Draft: 4/26/2017 (proposed version 4)
A new model: Insurance Data Security Model Law
Cybersecurity (EX) Working Group

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 Law."

Section 2. Purpose and Intent

A. The purpose and intent of this Act is to establish standards for data security as well as for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to Licensees, as defined in Section 3.

B. The Standards for Safeguarding Customer Information Regulation identifies basic requirements that Licensees must meet for a broadly defined universe of nonpublic personal information. This Act compliments and expands on the existing Standards for Safeguarding Customer Information Regulation for a defined set of nonpublic personal information, defined as Nonpublic Information.

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

Drafting Note: States that have not adopted the Standards for Safeguarding Customer Information Model Regulation should consider deleting Subsection B and substituting the following language: Cyber threats have evolved since the adoption of the Gramm-Leach-Bliley Act (GLBA) and will continue to evolve as our society becomes increasingly interconnected, bad actors adapt to new technology and defense measures, and industry adjusts its resiliency efforts. As such, this Act builds upon the principles established by the GLBA and identifies additional risk-based regulatory expectations for a defined set of Nonpublic Information.

Section 3. Definitions

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

A. "Commissioner" means the chief insurance regulatory official of the state.

B. "Consumer" means an individual, including but not limited to applicants, policyholders, insureds, beneficiaries, claimants, certificate holders and others who is a resident of this state and whose Nonpublic Information is in a Licensee's possession, custody or control.

C. "Cybersecurity Event" means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.

The term "Cybersecurity Event" does not include the unauthorized acquisition of Encrypted Nonpublic Information if the encryption, process or key is not also acquired, released or used without authorization.

Cybersecurity Event does not include an event with regard to which the Licensee has determined that the Nonpublic Information released to an unauthorized person has not been used and has been returned or destroyed without further release.

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. "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 Nonpublic Information.

F. "Information System" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

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 but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this state.

H. "Multi-Factor Authentication" means authentication through verification of at least two of the following types of authentication factors:

(1) Knowledge factors, such as a password; or

(2) Possession factors, such as a token or text message on a mobile phone; or

(3) Inherence factors, such as a biometric characteristic.

I. "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 an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements:

(a) Social security number,

(b) Drivers' 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 an individual'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 an individual and that relates to

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

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

(c) Payment for the provision of health care to any individual.

J. "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 subsection, 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 an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

K. "Third-Party Service Provider" means a person or entity, 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.

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 Nonpublic Information used by the Licensee or in the Licensee's possession, custody or control, each Licensee shall develop, implement, and maintain a comprehensive risk-focused written Information Security Program that contains administrative, technical, and physical safeguards for the protection of Nonpublic Information. The Licensee shall document, on an annual basis, compliance with its Information Security Program. The Licensee shall make this documentation available to the Commissioner upon request.

B. Objectives of Information Security Program

A Licensee's Information Security Program shall be designed to:

(1) Protect the security and confidentiality of Nonpublic Information;

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

(3) Protect against unauthorized access to or use of Nonpublic Information, and minimize the likelihood of harm or inconvenience to any Consumer; and

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

C. Risk Assessment

The Licensee shall:

(1) Designate one or more employees or an outside vendor and/or service provider designated to act on behalf of the Licensee who is 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 Nonpublic Information;

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

(4) Assess the sufficiency of policies, procedures, 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 classification, governance, 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

Based on its Risk Assessment, the Licensee shall:

(1) (a) 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, including consideration of whether implementing the security measures listed in Section 4D(2) is appropriate.

(b) Determine appropriate security measures listed in Section 4D(2). Licensees shall use the best practices for cybersecurity protection, detection, and remediation available commensurate with its nature, scope, scale and complexity.

