



130th MAINE LEGISLATURE

FIRST REGULAR SESSION-2021

Legislative Document

No. 51

H.P. 17

House of Representatives, January 13, 2021

An Act To Enact the Maine Insurance Data Security Act

Submitted by the Department of Professional and Financial Regulation pursuant to Joint Rule 204.

Received by the Clerk of the House on January 11, 2021. Referred to the Committee on Health Coverage, Insurance and Financial Services pursuant to Joint Rule 308.2 and ordered printed pursuant to Joint Rule 401.

A handwritten signature in cursive script that reads "R B. Hunt".

ROBERT B. HUNT
Clerk

Presented by Representative BLIER of Buxton.

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

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

3 **CHAPTER 24-B**

4 **MAINE INSURANCE DATA SECURITY ACT**

5 **§2261. Short title**

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

7 **§2262. Construction**

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

13 **§2263. Definitions**

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

16 **1. Authorized individual.** "Authorized individual" means an individual whose access
17 to the nonpublic information held by a licensee and its information systems is authorized
18 and determined by the licensee to be necessary and appropriate.

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

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

26 "Cybersecurity event" does not include the unauthorized acquisition of encrypted
27 nonpublic information if the encryption process or key is not also acquired, released or used
28 without authorization.

29 "Cybersecurity event" does not include an event with regard to which the licensee has
30 determined that the nonpublic information accessed by an unauthorized person has not been
31 used or released and has been returned or destroyed.

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

35 **5. Information security program.** "Information security program" means the
36 administrative, technical and physical safeguards that a licensee uses to access, collect,
37 distribute, process, protect, store, use, transmit, dispose of or otherwise handle nonpublic
38 information.

1 **6. Information system.** "Information system" means a discrete set of electronic
2 information resources organized for the collection, processing, maintenance, use, sharing,
3 dissemination or disposition of electronic information, as well as any specialized system
4 such as an industrial or process control system, a telephone switching and private branch
5 exchange system or an environmental control system.

6 **7. Insurance carrier.** "Insurance carrier" has the same meaning as in section 2204,
7 subsection 15.

8 **8. Licensee.** "Licensee" means a person licensed, authorized to operate or registered
9 or required to be licensed, authorized or registered pursuant to the insurance laws of this
10 State. "Licensee" does not include a purchasing group or a risk retention group chartered
11 and licensed in a state other than this State or a licensee that is acting as an assuming insurer
12 and is domiciled in another state or jurisdiction.

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

15 A. Knowledge factors, such as a password;

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

17 C. Inherence factors, such as a biometric characteristic.

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

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

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

26 (1) Social security number;

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

28 (3) Financial account number or credit or debit card number;

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

31 (5) Biometric records; or

32 C. Information or data, except age or gender, in any form or medium created by or
33 derived from a health care provider or a consumer and that relates to:

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

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

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

38 "Nonpublic information" does not include a consumer's personally identifiable information
39 that has been anonymized using a method no less secure than the so-called safe harbor

1 method under the federal Health Insurance Portability and Accountability Act of 1996,
2 Public Law 104-191.

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

6 A. Federal, state or local government records;

7 B. Widely distributed media; or

8 C. Disclosures to the general public that are required to be made by federal, state or
9 local law.

10 For the purposes of this definition, a licensee has a reasonable basis to believe that
11 information is lawfully made available to the general public if the licensee has taken steps
12 to determine that the information is of a type that is available to the general public and if a
13 consumer can direct that the information not be made available to the general public and,
14 if so, that the consumer has not done so.

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

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

21 **§2264. Information security program**

22 **1. Implementation of information security program.** Commensurate with the size
23 and complexity of the licensee, the nature and scope of the licensee's activities, including
24 its use of 3rd-party service providers, and the sensitivity of the nonpublic information used
25 by the licensee or in the licensee's possession, custody or control, a licensee shall develop,
26 implement and maintain a comprehensive, written information security program based on
27 the licensee's risk assessment and containing administrative, technical and physical
28 safeguards for the protection of nonpublic information and the licensee's information
29 systems.

