PLEASE NOTE: Legislative Information ***cannot*** perform research, provide legal advice, or interpret Maine law. For legal assistance, please contact a qualified attorney.

An Act To Enact the Maine Insurance Data Security Act

Be it enacted by the People of the State of Maine as follows:

Sec. 1. 24-A MRSA c. 24-B is enacted to read:

CHAPTER 24-B

MAINE INSURANCE DATA SECURITY ACT

§ 2261. Short title

This chapter may be known and cited as "the Maine Insurance Data Security Act."

§ 2262. Construction

This chapter establishes standards for data security and standards for the investigation of and notification to the superintendent regarding a cybersecurity event applicable to licensees. This chapter may not be construed to create or imply a private cause of action for violation of its provisions or to curtail a private cause of action that would otherwise exist in the absence of this chapter.

§ 2263. Definitions

As used in this chapter, unless the context otherwise indicates, the following terms have the following meanings.

1. Authorized individual. "Authorized individual" means an individual known to and screened by a licensee and whose access to the nonpublic information held by the licensee and its information systems is determined by the licensee to be necessary and appropriate.

2. Consumer. "Consumer" means an individual, including but not limited to an applicant for insurance, policyholder, insured, beneficiary, claimant or certificate holder, who is a resident of this State and whose nonpublic information is in a licensee's possession, custody or control.

3. Cybersecurity event. "Cybersecurity event" means an event resulting in unauthorized access to, disruption of or misuse of an information system or information stored on an information system.

"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 accessed by an unauthorized person has not been used or released and has been returned or destroyed.

4. Encrypted. "Encrypted," with respect to data, means that the data has been transformed into a form that results in a low probability of assigning meaning without the use of a protective process or key.

5. Information security program. "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.

6. Information system. "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 an industrial or process control system, a telephone switching and private branch exchange system or an environmental control system.

7. Insurance carrier. "Insurance carrier" means a health maintenance organization, fraternal benefit society, nonprofit hospital or medical service organization or nonprofit health plan.

8. Licensee. "Licensee" means a person licensed, authorized to operate or registered or required to be licensed, authorized or registered pursuant to the insurance laws of this State. "Licensee" does 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 and is domiciled in another state or jurisdiction.

9. Multifactor authentication. "Multifactor authentication" means authentication through verification of at least 2 of the following types of authentication factors:

A. Knowledge factors, such as a password;

B. Possession factors, such as a token or text message on a mobile telephone; and

C. Inherence factors, such as a biometric characteristic.

10. Nonpublic information. "Nonpublic information" means information that is not publicly available information and is:

A. Business-related information of a licensee the tampering with or unauthorized disclosure of, access to or use of which would materially and adversely affect the business, operations or security of the licensee;

B. Information that, because of name, number, personal mark or other identifier, can be used in combination with any one or more of the following data elements to identify a consumer:

(1) Social security number;

(2) Driver's license number or nondriver identification card number;

(3) Account number or credit or debit card number;

(4) Any security code, access code or password that would permit access to a consumer's financial account; or

(5) Biometric records; or

C. 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:

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

(2) The provision of health care to a consumer; or

(3) Payment for the provision of health care to a consumer.

11. Publicly available information. "Publicly available information" means information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:

A. Federal, state or local government records;

B. Widely distributed media; or

C. 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 that the information is of a type that is available to the general public; and whether a consumer can direct that the information not be made available to the general public and, if so, that the consumer has not done so.

12. Risk assessment. "Risk assessment" means the risk assessment that a licensee is required to conduct under section 2264, subsection 3.

13. Third-party service provider. "Third-party service provider" means a person that is not a licensee and that contracts with a licensee to maintain, process or store or otherwise is permitted access to nonpublic information through its provision of services to the licensee.

§ 2264. Information security program

1. Implementation of information security program. Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of 3rd-party service providers, and the sensitivity of the nonpublic information used by the licensee

or in the licensee's possession, custody or control, a licensee shall develop, implement and maintain a comprehensive, written information security program based on the licensee's risk assessment and containing administrative, technical and physical safeguards for the protection of nonpublic information and the licensee's information system.

2. Objectives of information security program. A licensee's information security program must be designed to:

A. Protect the security and confidentiality of nonpublic information and the security of the information system;

B. Protect against threats or hazards to the security or integrity of nonpublic information and the information system;

C. Protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to any consumer; and

D. Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when it is no longer needed.

