act (DPPA) and others. For example, 15 U.S. Code § 1681g. of the FCRA specifically already regulates how CRAs disclose information to individual consumers. Additionally, the FCRA defines the permissible purposes of consumer reports under 15 U.S. Code § 1681b. This section regulates the who, when and why around parties that can access consumer reports and the information in those reports.

- A lot of discussion needed about the definitions.
- Data Management. This could include the right to delete, correct and access. That is, the right to be forgotten, right to data portability and right to access data (nondiscrimination). Also, opt-in v. opt-out.
- Usage. For what purpose can the data be used? Legitimate purpose (like GDPR)? Data vendor products (public info used to establish consumer profiles?
- Data Access. What is meant by "recorded" personal information? If it is referring to all personal information we think the term "recorded" could be dropped? Shouldn't the rights provided here be applied more broadly to all personal information held by insurance institutions, agents or ISOs? Should this definition include "electronic" as a means to inform the individual? Should we drop the "in-person" requirement to view and copy this information. The consumer should be able to do so electronically, where feasible. If this recorded information is a subset of personal information held, then extend same amended updates to data more generally. This includes the right to correct, amend or delete information.

Section 9. Correction, Amendment or Deletion of Recorded Personal Information

A. Within thirty (30) business days from ~~the date of~~ receipt of a written request from an individual to correct, amend or delete any recorded personal information about the individual within its possession, an insurance institution, agent or insurance support organization shall either:

(1) Correct, amend or delete the portion of the recorded personal information in dispute; or

(2) Notify the individual of:

(a) Its refusal to make such correction, amendment or deletion;

There needs to be more accountability for an insurer's refusal to correct or delete information. The CCPA approach, per CIV 1798.105, is to specify grounds upon which correction/deletion may be refused, and require that any refusal state the grounds for that refusal.

ACLI: Addition of CCPA-type parameters (§1798.105) for denial of a deletion request – Flag for further discussion

CDIA: Section 9 (specifically pages 19-20) relating to correction, amendment or deletion of recorded personal information contains a comment concerning a "need to update the rights and processes". This another area where we would like to highlight examples of CRAs and the right to correct, amend or delete information already being regulated under federal law. Under the FCRA 15 U.S. Code § 1681c. there are requirements relating to information contained in consumer reports. The FCRA also contains other sections relating to correcting, amending and deleting information in consumer reports, which usually stems from a consumer dispute regarding information contained in a report.

(b) The reasons for the refusal, and

(c) The individual's right to file a statement as provided in Subsection C.

COMMENT: we need to discuss the 'right to be forgotten' provision and similar requirements.

ACLI: Addition of 'right to be forgotten' – Flag for further discussion

MPL: **(A)(2)(b). Disagree** as the notification requirements in the model are sufficient.
- **A. Disagree** that a *right to be forgotten* provision is necessary. MPL insurers need to retain personal information for legitimate business practices and legal purposes. Given the "long-tail" nature of MPL insurance, our member companies are required to store long-term underwriting, claims, and risk management information. Additionally, several states have laws on the books that require insurance companies to retain information for a certain number of years.

B. If the insurance institution, agent or insurance support organization corrects, amends or deletes recorded personal information under ~~in accordance with~~ Subsection A(1) above, the insurance institution, agent or insurance support organization shall so notify the individual in writing and furnish the correction, amendment or fact of deletion to:

(1) Any person specifically designated by the individual who may have, within the preceding two (2) years, received such recorded personal information;

COMMENT: we need to discuss whether or not the onus is on the "entitiy" to inform anyone they may have released the incorrect information to – it is not the consumer's responsibility to correct this.

(2) Any insurance support organization whose primary source of personal information is insurance institutions if the insurance support organization has ~~systematically~~ received such ~~recorded~~ personal information from the insurance institution within the preceding seven (7) years; provided, however, that the correction, amendment or fact of deletion need not be furnished if the insurance support organization no longer maintains recorded personal information about the individual; and

COMMENT: but what if the 2ndary entity that was sent the information still has the incorrect info? Whether or not the original entity still maintains the information is immaterial.

(3) Any insurance support organization that furnished the personal information that has been corrected, amended or deleted.

