Draft: 8/17/2016 (version 2)
A new model: Insurance Data Security Model Law
Cybersecurity (EX) Task Force

Comments are being requested on this draft by Friday, September 16, 2016. Comments should be sent by email to Sara Robben at srobben@naic.org.

INSURANCE DATA SECURITY MODEL LAW

Table of Contents

Section 1. Title

This act shall be known and may be cited as the "Insurance Data Security Act."

Section 2. Purpose and Intent

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. 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.

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

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.

The term "data breach" does not include the unauthorized acquisition, release or use of encrypted personal information if the encryption, process or key is not also acquired, released or used without authorization.

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) Fraudulent transactions on financial accounts; or

(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 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 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) Biometric data of the consumer that would permit access to financial accounts of the consumer;

(e) 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) 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) 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) 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) 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) 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) 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.

Section 4. Information Security Program

A. Implementation of an Information Security Program

Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities and the sensitivity of the personal information in the licensee's possession, custody or control, each licensee shall develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards for the protection of personal information. The licensee shall document, on an ongoing basis, compliance with its information security program.

B. Objectives of Information Security Program

A licensee's information security program shall be designed to:

(1) Protect the security and confidentiality of personal information;

(2) Protect against any anticipated threats or hazards to the security or integrity of the information;

(3) Protect against unauthorized access to or use of personal information, and minimize the likelihood of harm or inconvenience to any consumer; and

(4) Define and periodically reevaluate a schedule for retention of personal information and a mechanism for its destruction when no longer needed.

C. Risk Assessment

The licensee shall:

(1) Designate an employee or employees responsible for the information security program;

(2) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of personal information or personal information systems;

(3) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;

(4) Assess the sufficiency of policies, procedures, personal information systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the licensee's operations, including:

(a) Employee training and management;

(b) Information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and

(c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and

(5) Implement information safeguards to manage the threats identified in its assessment, and regularly assess the effectiveness of the safeguards' key controls, systems, and procedures.

D. Risk Management

The licensee shall, at a minimum:

(1) Design its information security program to mitigate the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities, based on generally accepted cybersecurity principles, including the following security measures, as appropriate:

(a) Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent the unauthorized acquisition, release or use of personal information to or by employees or unauthorized individuals outside of the licensee;

(b) Restrict access at physical locations containing personal information, only to authorized individuals;

(c) Encrypt all personal information while being transmitted on a public internet network or wirelessly and all personal information stored on a laptop computer or other portable computing or storage device or media;

(d) Ensure that information system modifications are consistent with the licensee's information security program;

(e) Utilize state of the art techniques, such as multi-factor authentication procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, personal information;

(f) Regularly test or monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(g) Implement response procedures that specify actions to be taken when the licensee suspects or detects that unauthorized individuals have gained access to information systems;

(h) Implement measures to protect against destruction, loss, or damage of personal information due to environmental hazards, such as fire and water damage or technological failures; and

(i) Develop, implement, and maintain procedures for the secure disposal of personal information in any format.

(2) Include cybersecurity risks in the licensee's enterprise risk management process; and

(3) Use generally accepted cybersecurity principles to share information and stay informed regarding emerging threats or vulnerabilities.

E. Oversight by Board of Directors

If the licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

(1) Oversee the development, implementation, and maintenance of the licensee's information security program, including assigning specific responsibility for the plan to the licensee's executive management; and

(2) Require the licensee's executive management to report in writing at least annually, the following information:

(a) The overall status of the information security program and the licensee's compliance with this Act; and

(b) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, data breaches or violations and management's responses thereto, and recommendations for changes in the information security program.

F. Oversight of Third-Party Service Provider Arrangements

The licensee shall contract only with third-party service providers that are capable of maintaining appropriate safeguards for personal information in the licensee's possession, custody or control, and the licensee shall be responsible for any failure by such third-party service providers to protect personal information provided by the licensee to the third-party service providers consistent with this Act.

G. Program Adjustments

The licensee shall monitor, evaluate and adjust, as appropriate, the information security program consistent with any relevant changes in technology, the sensitivity of its personal information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to personal information systems.

Section 5. Investigation of a Data Breach

A. If the licensee learns that a data breach has or may have occurred in relation to personal information in the possession, custody or control of the licensee or any of the licensee's third-party service providers, the licensee shall conduct a prompt investigation.

B. During the investigation, the licensee shall, at a minimum:

(1) Assess the nature and scope of the data breach or potential data breach;

(2) Identify any personal information that may have been involved in the data breach;

(3) Determine whether the personal information has been acquired, released or used without authorization; and

(4) Perform or oversee reasonable measures to restore the security of the information systems compromised in the data breach in order to prevent further unauthorized acquisition, release or use of personal information in the licensee's possession, custody or control.