(2) Implement the following security measures, as appropriate:

(a) Place access controls on Information Systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition, of Nonpublic Information;

(b) Ensure that the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy;

(c) Restrict access at physical locations containing Nonpublic Information, only to authorized individuals;

(d) Protect by encryption or other appropriate means, all Nonpublic Information while being transmitted wirelessly or on a public network and all Nonpublic Information stored on a laptop computer or other portable computing or storage device or media;

(e) Ensure the use of secure development practices for in-house developed applications utilized by the Licensee and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Licensee;

(f) Ensure that Information System modifications are consistent with the Licensee's Information Security Program;

(g) Utilize multi-factor authentication procedures, segregation of duties, and employee background checks for any individual assessing Nonpublic Information in the Licensees internal network from an external network;

(h) Regularly test or monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, Information Systems;

(i) Ensure the Information Security Program includes audit trails designed to detect Cybersecurity Events;

(j) Implement response procedures that specify actions to be taken when the Licensee suspects or detects that unauthorized individuals have gained access to Information Systems;

(k) Implement measures to protect against destruction, loss, or damage of Nonpublic Information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and

(l) Develop, implement, and maintain procedures for the secure disposal of Nonpublic Information in any format.

(3) Include cybersecurity risks in the Licensee's enterprise risk management process; and

(4) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared.

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 or its delegates;

(2) Require the Licensee's executive management or delegates thereof 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, Cybersecurity Events or violations and management's responses thereto, and recommendations for changes in the Information Security Program.

(3) If executive management delegates responsibilities under this section it shall oversee the development, implementation and maintenance of the Licensee's Information Security Program prepared by the delegate(s) and shall receive a report from the delegate(s) complying with the requirements of the report to the Board of Directors above.

F. Oversight of Third-Party Service Provider Arrangements

(1) Each Licensee shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third-Party

Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Licensee and shall address to the extent applicable:

(a) The identification and risk assessment of Third-Party Service Providers;

(b) Minimum cybersecurity practices required to be met by such Third-Party Service Providers in order for them to do business with the Licensee;

(c) Due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third-Party Service Providers; and

(d) Periodic assessment of such Third-Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(2) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third-Party Service Providers including, to the extent applicable, guidelines addressing:

(a) The Third-Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication, to limit access to relevant Information Systems and Nonpublic Information;

(b) The Third-Party Service Provider's policies and procedures for use of Encryption to protect Nonpublic Information in transit and at rest;

(c) Notice to be provided to the Licensee in the event of a Cybersecurity Event directly impacting the Licensee's Information Systems or the Licensee's Nonpublic Information being held by the Third-Party Service Provider; and

(d) Representations and warranties addressing the Third-Party Service Provider's cybersecurity policies and procedures that relate to the security of the Licensee's Information Systems or Nonpublic Information.

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 Nonpublic 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 Information Systems.

Section 5. Investigation of a Cybersecurity Event

A. If the Licensee learns that a Cybersecurity Event has or may have occurred the Licensee, or an outside vendor and/or service provider designated to act on behalf of the Licensee, shall conduct a prompt investigation.

B. During the investigation, the Licensee, or an outside vendor and/or service provider designated to act on behalf of the Licensee, shall, at a minimum determine as much of the following information as possible:

(1) Determine whether a Cybersecurity Event has occurred;

(2) Assess the nature and scope of the Cybersecurity Event;

(3) Identify any Nonpublic Information that may have been involved in the Cybersecurity Event; and

(4) Perform or oversee reasonable measures to restore the security of the Information Systems compromised in the Cybersecurity Event in order to prevent further unauthorized acquisition, release or use of Nonpublic Information in the Licensee's possession, custody or control.

C. If the Licensee learns that a Cybersecurity Event has or may have occurred in a system maintained by a Third-Party Service Provider, the Licensee will confirm and document that the Third-Party Service Provider has completed the steps listed in Section 5B above.

D. The Licensee shall maintain records concerning all Cybersecurity Events for a period of at least five years and shall produce those records upon demand of the Commissioner.

Section 6. Notification of a Cybersecurity Event

A. Notification to the Commissioner

Each Licensee shall notify the Commissioner as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred if:

(1) The Licensee is an insurer domiciled in this state; or

(2) The Licensee reasonably believes that the Nonpublic Information involved is of 250 or more residents of this state and that is either of the following:

(a) A Cybersecurity Event impacting the Licensee of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or

(b) A Cybersecurity Event that has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Licensee.

B. The Licensee shall provide as much of the following information as possible. The Licensee shall provide the information in electronic form as directed by the Commissioner. The Licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Commissioner concerning the Cybersecurity Event.