C. Whenever an individual disagrees with an insurance institution's, agent's or insurance support organization's refusal to correct, amend or delete recorded personal information, the individual shall be permitted to file with the insurance institution, agent or insurance support organization:

(1) A concise statement setting forth what the individual thinks is the correct, relevant or fair information; and

(2) A concise statement of the reasons why the individual disagrees with the insurance institution's, agent's or insurance support organization's refusal to correct, amend or delete recorded personal information.

D. ~~In the event~~ If an individual files either statement as described in Subsection C above, the insurance institution, agent or insurance support organizations shall:

(1) File the statement with the disputed personal information and provide a means by which anyone reviewing the disputed personal information will be [provided] ~~made aware of~~ the individual's statement ~~and have access to it~~; and

COMMENT: review language from FCRA

CDIA: Section 9 subsections C and D pertain to how consumers may dispute information with "insurance support organizations", which a CRA would fall under the current definition of. There is also a comment asking to "review language from FCRA". The FCRA already dictates how an individual may obtain information a CRA may have on that individual such that the portion of subsection F that states, "except to the extent that section imposes more stringent requirements on a consumer reporting agency than other state or federal law," should be deleted for the previously mentioned reasons.

(2) In any subsequent disclosure by the insurance institution, agent or support organization of the recorded personal information that is the subject of disagreement, clearly identify the matter or matters in dispute and provide the individual's statement along with the recorded personal information being disclosed; and

COMMENT: should the ongoing disclosure of disputed information be allowed? Restricted?

(3) Furnish the statement to the persons and in the manner specified in Subsection B above.

E. The rights granted to individuals in this section shall extend to all natural persons to the extent information about them is collected and maintained by an insurance institution, agent or insurance support organization in connection with an insurance transaction. The rights granted to all natural persons by this subsection shall not extend to information about them that relates to and is collected in connection with or in reasonable anticipation of a claim or civil or criminal proceeding involving them.

COMMENT: we need to discuss the last sentence above – "The rights granted … involving them.

F. For ~~purposes of~~ this section, the term "insurance support organization" does not include "consumer reporting agency" except if ~~to the extent that~~ this section imposes more stringent requirements on a consumer reporting agency than other state or federal law.

COMMENTS:

- Right to Correct and/or Delete Information. Need to update the rights and processes.

ACLI: Responsibility for correcting incorrect information – Flag for further discussion

- New Types of Data: the model needs to cover new types of data, *e.g.,* data produced through telematics programs, such as wearable devices, data collection in vehicles, ways we are just learning about.

- Conflicts. Conflicting state laws and conflicting provisions in generally applicable privacy laws. How should or can the Model integrate into existing federal and state privacy regimes, whether applicable industry-wide or specific to the insurance market? How can the Model dovetail with these other acts? It should be noted that the GDPR and the CCPA apply to all sectors, whereas our Model pertains only to the insurance sector.

MPL: **General.** Agree that this model law and its provisions should not conflict with federal and state laws related to data privacy.

- Operational functions to preserve and facilitate – need to review §13 of Model #672.

- What about provisions especially applicable to minors?

ACLI: Inclusion of minors – Flag for further discussion

Section 10. Reasons for Adverse Underwriting Decisions

A. ~~In the event of~~ If an adverse underwriting decision occurs the insurance institution or agent responsible for the decision shall:

(1) Either provide the applicant, policyholder or individual proposed for coverage with the specific reason or reasons for the adverse underwriting decision in writing or advise such person that upon written request he or she may receive the specific reason or reasons in writing; and

(2) Provide the applicant, policyholder or individual proposed for coverage with a summary of the rights established under Subsection B and Sections 8 and 9 of this Act.

COMMENT: the normal standard is "…clear and concise without the need for further inquiry."