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

32 A. Protect the security and confidentiality of nonpublic information and the security
33 of the licensee's information systems;

34 B. Protect against reasonably foreseeable threats or hazards to the security or integrity
35 of nonpublic information and the licensee's information systems;

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

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

40 **3. Risk assessment.** A licensee shall:

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

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

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

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

13 (1) Employee training and management;

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

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

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

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

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

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

31 (1) Place access controls on information systems, including controls to
32 authenticate and permit access only to authorized individuals to protect against the
33 unauthorized acquisition of nonpublic information;

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

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

40 (4) Protect, by encryption or other appropriate means, all nonpublic information
41 while it is being transmitted over an external network and all nonpublic

1 information stored on a laptop computer or other portable computing or storage
2 device or media;

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

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

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

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

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

15 (10) Implement measures to protect against destruction, loss or damage of
16 nonpublic information due to environmental hazards, such as fire and water
17 damage, or other catastrophes or technological failures; and

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

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

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

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

26 **5. Oversight by board of directors.** If a licensee has a board of directors, the board
27 or an appropriate committee of the board, at a minimum, shall require the licensee's
28 executive management or the executive management's delegates to:

29 A. Develop, implement and maintain the licensee's information security program; and

30 B. Report to the board in writing at least annually the following information:

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

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

39 If a licensee's executive management delegates any of its responsibilities under this section,
40 the licensee's executive management shall oversee each delegate's efforts with respect to
41 the development, implementation and maintenance of the licensee's information security

1 program and shall require each delegate to submit a report to the board pursuant to
2 paragraph B.

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

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

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

8 **7. Program adjustments.** A licensee shall monitor, evaluate and adjust, as
9 appropriate, its information security program consistent with any relevant changes in
10 technology, the sensitivity of the licensee's nonpublic information, internal or external
11 threats to nonpublic information and the licensee's own changing business arrangements,
12 such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements
13 and changes to information systems.

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

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

21 B. The goals of the incident response plan;

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

24 D. External and internal communications and information sharing;

25 E. Requirements for the remediation of any identified weaknesses in the licensee's
26 information systems and associated controls;

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

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

31 **9. Annual certification to superintendent.** By April 15th annually, an insurance
32 carrier domiciled in this State shall submit to the superintendent a written statement
33 certifying that the insurance carrier is in compliance with the requirements set forth in this
34 section. An insurance carrier shall maintain for examination by the superintendent all
35 records, schedules and data supporting this certification for a period of 5 years. To the
36 extent that an insurance carrier has identified areas, systems or processes that require
37 material improvement, updating or redesign, the insurance carrier shall document the
38 identification and the remedial efforts planned and underway to address such areas, systems
39 or processes. The documentation required pursuant to this subsection must be available for
40 inspection by the superintendent.

41 **§2265. Investigation of cybersecurity event**

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

6 A. Determine whether a cybersecurity event has occurred;

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

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

10 D. Perform or oversee the performance of reasonable measures to restore the security
11 of the information systems compromised in the cybersecurity event in order to prevent
12 further unauthorized acquisition, release or use of nonpublic information in the
13 licensee's possession, custody or control.

14 **2. System maintained by 3rd-party service provider.** If a licensee learns that a
15 cybersecurity event has or may have occurred in an information system maintained by a
16 3rd-party service provider, the licensee shall either use its best efforts to complete the steps
17 listed in subsection 1 or confirm that the 3rd-party service provider has completed those
18 steps.