Section 6. Notification of a Data Breach

A. If following an investigation under Section 5, the licensee determines that an unauthorized acquisition of personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) involved in a data breach has occurred, the licensee, or a third party acting on behalf of the licensee, shall notify:

(1) All consumers to whom the personal information relates;

(2) The insurance commissioner in the licensee's state of domicile and the insurance commissioners of all the states in which a consumer whose information was or may have been compromised resides;

(3) The relevant Federal and state law enforcement agencies, as appropriate;

(4) Any relevant payment card network, if the data breach involves payment card numbers; and

(5) Each consumer reporting agency, if the data breach involves personal information relating to 500 or more consumers.

B. Notification to the Commissioner

Notwithstanding the responsibilities prescribed in Sections 5A and 6A of this Act, no later than three (3) business days after determining that a data breach has occurred, the licensee shall notify the commissioner that a data breach has occurred. The licensee shall provide as much of the following information as possible:

(1) Date of the data breach;

(2) Description of the data breach, including how the information was exposed, whether lost, stolen, or breached;

(3) How the data breach was discovered;

(4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done;

(5) The identity of the source of the data breach;

(6) Whether licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;

(7) Description of the type of information lost, stolen, or breached (equipment, paper, electronic, claims, applications, underwriting forms, medical records etc.);

(8) Whether, if the information was encrypted, the encryption, redaction or protection process or key was also acquired without authorization;

(9) The period during which the information system was compromised by the data breach;

(10) The number of total consumers and consumers of each state affected by the data breach;

(11) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;

(12) Identification of efforts being undertaken to remediate the situation which permitted the data breach to occur;

(13) A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the data breach; and

(14) Name of a contact person who is both familiar with the data breach and authorized to act for the licensee.

The licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the commissioner concerning the data breach.

C. Notification to Consumer Reporting Agencies

The licensee shall notify, as expediently as possible and without unreasonable delay, after determining that a data breach has occurred, each consumer reporting agency, if the data breach involves personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) relating to 500 or more consumers. Notification must include the date of the data breach, an estimate of the number of persons affected by the data breach, if known, and the actual or anticipated date that persons were or will be notified of the data breach.

D. Notification to Consumers

(1) The licensee shall notify all consumers whose personal information listed in Section 3H(1), (2)(a) through (f), (3) or (4) was affected as expediently as possible and without unreasonable delay, and in no case later than sixty (60) calendar days after determining that a data breach has occurred.

(2) Prior to sending the notification, the licensee shall provide the commissioner with a draft of the proposed written communication to consumers. The commissioner shall have the right to review the proposed communication before the licensee sends it to consumers, to ensure compliance with this subsection and to prescribe the appropriate level of consumer protection pursuant to Section 7.

The notice must be written in straightforward language and include the following information::

(a) A description of the type of information involved in the data breach;

(b) A description of the action that the licensee or third-party service provider has taken to safeguard the information;

(c) A summary of rights of victims of identity theft prepared under § 609(d) of the Fair Credit Reporting Act (15 U.S.C. 1681g(d));

(d) The steps consumers can take to protect themselves from identity theft or fraud, which shall include an explanation that consumers shall have a right to do the following:

(i) Place a 90-day initial fraud alert on their consumer reports;

(ii) Place a seven-year extended fraud alert on their consumer reports;

(iii) Place a credit freeze on their consumer reports;

(iv) Have a free copy of their consumer report from each credit bureau;

(v) Receive fraudulent information related to the data breach removed (or "blocked") from their consumer reports;

(vi) Dispute fraudulent or wrong information on their consumer reports;

(vii) Stop creditors and debt collectors from reporting fraudulent accounts related to the data breach;

(viii) Receive copies of documents related to the identity theft; and

(ix) Stop contacts from debt collectors related to the data breach;

(e) Contact information for the three nationwide consumer reporting agencies;

(f) Contact information for the licensee or its designated call center; and

(g) An offer from the licensee to the consumer to provide appropriate identity theft protection services free of cost to the consumer for a period of not less than twelve (12) months, if appropriate, or other consumer protections ordered by the commissioner pursuant to Section 7 of this Act.