B. Upon receipt of a written request within ninety (90) business days from ~~the date of~~ the mailing of notice or other communication of an adverse underwriting decision to an applicant, policyholder or individual proposed for coverage, the insurance institution or agent shall furnish to such person within twenty-one (21) business days from ~~the date of~~ receipt of such written request:

COMMENT: review the timeframes, they seem too lengthy

(1) The specific reason or reasons for the adverse underwriting decision, in writing, if such information was not initially furnished in writing under ~~pursuant to~~ Subsection A(1);

(2) The specific items of personal and privileged information that support those reasons; provided, however:

(a) The insurance institution or agent shall not be required to furnish specific items of privileged information if it has a reasonable suspicion, based upon specific information available for review by the Commissioner, that the applicant, policyholder or individual proposed for coverage has engaged in criminal activity, fraud, material misrepresentation or material nondisclosure, and

(b) Specific items of medical-record information supplied by a medical care institution or medical professional shall be disclosed either directly to the individual about whom the information relates or to a medical professional designated by the individual and licensed to provide medical care regarding ~~with respect to~~ the condition to which the information relates, whichever the insurance institution or agent prefers, and

COMMENT: this provision needs to track with HIPAA; there is no preference allowed, the entity must have an actual practice/procedure/protocol.

Drafting Note: The exception in Section 10B(2)(a) to the obligation of an insurance institution or agent to furnish the specific items of personal and privileged information that support the reasons for an adverse underwriting decision extends only to information about criminal activity, fraud, material misrepresentation or material nondisclosure that is privileged information and not to all information.

(3) The names and addresses of the institutional sources that supplied the specific items of information under ~~pursuant to~~ Subsection B(2); provided, however, that the identity of any medical professional or medical care institution shall be disclosed either directly to the individual or to the designated medical professional, whichever the insurance institution or agent prefers.

COMMENTS:

- This provision needs to track with HIPAA; there is no preference allowed, the entity must have an actual practice/procedure/protocol. Also, this section needs to be updated in order to clarify that simply referencing a report or risk scoring model does not adequately meet the requirements of this disclosure.
- Institutional Sources is defined earlier as "any person or governmental entity that provides information about an individual to an agent, insurance institution or insurance support organization." We would like to see an update here which requires disclosure of the categories of consumer information from which the institutional source drew.
- The list of elements below in (4) needs to be refined to show the data types most pertinent to the insurance consumer and the insurance company.

(4) The types of consumer data that institutional sources utilized to supply the specific items of information pursuant to Subsection B(2), including but not limited to:

a. Social Media Activity
b. Web Traffic or Search Data
c. Geo-Location Information
d. Satellite Imagery
e. Consumer Purchasing/Subscription History
f. Cell Phone Application Activity Data
g. Genetic Genealogy Information

C. The obligations imposed by this section upon an insurance institution or agent may be satisfied by another insurance institution or agent authorized to act on its behalf.

D. When an adverse underwriting decision results solely from an oral request or inquiry, the explanation of reasons and summary of rights required by Subsection A may be given orally.

COMMENT: regarding paragraph D above - nothing should be allowed orally b/c it cannot be recreated or tested. Both paragraph C and D above need a lot of discussion.

Section 11. Information Concerning Previous Adverse Underwriting Decisions

COMMENT: does Section 11 really belong in this act? It needs a rewrite but we think it better belongs in another model law, perhaps UTPA since it does not allow using previously cancelled or nonrenewed activities as a basis for an underwriting action.

No insurance institution, agent or insurance support organization may seek information in connection with an insurance transaction about ~~concerning~~:

A. Any previous adverse underwriting decision experienced by an individual; or

B. Any previous insurance coverage obtained by an individual through a residual market mechanism, unless such inquiry also requests the reasons for any previous adverse underwriting decision or the reasons ~~why~~ insurance coverage was ~~previously~~ obtained through a residual market mechanism.

Section 12. Previous Adverse Underwriting Decisions

COMMENT: does Section 12 really belong in this act? It needs a reqrite but we think it better belongs in another model law, perhaps UTPA.

No insurance institution or agent may base an adverse underwriting decision in whole or in part:

A. On the fact of a previous adverse underwriting decision or on the fact that an individual previously obtained insurance coverage through a residual market mechanism; provided, however, an insurance institution or agent may base an adverse underwriting decision on further information obtained from an insurance institution or agent responsible for a previous adverse underwriting decision;

COMMENT: the term 'further' is too vague. The standard is you cannot restrict/impact coverage b/c of a previous cancellation or nonrenewal. The company is suppose to conduct its own underwriting. See UTPA.