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

22 **§2266. Notification of cybersecurity event**

23 **1. Notification to superintendent.** Notwithstanding Title 10, chapter 210-B, a
24 licensee shall notify the superintendent as promptly as possible but in no event later than 3
25 business days from a determination that a cybersecurity event has occurred if:

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

29 B. The licensee reasonably believes that the nonpublic information involved concerns
30 250 or more consumers residing in this State and that the cybersecurity event is either
31 of the following:

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

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

36 (a) Any consumer residing in this State; or

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

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

41 A. The date of the cybersecurity event;

- 1 B. A description of how the information was exposed, lost, stolen or breached,
2 including the specific roles and responsibilities of 3rd-party service providers, if any;
- 3 C. How the cybersecurity event was discovered;
- 4 D. Whether any lost, stolen or breached information has been recovered and, if so,
5 how this was done;
- 6 E. The identity of the source of the cybersecurity event;
- 7 F. Whether the licensee has filed a police report or has notified any regulatory,
8 government or law enforcement agencies and, if so, when the report was filed or the
9 notification was provided;
- 10 G. A description of the specific types of information acquired without authorization.
11 For purposes of this subsection, "specific types of information" includes, but is not
12 limited to, medical information, financial information and information allowing
13 identification of a consumer;
- 14 H. The period of time during which the information system was compromised by the
15 cybersecurity event;
- 16 I. The total number of consumers in this State affected by the cybersecurity event. The
17 licensee shall provide its best estimate in the notification provided pursuant to
18 subsection 1 to the superintendent and update this estimate with each subsequent report
19 to the superintendent pursuant to this section;
- 20 J. The results of any review conducted by or for the licensee identifying a lapse in
21 either automated controls or internal procedures or confirming that all automated
22 controls or internal procedures were followed;
- 23 K. A description of efforts being undertaken to remediate the situation that permitted
24 the cybersecurity event to occur;
- 25 L. A copy of the licensee's privacy policy and a statement outlining the steps the
26 licensee will take to investigate and notify consumers affected by the cybersecurity
27 event; and
- 28 M. The name and contact information of a person who is familiar with the
29 cybersecurity event and authorized to act for the licensee.
- 30 The licensee has a continuing obligation to update and supplement initial and subsequent
31 notifications to the superintendent concerning the cybersecurity event.
- 32 **3. Notification to consumers.** A licensee shall comply with Title 10, chapter 210-B,
33 as applicable, and, when required to notify the superintendent under subsection 1, provide
34 to the superintendent a copy of the notice sent to consumers pursuant to Title 10, chapter
35 210-B.
- 36 **4. Notice regarding cybersecurity events of 3rd-party service providers.** In the
37 case of a cybersecurity event in an information system maintained by a 3rd-party service
38 provider of which the licensee has become aware:
- 39 A. The licensee shall respond to the cybersecurity event as described under subsection
40 1; and

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

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

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

11 A. In the case of a cybersecurity event involving nonpublic information that is used
12 by a licensee that is acting as an assuming insurer or is in the possession, custody or
13 control of a licensee that is acting as an assuming insurer and that does not have a direct
14 contractual relationship with the affected consumers:

15 (1) The assuming insurer shall notify its affected ceding insurers and the
16 superintendent of its state of domicile within 3 business days of making the
17 determination that a cybersecurity event has occurred; and

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

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

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

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

32 **6. Notice regarding cybersecurity events of insurance carriers to producers of**
33 **record.** In the case of a cybersecurity event involving nonpublic information that is in the
34 possession, custody or control of a licensee that is an insurance carrier or its 3rd-party
35 service provider, and for which information a consumer accessed the insurance carrier's
36 services through an independent insurance producer, the insurance carrier shall notify the
37 producers of record of all affected consumers no later than the time consumers must be
38 notified under subsection 3 or as directed by the superintendent, except that the insurance
39 carrier is excused from this obligation for those instances in which it does not have the
40 current producer of record information for any individual consumer.

41 **§2267. Power of superintendent**

42 **1. Investigate.** The superintendent may examine and investigate the affairs of any
43 licensee to determine whether the licensee has been or is engaged in any conduct in

1 violation of this chapter. This power is in addition to the powers the superintendent has
2 under sections 220 and 221. Any such examination or investigation must be conducted
3 pursuant to those sections.