3. Risk assessment. A licensee shall:

A. Designate one or more employees, an affiliate or another person designated to act on behalf of the licensee to be responsible for the licensee's information security program;

B. Identify reasonably foreseeable internal or external threats that could result in unauthorized access to or transmission, disclosure, misuse, alteration or destruction of nonpublic information, including threats to the security of the licensee's information systems and nonpublic information that are accessible or held by 3rd-party service providers;

C. Assess the likelihood and potential damage of the threats described in paragraph B, taking into consideration the sensitivity of the nonpublic information;

D. Assess the sufficiency of policies, procedures, information systems and other safeguards in place to manage the threats described in paragraph B, including consideration of threats in each relevant area of the licensee's operations, including:

(1) Employee training and management;

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

(3) Detecting, preventing and responding to attacks, intrusions or other system failures; and

E. At least annually, assess the effectiveness of the key controls, systems and procedures of information safeguards implemented to manage the threats described in paragraph B identified in the licensee's ongoing assessment.

4. Risk management. Based on its risk assessment pursuant to subsection 3, a licensee shall:

A. Design its information security program to mitigate the identified risks, commensurate with the size and complexity of the licensee's activities, including its use of 3rd-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody or control;

B. Consider the following security measures and implement the measures considered appropriate:

(1) 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;

(2) Identify and manage the data, personnel, devices, systems and facilities that enable the licensee to achieve its business purposes in accordance with their relative importance to business objectives and the licensee's risk management strategy;

(3) Restrict to only authorized individuals access at physical locations containing nonpublic information;

(4) Protect, by encryption or other appropriate means, all nonpublic information while it is being transmitted over an external network and all nonpublic information stored on a laptop computer or other portable computing or storage device or media;

(5) Adopt secure development practices for applications developed and used by the licensee and procedures for evaluating, assessing or testing the security of externally developed applications used by the licensee;

(6) Modify the information system in accordance with the licensee's information security program;

(7) Use effective controls, which may include multifactor authentication procedures, for individuals accessing nonpublic information;

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

(9) Include audit trails within the information security program designed to detect and respond to cybersecurity events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee;

(10) 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

(11) Develop, implement and maintain procedures for the secure disposal of nonpublic information in any format;

C. Include cybersecurity risks in the licensee's enterprise risk management process;

D. Stay informed regarding emerging threats or vulnerabilities and use reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and

E. Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in the risk assessment.

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

A. Require the licensee's executive management or the executive management's delegates to develop, implement and maintain the licensee's information security program; and

B. Require the licensee's executive management or the executive management's delegates to report to the board in writing at least annually the following information:

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

(2) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, 3rd-party service provider arrangements, results of testing, cybersecurity events or cybersecurity violations and the executive management's responses to cybersecurity events or cybersecurity violations, and recommendations for changes to the information security program.

If a licensee's executive management delegates any of its responsibilities under this section, the licensee's executive management shall oversee each delegate's efforts with respect to the development, implementation and maintenance of the licensee's information security program and shall require each delegate to submit a report to the board pursuant to paragraph B.

6. Oversight of 3rd-party service provider arrangements. A licensee shall:

A. Exercise due diligence in selecting its 3rd-party service providers; and

B. Require each 3rd-party service provider to implement appropriate administrative, technical and physical measures to protect and secure the information systems and nonpublic information that are accessible or held by the 3rd-party service provider.

7. Program adjustments. A licensee shall monitor, evaluate and adjust, as appropriate, its information security program consistent with any relevant changes in technology, the sensitivity of the licensee's 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.

8. Incident response plan. As part of its information security program, a licensee shall establish a written incident response plan designed to promptly respond to and recover from any cybersecurity event that compromises the confidentiality, integrity or availability of nonpublic information in its possession; the licensee's information systems; or the continuing functionality of any aspect of the licensee's business or operations. The incident response plan must address the following areas:

A. The internal process for responding to a cybersecurity event;

B. The goals of the incident response plan;

C. The definition of clear roles, responsibilities and levels of decision-making authority;

D. External and internal communications and information sharing;

E. Requirements for the remediation of any identified weaknesses in information systems and associated controls;

F. Documentation and reporting regarding cybersecurity events and related incident response activities; and

G. The evaluation and revision as necessary of the incident response plan following a cybersecurity event.

9. Annual certification to superintendent. By February 15th annually, an insurance carrier domiciled in this State shall submit to the superintendent a written statement certifying that the insurance carrier is in compliance with the requirements set forth in this section. An insurance carrier shall maintain for examination by the superintendent all records, schedules and data supporting this

certification for a period of 5 years. To the extent that an insurance carrier has identified areas, systems or processes that require material improvement, updating or redesign, the insurance carrier shall document the identification and the remedial efforts planned and under way to address such areas, systems or processes. The documentation required pursuant to this subsection must be available for inspection by the superintendent.