B. On personal information received from an insurance support organization whose primary source of information is insurance institutions; provided, however, an insurance institution or agent may base an adverse underwriting decision on further personal information obtained because ~~as a result~~ of information received from such insurance support organization.

Section 13. Disclosure Limitations and Conditions

An insurance institution, agent or insurance support organization shall not disclose any personal or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure is:

A. With the written authorization of the individual, provided:

(1) If such authorization is submitted by another insurance institution, agent or insurance support organization, the authorization meets the requirements of Section 6 of this Act; or

COMMENT: it is not clear that A(1) above is needed or even correct.

(2) If such authorization is submitted by a person other than an insurance institution, agent or insurance support organization, the authorization is:

(a) Dated;

(b) Signed by the individual; and

(c) Obtained one (1) year or less before ~~prior to~~ the date a disclosure is sought under ~~pursuant to~~ this subsection; or

B. To a person other than an insurance institution, agent or insurance support organization, provided such disclosure is ~~reasonably necessary~~:

COMMENT: all of paragraph 13B needs discussion and a rewrite

(1) To enable such person to perform a business, professional or insurance function for the disclosing insurance institution, agent or insurance support organization and such person agrees not to disclose the information further without the individual's written authorization unless the further disclosure:

(a) Would otherwise be permitted by this section if made by an insurance institution, agent or insurance support organization; or

(b) Is reasonably necessary for such person to perform its function for the disclosing insurance institution, agent or insurance support organization; or

(2) To enable such person to inform ~~provide information to~~ the disclosing insurance institution, agent or insurance support organization for ~~the purpose of~~:

(a) Determining an individual's eligibility for an insurance benefit or payment; or

(b) Detecting or preventing criminal activity, fraud, material misrepresentation or material nondisclosure in connection with an insurance transaction; or

C. To an insurance institution, agent, insurance support organization, or self-insurer, provided the information disclosed is limited to that which is reasonably necessary:

COMMENT: "reasonably necessary" is too vague, not defined; need a standard of practice

(1) To detect or prevent criminal activity, fraud, material misrepresentation or material nondisclosure in connection with insurance transactions; or

(2) For either the disclosing or receiving insurance institution, agent or insurance support organization to perform its function in connection with an insurance transaction involving the individual; or

COMMENT: it is not clear what "perform its function in connection" means?

D. To a medical care institution or medical professional for the purpose of:

(1) Verifying insurance coverage or benefits;

(2) Informing an individual of a medical problem of which the individual may not be aware; or

COMMENT: HIPAA concerns, among others

(3) Conducting an operations or services audit to verify the individuals treated by the medical professional or at the medical care institution; provided only such information is disclosed as is reasonably necessary to accomplish the foregoing purposes; or

COMMENT: No; (3) above needs discussion and a rewrite

E. To an insurance regulatory authority; or

F. To a law enforcement or other governmental authority:

(1) To protect the interests of the insurance institution, agent or insurance support organization in preventing or prosecuting the perpetration of fraud upon it; or

(2) If the insurance institution, agent or insurance support organization reasonably believes that illegal activities have been conducted by the individual; or

COMMENT: we need to review anti-fraud requirements; draft clearer language

G. Otherwise permitted or required by law; or

H. In response to a ~~facially~~valid administrative or judicial order, including a search warrant or subpoena; or

I. ~~Made for the purpose of conducting~~To conduct actuarial or research studies, provided:

(1) No individual may be identified in any actuarial or research report;

(2) Materials allowing the individual to be identified are returned or destroyed as soon as they are no longer needed; and

COMMENT: specific record retention and document, data and information destruction rules exist. Do we need to include a reference [or drafting note] here?