(1) Date of the Cybersecurity Event;

(2) Description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of Third-Party Service Providers;

(3) How the Cybersecurity Event 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 Cybersecurity Event;

(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 specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information or types of information allowing identification of the Consumer;

(8) The period during which the Information System was compromised by the Cybersecurity Event;

(9) The number of total Consumers in this state affected by the Cybersecurity Event. The Licensee shall provide the best estimate in the initial report to the Commissioner and update this estimate with each subsequent report to the Commissioner pursuant to this section;

(10) 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;

(11) Description of efforts being undertaken to remediate the situation which permitted the Cybersecurity Event to occur;

(12) 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 Cybersecurity Event; and

(13) Name of a contact person who is both familiar with the Cybersecurity Event and authorized to act for the Licensee.

C. Notification to Consumers. The Licensee shall comply with [insert states' data breach notification law] and provide a copy of the notice sent to Consumers under that statute to the Commissioner.

D. Notice Regarding Cybersecurity Events of Third-Party Service Providers

(1) In the case of a Cybersecurity Event in a system maintained by a Third-Party Service Provider, for which the Licensee has received notice, the Licensee shall treat such event as it would under Section 6A.

(2) The computation of Licensee's deadlines shall begin on the day after the Third-Party Service Provider notifies the Licensee of the Cybersecurity Event or the Licensee otherwise has actual knowledge of the Cybersecurity Event, whichever is sooner.

(3) Nothing in this Act shall prevent or abrogate an agreement between a Licensee and another Licensee, a Third-Party Service Provider or any other party to fulfill any of the investigation requirements imposed under Section 5 or notice requirements imposed under Section 6.

E. Notice Regarding Cybersecurity Events of Reinsurers to Insurers

(1) In the case of a Cybersecurity Event involving Nonpublic Information that is used by the Licensee that is acting as an assuming insurer or in the possession, custody or control of a Licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected Consumers, the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of making the determination that a Cybersecurity Event has occurred; and

(2) In the case of a Cybersecurity Event involving Nonpublic Information that is in the possession, custody or control of a Third-Party Service Provider of a Licensee that is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of receiving notice from its Third-Party Service Provider that a Cybersecurity Event has occurred.

F. Notice Regarding Cybersecurity Events of Insurers to Producers of Record

(1) In the case of a Cybersecurity Event involving Nonpublic Information that is in the possession, custody or control of a Licensee that is an insurer or its Third-Party Service Provider and for which a Consumer accessed the insurer's services through an independent insurance producer, the insurer shall notify the producers of record of all affected Consumers within 72 hours of making the determination that a Cybersecurity Event has occurred.

(2) The insurer is excused from this obligation for those instances in which it does not have the current producer of record information for any individual Consumer.

Section 7. Power of Commissioner

A. 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].

B. 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.

Section 8. 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), (8), (10), and (11), or that are obtained by the Commissioner in an investigation or examination pursuant to Section 7 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 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 Commissioner's duties.

B. Neither the Commissioner nor any person who received documents, materials or other information while acting under the authority of the Commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to Section 8A.

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

(1) May share documents, materials or other information, including the confidential and privileged documents, materials or information subject to Section 8A, 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 in writing 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) 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 8C.

E. Nothing in this Act shall prohibit the 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 9. Exceptions

A. The following exceptions shall apply to this Act:

(1) A Licensee with fewer than ten employees, including any independent contractors is exempt from Section 4 of this Act;

(2) A Licensee subject to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996 (Health Insurance Portability and Accountability Act) that has established and maintains an Information Security Program pursuant to such statutes, or rules, regulations, procedures or guidelines established thereunder, is deemed to be in compliance with the requirements of Section 4. 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;

(3) An employee, agent, representative or designee of a Licensee, who is also a Licensee, is exempt from Section 4 and need not develop its own Information Security Program to the extent that the employee, agent, representative or designee is covered by the Information Security Program of the other Licensee.

B. In the event that a Licensee ceases to qualify for an exception, such Licensee shall have 180 days to comply with this Act.

Section 10. Penalties

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

Section 11. 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.

Section 12. 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 13. Effective Date

This Act shall take effect on [insert a date]. Licensees shall have 180 days 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 4(F) of this Act.