§ 2265. Investigation of cybersecurity event

1. Investigation. If a licensee learns that a cybersecurity event has or may have occurred, the licensee or an outside vendor or service provider designated to act on behalf of the licensee shall conduct a prompt investigation. During the investigation, the licensee or an outside vendor or service provider designated to act on behalf of the licensee shall, at a minimum:

A. Determine whether a cybersecurity event has occurred;

B. Assess the nature and scope of the cybersecurity event;

C. Identify any nonpublic information that may have been involved in the cybersecurity event; and

D. 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.

2. System maintained by 3rd-party service provider. If a licensee learns that a cybersecurity event has or may have occurred in an information system maintained by a 3rd-party service provider, the licensee shall complete the steps listed in subsection 1 or confirm and document that the 3rd-party service provider has completed those steps.

3. Maintenance of records. A licensee shall maintain records concerning a cybersecurity event for a period of at least 5 years from the date of the cybersecurity event and shall produce those records upon demand of the superintendent.

§ 2266. Notification of cybersecurity event

1. Notification to superintendent. Notwithstanding Title 10, chapter 210-B, a licensee shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred if:

A. This State is the licensee's state of domicile, in the case of an insurance carrier, or this State is the licensee's home state, as that term is defined in section 1420-A, subsection 2, in the case of an insurance producer; or

B. The licensee reasonably believes that the nonpublic information involved concerns 250 or more consumers residing in this State and that the cybersecurity event is either of the following:

(1) A cybersecurity event affecting the licensee of which notice is required to be provided to any government body, self-regulatory organization or other supervisory body pursuant to any state or federal law; or

(2) A cybersecurity event that has a reasonable likelihood of materially harming:

(a) Any consumer residing in this State; or

(b) Any material part of the normal operation of the licensee.

2. Provision of information by licensee. A licensee shall provide in electronic form as directed by the superintendent as much of the following information regarding a cybersecurity event as possible:

A. The date of the cybersecurity event;

B. A description of how the information was exposed, lost, stolen or breached, including the specific roles and responsibilities of 3rd-party service providers, if any;

C. How the cybersecurity event was discovered;

D. Whether any lost, stolen or breached information has been recovered and, if so, how this was done;

E. The identity of the source of the cybersecurity event;

F. Whether the licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when the report was filed or the notification was provided;

G. A description of the specific types of information acquired without authorization. For purposes of this subsection, "specific types of information" includes, but is not limited to, medical information, financial information and information allowing identification of a consumer;

H. The period of time during which the information system was compromised by the cybersecurity event;

I. The total number of consumers in this State affected by the cybersecurity event. The licensee shall provide its best estimate in the initial report to the superintendent and update this estimate with each subsequent report to the superintendent pursuant to this section;

J. The results of any review conducted by or for the licensee identifying a lapse in either automated controls or internal procedures or confirming that all automated controls or internal procedures were followed;

K. A description of efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur;

L. 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

M. The name and contact information of a person who is both familiar with the cybersecurity event and authorized to act for the licensee.

The licensee has a continuing obligation to update and supplement initial and subsequent notifications to the superintendent concerning the cybersecurity event.

3. Notification to consumers. A licensee shall comply with Title 10, chapter 210-B, as applicable, and, when required to notify the superintendent under subsection 1, provide to the superintendent a copy of the notice sent to consumers pursuant to Title 10, chapter 210-B.

4. Notice regarding cybersecurity events of 3rd-party service providers. In the case of a cybersecurity event in an information system maintained by a 3rd-party service provider of which the licensee has become aware:

A. The licensee shall respond to the cybersecurity event as described under subsection 1; and

B. The computation of the licensee's deadlines for notification under this section begins on the day after the 3rd-party service provider notifies the licensee of the cybersecurity event or the day after the licensee otherwise has actual knowledge of the cybersecurity event, whichever is sooner.

Nothing in this subsection or in this chapter may be construed to prevent or abrogate an agreement between a licensee and another licensee, a 3rd-party service provider or any other party to fulfill any of the investigation requirements imposed under section 2265 or notice requirements imposed under this subsection.

5. Notice regarding cybersecurity events of reinsurers to insurers. This subsection governs notice regarding cybersecurity events of reinsurers to insurers.