(3) The actuarial or research organization agrees not to disclose the information unless the disclosure would otherwise be permitted by this section if made by an insurance institution, agent or insurance support organization; or

COMMENT: CCPA & GDPR focus

J. To a party or representative of a party to a proposed or consummated sale, transfer, merger or consolidation of all or part of the business of the insurance institution, agent or insurance support organization, provided:

(1) ~~Prior to~~ Before the consummation of the sale, transfer, merger or consolidation only such information is disclosed as is reasonably necessary to enable the recipient to make business decisions about the purchase, transfer, merger or consolidation; and

COMMENT: discuss the ability to specifically exclude marketing; we need a definition of "reasonably necessary;" we need to ensure current business practices are accurately defined in K, L and M.

(2) The recipient agrees not to disclose the information unless the disclosure would otherwise be permitted by this section if made by an insurance institution, agent or insurance support organization; or

K. To a person whose only use of such information will be in connection with the marketing of a product or service, provided:

(1) No medical record information, privileged information or personal information relating to an individual's character, personal habits, mode of living or general reputation is disclosed, and no classification derived from such information is disclosed;

(2) The individual has been given an opportunity to indicate that he or she does not want personal information disclosed for marketing purposes and has given no indication that he or she does not want the information disclosed; and [given no indication]

(3) The person receiving such information agrees not to use it except in connection with the marketing of a product or service; or

COMMENT: we need to discuss an opt-in provision instead of opt-out provision; we also need to discuss restrictions against marketing purposes.

L. To an affiliate whose only use of the information will be in connection with an audit of the insurance institution or agent or the marketing of an insurance product or service, provided the affiliate agrees not to disclose the information for any other purpose or to unaffiliated persons; or

COMMENT: it is not clear why an affiliate needs any of the data/info? Disclosure requirements should not vary among companies.

M. By a consumer reporting agency, provided the disclosure is to a person other than an insurance institution or agent; or

N. To a group policyholder to report ~~for the purpose of reporting~~ claims experience or conducting an audit of the insurance institution's or agent's operations or services, provided the information disclosed is reasonably necessary for the group policyholder to conduct the review or audit; or

COMMENT: we need to add a definition of "reasonably necessary" and the protocols for making such a determination.

O. To a professional peer review organization to review ~~for the purpose of reviewing~~ the service or conduct of a medical care institution or medical professional; or

P. To a governmental authority to determine ~~for the purpose of determining~~ the individual's eligibility for health benefits for which the governmental authority may be liable; or

Q. To a certificateholder or policyholder to provide ~~for the purpose of providing~~ information regarding the status of an insurance transaction; or

R. To a lienholder, mortgagee, assignee, lessor or other person shown on the records of an insurance institution or agent as having a legal or beneficial interest in a policy of insurance, provided that:

(1) No medical record information is disclosed unless the disclosure would otherwise be permitted by this section; and

(2) The information disclosed is limited to that which is reasonably necessary to permit such person to protect its interests in such policy.

COMMENT: we need to add a definition of "reasonably necessary" and the protocols for making such a determination.

COMMENT: There needs to be a provision which prevents discrimination against consumers who exercise their rights to privacy. This should be its own section. Compare the CCPA at CIV 1798.125. Note that, while CCPA permits "incentive programs," it doesn't appear that "incentives" are consistent with the requirement that insurance premiums are based on rating data.

Section 14. Power of Commissioner

COMMENT: we need to ask NAIC Legal Staff to review this section. We need to ensure all definitions from Section 2 are consistent with the rest of this document and that they accurately capture the business practices of today.

A. The Commissioner shall have power to examine and investigate into the affairs of every insurance institution or agent [or third party vendor] doing business in this state to determine whether the insurance institution or agent [or vendor] has been or is engaged in any conduct in violation of this Act. The Commissioner shall have power to examine and investigate into the affairs of any Licensee to determine whether the Licensee has been or is engaged in any conduct in violation of this Act. This power is in addition to the powers which the Commissioner has under [insert applicable statutes governing the investigation or examination of insurers]. Any such investigation or examination shall be conducted pursuant to [insert applicable statutes governing the investigation or examination of insurers]. (From 668-IDSM)

COMMENT: do we need to add "third party vendor"? It does need to be understood that the requirements of a company are also applicable to a 3pv.

