

## Insurance Data Security Model Law

[Proposed Revisions to Version 2 – for discussion on Dec. 20 Drafting Group Call]

### Section 2. Purpose and Intent

A. Notwithstanding any other provision of law including [insert reference to state’s general data security breach notification law], the purpose and intent of this Act is to establish the exclusive standards in this state for data security and investigation and notification of a data breach applicable to licensees, as defined in Section 3G.

B. It is not the intent of this Act to require that a licensee send notice to consumers affected by a data breach under Section 6D when notice has been or is being sent to consumers in accordance with a federal statute or regulation applicable to that licensee. It is also not the intent of this Act that a licensee be required to set up a separate information security program under Section 4 if that licensee has established and maintained an information security program in accordance a federal statute or regulation applicable to that licensee. If a licensee relies upon this provision it shall provide to the Commissioner upon request the specific federal statute or regulation upon which it relies and the manner in which it asserts compliance.

~~A licensee subject to and compliant with the privacy and information security program requirements of Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999, or to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996, any amendments thereto, and any accompanying regulations such statutes, or rules, regulations, procedures or guidelines established thereunder, is deemed compliant with Section 4, Information Security Program, of this Act to the extent such statutes, rules, regulations, procedures, or guidelines apply to all personal information, as defined in Section 3H, in whatever form maintained by that licensee.~~

~~A licensee subject to and compliant with data breach notification requirements of Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999, or to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996, any amendments thereto, and any accompanying regulations such statutes, or rules, regulations, procedures or guidelines established thereunder, is deemed compliant with Section 6D, Notification to Consumers. This Act shall not be construed as superseding, altering, or affecting any statute, regulation, order or interpretation of law in this state, except to the extent that such statute, regulation, order or interpretation is inconsistent with the provisions of this Act and then only to the extent of the inconsistency. A state statute, regulation, order or interpretation is not inconsistent with the provisions of this Act if the protection such statute, regulation, order or interpretation affords any person is greater than the protection provided under this Act.~~

C. This Act may not be construed to create or imply any new private causes of action for violation of its provisions that does not already exist under the laws of this state nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Comment [JMM1]: We may place this language in Section 4.

Comment [JMM2]: We may place this language in Section 6.

Drafting Note: This model law is intended to supplant the provisions of the NAIC's Standards for Safeguarding Consumer Information Model Regulation (#673). Therefore, states that have adopted that model law should repeal it when it enacts this model law.

### Section 3. Definitions

As used in this Act, the following terms shall have these meanings:

A. "Consumer" means an individual, including but not limited to applicants, policyholders, insureds, beneficiaries, claimants, certificate holders and others whose personal information is in a licensee's possession, custody or control.

B. "Consumer reporting agency" has the same meaning as "Consumer reporting agency that compiles and maintains files on Consumers on a nationwide basis" in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).

C. "Data breach" means the unauthorized acquisition, release or use of personal information that is reasonably likely to result in harm or inconvenience to a Consumer.

The term "data breach" does not include:

(1) the unauthorized acquisition, release or use of encrypted personal information that is encrypted or otherwise protected by another method that renders the information unreadable, unusable, inaccessible, or indecipherable if the encryption, or other protective process or key is not also acquired, released or used without authorization.

(2) the good faith acquisition of personal information by an employee if not subject to further disclosure; or

(3) the unauthorized disclosure of personal information to an employee of another licensee if no further disclosure;

(4) the unauthorized disclosure of personal information where the licensee has a good faith belief that the person to whom the unauthorized disclosure was made is not reasonably able to retain the information.

D. "Encrypted" means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.

E. "Harm or inconvenience" means any of the following or the reasonable likelihood thereof:

(1) Identity theft;

(2) Other types of fraud; or Fraudulent transactions on financial accounts; or

(3) Any act or event that results in financial or reputational damage or loss of privacy to the consumer.

(3) Other misuse as defined by [insert state definition of misuse or comparable term, if applicable].

Drafting Note: Several states have defined the term "misuse" in state law and can refer to this in Section 3E(3). If a state does not have this term defined, they may consider either deleting that paragraph or defining misuse

**Comment [JMM3]:** We will be discussing the definition of data breach on the call. Look for the Data Breach Definition Comparison Chart posted under Meeting Materials at: [http://www.naic.org/cmte\\_ex\\_cybersecurity\\_tf.htm](http://www.naic.org/cmte_ex_cybersecurity_tf.htm)

above using a definition similar to that of other states. For example, see 17-A Me. Rev. Stat. § 905-A, which provides that

A person is guilty of misuse of identification if, in order to obtain confidential information, property or services, the person intentionally or knowingly:

A. Presents or uses a credit or debit card that is stolen, forged, canceled or obtained as a result of fraud or deception;

B. Presents or uses an account, credit or billing number that that person is not authorized to use or that was obtained as a result of fraud or deception; or

C. Presents or uses a form of legal identification that that person is not authorized to use.

F. "Information security program" means the administrative, technical, and physical safeguards that a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personal information.

G. "Licensee" means any person or entity licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this state.

H. "Personal Information" means:

(1) A financial account number relating to a Consumer, including a credit card number or debit card number, in combination with any security code, access code, password, or other personal identification information required to access the financial account; or

(2) ~~Information including:~~

The first name or first initial and last name of a Consumer in combination with:

(a) The Consumer's non-truncated social security number;

(b) The Consumer's driver's license number, passport number, military identification number, or other similar number on a government-issued document;

~~(c) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online or financial account of the Consumer;~~

~~(d)~~ (c) Biometric data of the Consumer that would permit access to financial accounts of the Consumer;

(e) (d) Any information of the Consumer that the licensee has a legal or contractual duty to protect from unauthorized access or public disclosure;

~~(f) The Consumer's date of birth;~~

(g) (e) Information that the Consumer provides to a licensee to obtain an insurance product or service used primarily for personal, family, or household purposes from the licensee;

(~~h~~ f) Information about the Consumer resulting from a transaction involving an insurance product or service used primarily for personal, family, or household purposes between a licensee and the Consumer;

(~~i~~ g) Information the licensee obtains about the Consumer in connection with providing an insurance product or service used primarily for personal, family, or household purposes to the Consumer; or

(~~j~~ h) A list, description, or other grouping of Consumers (and publicly available information pertaining to them), that is derived using the information described in Section 3H(2)(g) through (i), that is not publicly available.

(3) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online or financial account of the Consumer;

(~~3~~ 4) Any of the data elements identified in Section 3H(2)(a) through (f) when not in connection with the Consumer's first name or initial and last name, if those elements would be sufficient to permit the fraudulent assumption of the Consumer's identity or unauthorized access to an account of the Consumer.

(4 5) The first name or first initial and last name of a Consumer in combination with any information or data except age or gender, that relates to:

- (a) The past, present or future physical, mental or behavioral health or condition of a Consumer;
- (b) The provision of health care to a Consumer; or
- (c) Payment for the provision of health care to a Consumer.

The term "personal information" does not include publicly available information that is lawfully made available to the general public and obtained from federal, state, or local government records; or widely distributed media.

- I. "Third-party service provider" means a person or entity that contracts with a licensee to maintain, process, store or otherwise have access to personal information under the licensee's possession, custody or control.