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

7 **§2268. Confidentiality**

8 **1. Materials held confidential.** Documents, materials and other information in the
9 control or possession of the bureau that are furnished by a licensee or an employee or agent
10 acting on behalf of the licensee pursuant to section 2264, subsection 9 or section 2266,
11 subsection 2, paragraph B, C, D, E, H, J or K or that are obtained by the superintendent in
12 an investigation or examination pursuant to section 2267 are confidential by law and
13 privileged, are not subject to Title 1, chapter 13, subchapter 1, are not subject to subpoena
14 and are not subject to discovery or admissible in evidence in any private civil action;
15 however, the superintendent is authorized to use the documents, materials and other
16 information in the furtherance of any regulatory or legal action brought as a part of the
17 superintendent's duties and to share them on a confidential basis in accordance with section
18 216, subsection 5.

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

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

27 **4. Final actions.** This chapter may not be construed to prohibit the superintendent
28 from releasing final, adjudicated actions that are open to public inspection pursuant to Title
29 1, chapter 13, subchapter 1 to a database or other clearinghouse service maintained by the
30 National Association of Insurance Commissioners, its affiliates or subsidiaries or any
31 successor organization.

32 **§2269. Application; exceptions**

33 **1. Small business exception.** A licensee with fewer than 10 employees, including any
34 independent contractors working for the licensee in the business of insurance, is exempt
35 from section 2264.

36 **2. Licensees subject to federal law.** The following provisions apply to licensees
37 subject to federal law.

38 A. A licensee that is subject to and in compliance with the federal Health Insurance
39 Portability and Accountability Act of 1996, Public Law 104-191 and related privacy,
40 security and breach notification regulations pursuant to 45 Code of Federal
41 Regulations, Parts 160 and 164 and the federal Health Information Technology for
42 Economic and Clinical Health Act, Public Law 111-5 is considered to meet the
43 requirements of this chapter, other than the requirements of section 2266, subsection 1
44 for notification to the superintendent, if:

1 (1) The licensee maintains a program for information security and breach
2 notification that treats all nonpublic information relating to consumers in this State
3 in the same manner as protected health information;

4 (2) The licensee annually submits to the superintendent a written statement
5 certifying that the licensee is in compliance with the requirements of this
6 paragraph; and

7 (3) The superintendent has not issued a determination finding that the applicable
8 federal regulations are materially less stringent than the requirements of this
9 chapter.

10 B. A licensee that is an insurance producer business entity, as licensed pursuant to
11 section 1420-E, owned by a depository institution and that maintains an information
12 security program in compliance with the standards for safeguarding customer
13 information as set forth pursuant to the federal Gramm-Leach-Bliley Act, 15 United
14 States Code, Sections 6801 and 6805 is considered to meet the requirements of section
15 2264 if:

16 (1) Upon request, the licensee produces documentation satisfactory to the
17 superintendent that independently validates the controlling depository institution's
18 adoption of an information security program that satisfies the standards for
19 safeguarding customer information;

20 (2) The licensee annually submits to the superintendent a written statement
21 certifying that the licensee is in compliance with the requirements of this
22 paragraph; and

23 (3) The superintendent has not issued a determination finding that the standards for
24 safeguarding customer information are materially less stringent than the
25 requirements of section 2264.

26 **3. Employee, agent, representative or designee also a licensee.** An employee, agent,
27 representative or designee of a licensee that is also a licensee is exempt from section 2264
28 and need not develop its own information security program to the extent that the employee,
29 agent, representative or designee is covered by the information security program of the
30 other licensee.

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

33 **§2270. Penalties**

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

36 **§2271. Rules**

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

40 **§2272. Effective date; implementation**

1 This chapter takes effect January 1, 2022. A licensee must comply with section 2264
2 no later than January 1, 2022, except that a licensee must comply with section 2264,
3 subsection 6 no later than January 1, 2023.

4 **SUMMARY**

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