B. The Commissioner shall have the power to examine and investigate into the affairs of every insurance support organization acting on behalf of an insurance institution or agent which either transacts business in this state or transacts business outside this state with ~~that has~~ an effect on a person residing in this state ~~in order~~ to determine whether such insurance support organization has been or is engaged in any conduct in violation of this Act. Whenever the Commissioner has reason to believe that a Licensee has been or is

engaged in conduct in this State which violates this Act, the Commissioner may take action that is necessary or appropriate to enforce the provisions of this Act. (From 668-IDSM)

COMMENT: we need to ensure definition includes third party vendors. If so, can we collapse paragraphs A and B into one?

Section 15. Hearings, Witnesses, Appearances, Production of Books and Service of Process

COMMENT: we need to ask NAIC Legal Staff to streamline/compare this language to recent models.

A. Whenever the Commissioner has reason to believe that an insurance institution, agent or insurance support organization has been or is engaged in conduct in this state which violates this Act, or if the Commissioner believes that an insurance support organization has been or is engaged in conduct outside this state which ~~has an effect on~~ affects a person residing in this state and which violates this Act, the Commissioner shall issue and serve upon such insurance institution, agent or insurance support organization a statement of charges and notice of hearing to be held at a time and place fixed in the notice. The date for such hearing shall be not less than [insert number] days after ~~the date of~~ service.

B. At the time and place fixed for such hearing the insurance institution, agent or insurance support organization charged can ~~shall have an opportunity to~~ answer the charges against it and present evidence on its behalf. Upon good cause shown, the Commissioner shall permit any adversely affected person to intervene, appear and be heard ~~at such hearing~~ by counsel or in person.

D. At any hearing under ~~conducted pursuant to~~ this section the Commissioner may administer oaths, examine and cross-examine witnesses and receive oral and documentary evidence. The Commissioner shall have the power to subpoena witnesses, compel their attendance and require the production of books, papers, records, correspondence and other documents ~~which are~~ relevant to the hearing. A stenographic record of the hearing shall be made upon the request of any party or at the discretion of the Commissioner. If no stenographic record is made and if judicial review is sought, the Commissioner shall prepare a statement of the evidence for use on the review. Hearings conducted under this section shall be governed by the same rules of evidence and procedure applicable to administrative proceedings conducted under the laws of this state.

COMMENT: we need to draft an updated definition of "data and related information" and ensure it is not just limited to documents.

D. Statements of charges, notices, orders and other processes of the Commissioner under this Act may be served by anyone duly authorized to act on behalf of the Commissioner. Service of process may be completed in the manner provided by law for service of process in civil actions or by registered mail. A copy of the statement of charges, notice, order or other process shall be provided to the person or persons whose rights under this Act have been allegedly violated. A verified return setting forth the manner of service, or return postcard receipt with ~~in the case of~~ registered mail, shall be sufficient proof of service.

Section 16. Service of Process - Insurance Support Organizations

For ~~the purpose of~~ this Act, an insurance support organization transacting business outside this state which affects ~~has an effect on~~ a person residing in this state shall be deemed to have appointed the Commissioner to accept service of process on its behalf; provided the Commissioner causes a copy of such service to be mailed forthwith by registered mail to the insurance support organization at its last known principal place of business. The return postcard receipt for such mailing shall be sufficient proof that the same was properly mailed by the Commissioner.

COMMENT: does service have to be via mail? Can't we accept proof via e-service? Are there any UCC requirements for how a business entity is to receive notice? Can we streamline this language?

Section 17. Cease and Desist Orders and Reports

COMMENT: we need to ask NAIC Legal Staff to review.

A. If, after a hearing pursuant to Section 15, the Commissioner determines that the insurance institution, agent or insurance support organization charged has engaged in conduct or practices in violation of this Act, the Commissioner shall reduce his or her findings to writing and shall issue and cause to be served upon such insurance institution, agent or insurance support organization a copy of such findings and an order

requiring such insurance institution, agent or insurance support organization to cease and desist from the conduct or practices violating ~~constituting a violation of~~ this Act.

B. If, after a hearing under ~~pursuant to~~ Section 15, the Commissioner determines that the insurance institution, agent or insurance support organization charged has not engaged in conduct or practices in violation of this Act, the Commissioner shall prepare a written report which sets forth findings of fact and conclusions of law. Such report shall be served upon the insurance institution, agent or insurance support organization charged and upon the person or persons~~, if any,~~ whose rights under this Act were allegedly violated.