(3) The licensee will provide the consumer notification:

(a) In writing by first class mail; or

(b) Electronically if the consumer has agreed to be contacted through e-mail or other means pursuant to [insert reference to state Electronic Transactions Act.]; or

(c) By substitute method, if the licensee demonstrates to the commissioner's satisfaction that the cost of providing notice by Section 6D(3)(a) or (b) would be excessive or that another legitimate reason exists for substitute notice. The substitute method must include conspicuous posting of the notice on the licensee's publicly accessible website and publication in statewide media in this state.

E. Notice Regarding Data Breaches of Third-Party Service Providers

In the event of a data breach in a system maintained by a third-party service provider, the licensee shall comply with Section 6A through D. The computation of licensee's deadlines shall begin on the day after the third-party service provider notifies the licensee of the data breach or the licensee otherwise has actual knowledge of the data breach, whichever is sooner.

F. Notwithstanding the requirements of Section 6C, D, and E, notice may be delayed where requested by an appropriate state or federal law enforcement agency. The commissioner shall be notified of any such request.

Drafting Note: Section 5 and Section 6 may be duplicative of current state law. Each state should conduct its own analysis to determine whether or not Section 5 and Section 6, in whole or in part, are necessary to be included in its statutes.

Section 7. Consumer Protections Following a Data Breach

After reviewing the licensee's data breach notification, the commissioner shall prescribe the appropriate level of consumer protection required following the data breach and how long that protection will be provided. The commissioner may order the

licensee to offer to pay for twelve (12) months or more of identity theft protection for affected consumers, pay for a credit freeze, or take other action deemed necessary to protect consumers.

Drafting Note: Many states have statutes providing that a consumer reporting agency cannot charge a fee for a credit freeze on a consumer file when the consumer is a victim of identity theft, which is shown by providing a police report. For an example, *see* Tex. Bus. & Com. Code § 20.04(b). As an alternative to having the licensee pay for the credit freeze, a state should consider referencing that law and providing that the credit freeze is free for consumers after the data breach is reported to law enforcement by the licensee, by showing a data breach notification letter from the licensee. The state may also need to amend its free credit freeze law to ensure this is covered.

If the data breach has affected consumers in other states, the commissioner shall, consistent with the requirements of [reference to statute describing the commissioner's general powers] and with the circumstances of the data breach as they affect consumers in this state, cooperate with the insurance regulators of those states in prescribing the appropriate level of consumer protection described in the previous sentence.

Section 8. Power of Commissioner

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].

Section 9. Enforcement

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 issue and serve upon such licensee a statement of charges and notice of hearing to be held at a time and place fixed in the notice. The hearing shall be conducted in accordance with [cite provisions of state administrative procedure act or insurance code applicable to administrative enforcement proceedings for serious violations].

Section 10. Confidentiality

A. Any documents, materials or other information in the control or possession of the department of insurance that are furnished by a licensee or an employee or agent thereof acting on behalf of licensee pursuant to Section 6B(2), (3), (4), (5), (6), (8), (11), and (12), or that are obtained by the insurance commissioner in an investigation or examination pursuant to Section 8 of this Act shall be confidential by law and privileged, shall not be subject to [insert reference to state open records, freedom of information, sunshine or other appropriate law], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the insurance commissioner is authorized to use the documents, materials or other information in the furtherance of any regulatory or legal action brought as a part of the insurance commissioner's duties.

B. Neither the insurance commissioner nor any person who received documents, materials or other information while acting under the authority of the insurance commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to Section 10A.

C. In order to assist in the performance of the insurance commissioner's duties under this Act, the insurance commissioner:

(1) May share documents, materials or other information, including the confidential and privileged documents, materials or information subject to Section 10A, with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees to maintain the confidentiality and privileged status of the document, material or other information;

(2) May receive documents, materials or information, including otherwise confidential and privileged documents, materials or information, from the National Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or

domestic jurisdictions, and shall maintain as confidential or privileged any document, material or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material or information; and

(3) **[OPTIONAL]** May enter into agreements governing sharing and use of information consistent with this subsection.

D. No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the commissioner under this section or as a result of sharing as authorized in Section 10C.

E. Nothing in this Act shall prohibit the insurance commissioner from releasing final, adjudicated actions including for cause terminations that are open to public inspection pursuant to [insert appropriate reference to state law] to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries.

Drafting Note: States conducting an investigation or examination under their examination law may apply the confidentiality protections of that law to such an investigation or examination.

Section 11. Penalties

In the case of a violation of this Act a licensee may be penalized in accordance with [insert general penalty statute].

Section 12. Rules and Regulations

The commissioner may, upon notice and opportunity for all interested persons to be heard, issue such rules, regulations and orders as shall be necessary to carry out the provisions of this Act.

Section 13. 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.

Section 14. Effective Date

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].