A. In the case of a cybersecurity event involving nonpublic information that is used by a 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:

(1) The assuming insurer shall notify its affected ceding insurers and the superintendent of its state of domicile within 72 hours of making the determination that a cybersecurity event has occurred; and

(2) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under the laws of this State and any other notification requirements relating to a cybersecurity event imposed under this section.

B. In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of a 3rd-party service provider of a licensee that is acting as an assuming insurer:

(1) The assuming insurer shall notify its affected ceding insurers and the superintendent of its state of domicile within 72 hours of receiving notice from its 3rd-party service provider that a cybersecurity event has occurred; and

(2) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under the laws of this State and any other notification requirements relating to a cybersecurity event imposed under this section.

6. Notice regarding cybersecurity events of insurance carriers to producers of record. In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of a licensee that is an insurance carrier or its 3rd-party service provider and for which information a consumer accessed the insurance carrier's services through an independent insurance producer, the insurance carrier shall notify the producers of record of all affected consumers as soon as practicable as directed by the superintendent, except that the insurance carrier is excused from this obligation for those instances in which it does not have the current producer of record information for any individual consumer.

§ 2267. Power of superintendent

1. Investigate. The superintendent may examine and investigate the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of this chapter. This power is in addition to the powers the superintendent has under sections 220 and 221. Any such examination or investigation must be conducted pursuant to those sections.

2. Enforcement. Whenever the superintendent has reason to believe that a licensee has been or is engaged in conduct in this State that violates this chapter, the superintendent may take action that is necessary or appropriate to enforce the provisions of this chapter.

§ 2268. Confidentiality

1. Materials held confidential. Documents, materials and other information in the control or possession of the bureau that are furnished by a licensee or an employee or agent acting on behalf of the licensee pursuant to section 2264, subsection 9 or section 2266, subsection 2, paragraph B, C, D, E, H, J or K or that are obtained by the superintendent in an investigation or examination pursuant to section 2267 are confidential by law and privileged, are not subject to Title 1, chapter 13, subchapter 1, are not

subject to subpoena and are not subject to discovery or admissible in evidence in any private civil action; however, the superintendent is authorized to use the documents, materials and other information in the furtherance of any regulatory or legal action brought as a part of the superintendent's duties and to share them on a confidential basis in accordance with section 216, subsection 5.

2. Private civil action. Neither the superintendent nor any person who received documents, materials or other information while acting under the authority of the superintendent may be permitted or required to testify in any private civil action concerning any confidential documents, materials or information subject to subsection 1.

3. Disclosure not a waiver. Disclosure of information to the superintendent under this section or as a result of sharing as authorized in section 216, subsection 5 does not constitute a waiver of any applicable privilege or claim of confidentiality regarding the documents, materials or information.

4. Final actions. Nothing in this chapter may be construed to prohibit the superintendent from releasing final, adjudicated actions that are open to public inspection pursuant to Title 1, chapter 13, subchapter 1 to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries or any successor organization.

§ 2269. Application; exceptions

1. Small business exception. A licensee with fewer than 10 employees, including any independent contractors, is exempt from section 2264.

2. Subject to federal law. A licensee subject to the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 that has established and maintains an information security program pursuant to that law and the rules, regulations, procedures or guidelines established under that law is considered to meet the requirements of section 2264 as long as the licensee is compliant with, and submits a written statement certifying its compliance with, that federal law.

3. Employee, agent, representative or designee also a licensee. An employee, agent, representative or designee of a licensee that is also a licensee is exempt from section 2264 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.

If a licensee ceases to qualify for an exception under this section, the licensee has 180 days to comply with this chapter.

§ 2270. Penalties

The superintendent may take any enforcement action permitted under section 12-A against any person that violates any provision of this chapter.

§ 2271. Rules

The superintendent may adopt rules necessary to carry out the provisions of this chapter. Rules adopted pursuant to this section are routine technical rules as defined by Title 5, chapter 375, subchapter 2-A.

§ 2272. Effective date; implementation

This chapter takes effect January 1, 2021. A licensee must comply with section 2264 no later than January 1, 2021, except that a licensee must comply with section 2264, subsection 6 no later than January 1, 2023.

SUMMARY

This bill enacts the Maine Insurance Data Security Act. The bill establishes standards for information security programs based on ongoing risk assessment for protecting consumers' personal information. The bill establishes requirements for the investigation of and notification to the Superintendent of Insurance regarding cybersecurity events.