C. Until the expiration of the time allowed under Section 19 of this Act for filing a petition for review or until such petition is actually filed, whichever occurs first, the Commissioner may modify or set aside any order or report issued under this section. After the expiration of the time allowed under Section 19 of this Act for filing a petition for review, if no such petition has been duly filed, the Commissioner may, after notice and opportunity for hearing, alter, modify or set aside, in whole or in part, any order or report issued under this section whenever conditions of fact or law warrant such action or if the public interest so requires.

Section 18. Penalties

COMMENT: can we simplify this language? How about - NEW: In the case of a violation of this Act, a Licensee may be penalized in accordance with [insert general penalty statute]. Ask NAIC Legal Staff for input. We also need to review the dollar amounts for consistency with other models and resources documents? In the case of a violation of this Act, a Licensee may be penalized in accordance with [insert general penalty statute]. (From 668-IDSM)

A. In any case where a hearing pursuant to Section 15 results in the finding of a knowing violation of this Act, the Commissioner may, in addition to the issuance of a cease and desist order as prescribed in Section 17, order payment of a monetary penalty of not more than [$500] for each violation but not to exceed [$10,000] in the aggregate for multiple violations.

B. Any person who violates a cease and desist order of the Commissioner under Section 17 of this Act may, after notice and hearing and upon order of the Commissioner, be subject to one or more of the following penalties, at the discretion of the Commissioner:

(1) A monetary fine of not more than [$10,000] for each violation;

(2) A monetary fine of not more than [$50,000] if the Commissioner finds that violations have occurred with such frequency as to constitute a general business practice; or

(3) Suspension or revocation of an insurance institution's or agent's license.

Section 19. Judicial Review of Orders and Reports

COMMENT: we need to ask NAIC Legal Staff to review this section. Please note there are a few suggested changes.

A. Any person subject to an order of the Commissioner under Section 17 or Section 18 or any person whose rights under this Act were allegedly violated may obtain a review of any order or report of the Commissioner by filing in the [insert title] Court of [insert county] County, within [insert number] days from the date of the service of such order or report, a written petition requesting that the order or report of the Commissioner be set aside. A copy of such petition shall be simultaneously served upon the Commissioner, who shall forthwith certify and file in such court a transcript of the entire record of the proceeding causing ~~giving rise to~~ the order or report which is the subject of the petition. Upon filing of the petition and transcript the [insert title] Court shall have jurisdiction to make and enter a decree modifying, affirming or reversing any order or report of the Commissioner, in whole or in part. The findings of the Commissioner as to the facts supporting any order or report, if supported by clear and convincing evidence, shall be conclusive.

B. To the extent an order or report of the Commissioner is affirmed, the Court shall issue its own order commanding obedience to the terms of the order or report of the Commissioner. If any party affected by an order or report of the Commissioner shall apply to the court for leave to produce additional evidence and shall show to the satisfaction of the court that such additional evidence is material and that there are reasonable grounds for failing ~~the failure~~ to produce such evidence in prior proceedings, the court may order such additional evidence to be taken before the Commissioner in such manner and upon such terms ~~and conditions~~ as the court may deem proper. The Commissioner may modify his or her findings of fact or make new findings by reason of the additional evidence so taken and shall file such modified or new findings along with any recommendation~~, if any,~~ for the modification or revocation of a previous order or report. If supported by clear and convincing evidence, the modified or new findings shall be conclusive as to the matters contained therein.

C. An order or report issued by the Commissioner under Section 17 or 18 shall become final:

(1) Upon the expiration of the time allowed for ~~the~~ filing ~~of~~ a petition for review, if no such petition has been duly filed; except that the Commissioner may modify or set aside an order or report to the extent provided in Section 17C; or

(2) Upon a final decision of the [insert title] Court if the court directs that the order or report of the Commissioner be affirmed or the petition for review dismissed.

D. No order or report of the Commissioner under this Act or order of a court to enforce the same shall ~~in any way~~ relieve or absolve any person affected by such order or report from any liability under any law of this state.

Section 20. Individual Remedies

COMMENT: we need to discuss this section and compare it to CCPA & GDPR requirements. Should we prepare two drafts – one that has a private cause of action and one that does not? Do we want to mirror the requirements in CCPA & GDPR? Please also note that this section contains several suggested changes.

A. If any insurance institution, agent or insurance support organization violates ~~fails to comply with~~ Section 8, 9 or 10 of this Act regarding ~~with respect to~~ the rights granted under those sections, any person whose rights are violated may apply to the [insert title] Court of this state, or any other court of competent jurisdiction, for appropriate equitable relief.

B. An insurance institution, agent or insurance support organization which discloses information in violation of Section 13 of this Act shall be liable for damages sustained by the individual about whom the information relates; provided, however, that no individual may have ~~shall be entitled to~~ a monetary award which exceeds the actual damages sustained by the individual as a result of a violation of Section 13 of this Act.

C. In any action brought pursuant to this section, the court may award the cost ~~of the action~~ and reasonable attorney's fees to the prevailing party.

D. An action under this section must be brought within two (2) years from the date the alleged violation is or should have been discovered.

E. Except as specifically provided in this section, there shall be no remedy or recovery available to individuals, in law or in equity, for occurrences violating ~~constituting a violation of~~ any provisions of this Act.

Section 21. Immunity

COMMENT: we need to discuss this section and compare it to CCPA & GDPR requirements. Should we prepare two drafts – one that has a private cause of action and one that does not? Do we want to

mirror the requirements in CCPA & GDPR? Please also note that this section contains a few suggested changes.

No cause of action such as ~~in the nature of~~ defamation, invasion of privacy or negligence shall arise against any person for disclosing personal or privileged information under ~~in accordance with~~ this Act, nor shall such a cause of action arise against any person for furnishing personal or privileged information to an insurance institution, agent or insurance support organization~~;~~, provided, however, this section shall provide no immunity for disclosing or furnishing false information with malice or willful intent to injure any person.

Section 22. Obtaining Information Under False Pretenses

Any person who knowingly and willfully obtains information about an individual from an insurance institution, agent or insurance support organization under false pretenses shall be fined not more than [$10,000] or imprisoned for not more than one year, or both.

COMMENT: no changes are suggested at this time.

Section 23. Rules and Regulations [OPTIONAL]

The Commissioner may, in accordance with [the state statute setting forth the ability of the Department to adopt regulations] issue such regulations as shall be necessary to carry out the provisions of this Act.

Drafting Note: This provision is applicable only to states requiring this language. (From 668-IDSM)

Section 24. Severability

If any provisions of this Act or the application thereof to any person or circumstance is ~~for any reason~~ held to be invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected~~ thereby~~. If any provisions of this Act or the application thereof to any person or circumstance is for any reason held to be invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected thereby. (From 668-IDSM)

COMMENT: is the “for any reason” clause and “thereby” really needed?

Section 25. Effective Date

A. This Act shall take effect on [insert a date which allows at least a one year interval between the date of enactment and the effective date].

B. The rights granted under Sections 8, 9 and 13 of this Act shall take effect on [insert effective date] regardless of the date of the collection or receipt of the information which is the subject of such sections.

COMMENT: do we need to include a reference note in each section pertaining to the effective date?

This Act shall take effect on [insert a date]. Licensees shall have one year from the effective date of this Act to implement Section 4 of this Act and two years from the effective date of this Act to implement Section 4F of this Act. (From 668-IDSM)

Section 4. Information Security Program

COMMENT: include a Privacy Policy/Plan and Third-Party Service Provider Arrangements?

F. Oversight of Third-Party Service Provider Arrangements

(1) A Licensee shall exercise due diligence in selecting its Third-Party Service Provider; and

(2) A Licensee shall require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures to protect and secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider. (From 668-IDSM)

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

1980 Proc. I 34, 38, 281, 319, 320-335 (adopted).
1981 Proc. I 47, 51, 255, 259, 290-313 (revised and reprinted).
1982 Proc. I 19, 27, 155, 198 (amended).

This page is intentionally left blank