

SENATE

HEATHER B. SANBORN, DISTRICT 28, CHAIR  
GEOFFREY M. GRATWICK, DISTRICT 9  
ROBERT A. FOLEY, DISTRICT 34

COLLEEN MCCARTHY REID, LEGISLATIVE ANALYST  
VERONICA SNOW, COMMITTEE CLERK



HOUSE

DENISE A. TEPLER, TOPSHAM, CHAIR  
MICHAEL F. BRENNAN, TOPSHAM  
ANNE MARIE MASTRACCIO, SANFORD  
HEIDI E. BROOKS, LEWISTON  
GINA M. MELARAGNO, AUBURN  
VICTORIA FOLEY, BIDDEFORD  
DWAYNE W. PRESCOTT, WATERBORO  
MARK JOHN BLIER, BUXTON  
JOSHUA MORRIS, TURNER  
GREGORY LEWIS SWALLOW, HOULTON

STATE OF MAINE  
ONE HUNDRED AND TWENTY-NINTH LEGISLATURE  
COMMITTEE ON HEALTH COVERAGE, INSURANCE AND FINANCIAL SERVICES

TO: Sen. Michael E. Carpenter, Senate Chair  
Rep. Donna Bailey, House Chair  
Joint Standing Committee on Judiciary

FROM: Sen. Heather B. Sanborn, Senate Chair  
Rep. Denise A. Tepler, House Chair  
Joint Standing Committee on Health Coverage, Insurance and Financial Services

DATE: July 7, 2020

RE: Public Records Exception Review of LD 1995

*all  
by  
wants*

We are writing to request review of LD 1995, An Act To Enact the Maine Insurance Data Security Act pursuant to Title 1, section 434, subsection 2. This bill was submitted by the Bureau of Insurance. The committee held a public hearing on the bill in compliance with the public hearing requirement of Title 1, section 434, subsection 1. The committee voted unanimously OTP-A; a copy of the bill and draft committee amendment is attached. We note that the bill as drafted includes an effective date of January 1, 2021 and, given the delay in completing the Legislature's work, we anticipate further amending the bill to extend that date.

LD 1995 enacts the Maine Insurance Data Security Act. The bill establishes standards for information security programs used by insurers licensed in the State. The bill establishes requirements for the filing of information by insurers related to their information security programs and for the investigation of and notification to the Superintendent of Insurance regarding cybersecurity events. There is a provision included in LD 1995 that protects as confidential documents, materials and other information provided to the Bureau of Insurance related to an insurer's information security program or notification of cybersecurity events as well as information obtained by the Bureau of Insurance during an investigation. See proposed section §2268 on pages 10 and 11 of LD 1995.

We have reviewed the statutory criteria in Title 1, section 434, subsection 2 and we offer the following comments on LD 1995:

A. Whether the record protected by the proposed exception needs to be collected and maintained.

*pp 14-15  
of  
packet*

*(1)*

*B. The value to the agency or official or to the public in maintaining a record protected by the proposed exception.*

A & B. It is important for the Bureau of Insurance to have access to documents and information related to an insurer's information security plans and cybersecurity events to ensure that the standards enacted in the bill are complied with and that personal information and financial information related to insurance consumers and insurance companies are protected as much as possible and not subject to hacking or other unauthorized access. This is sensitive information that insurance regulators previously did not have access to and the confidentiality protections are based on uniform national standards and are consistent with the existing provisions.

*C. Whether federal law requires a record covered by the proposed exception to be confidential.*

C. We are not aware of any federal law that applies here.

*D. Whether the proposed exception protects an individual's privacy interest and, if so, whether that interest substantially outweighs the public interest in the disclosure of records.*

D. We believe that the confidentiality of this information filed with the Bureau of Insurance is an important concern because it could involve both proprietary information about an insurer's information security program and personal information about insurance consumers. We believe the privacy interests of insurance companies and insurance consumers outweigh the public interest in disclosure of all materials, but note that the provision does authorize the release of certain information related to a cybersecurity event, including the date of the event, whether a police report was filed or law enforcement notified, a description of the information that was compromised, the number of consumers affected and the steps that will be taken by the insurer to investigate and notify consumers. public disclosure.

*E. Whether public disclosure puts a business at a competitive disadvantage and, if so, whether that business's interest substantially outweighs the public interest in the disclosure of records.*

E. Yes, we believe that public disclosure about information security programs and specific cybersecurity events may affect an insurer's security and its competitive position. Public disclosure may also provide information that can be used to enable unauthorized access in the future.

*F. Whether public disclosure compromises the position of a public body in negotiations and, if so, whether that public body's interest substantially outweighs the public interest in the disclosure of records.*

F. We do not believe paragraph F is applicable.

*G. Whether public disclosure jeopardizes the safety of a member of the public or the public in general and, if so, whether that safety interest substantially outweighs the public interest in the disclosure of records.*

(2)

G. Yes, public disclosure of information related to cybersecurity events and information security programs may jeopardize the security of personal and financial information of insurance consumers.

*H. Whether the proposed exception is as narrowly tailored as possible.*

H. Although the language as drafted appears broad, we believe it is necessary to protect against unauthorized access to cybersecurity information about insurance companies and insurance consumers. And, as noted above, the provision does not protect from public disclosure certain information related to a cybersecurity event, including the date of the event, whether a police report was filed or law enforcement notified, a description of the information that was compromised, the number of consumers affected and the steps that will be taken by the insurer to investigate and notify consumers.

*I. Any other criteria that assist the review committee in determining the value of the proposed exception as compared to the public's interest in the record protected by the proposed exception.*

I. We want to point out that the changes proposed in the bill, including the confidentiality provisions, are being made to enact a model law adopted by the National Association of Insurance Commissioners in order to maintain the State's compliance with uniform national standards and with the NAIC's accreditation requirements for state insurance regulators.

Thank you for your consideration of our comments. Please contact us or our legislative analyst, Colleen McCarthy Reid, if you have any questions or need additional information. We look forward to discussing this with your committee in work session.

Enclosure: LD 1995 and Draft Committee Amendment

cc: Members, Joint Standing Committee on Health Coverage, Insurance and Financial Services

(2)



# 129th MAINE LEGISLATURE

## SECOND REGULAR SESSION-2020

---

Legislative Document

No. 1995

S.P. 697

In Senate, January 8, 2020

### An Act To Enact the Maine Insurance Data Security Act

---

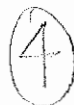
Submitted by the Department of Professional and Financial Regulation pursuant to Joint Rule 203.

Reference to the Committee on Health Coverage, Insurance and Financial Services suggested and ordered printed.

A handwritten signature in black ink that reads "D M Grant".

DAREK M. GRANT  
Secretary of the Senate

Presented by Senator FOLEY of York.



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 standards for the investigation  
9 of and notification to the superintendent regarding a cybersecurity event applicable to  
10 licensees. This chapter may not be construed to create or imply a private cause of action  
11 for violation of its provisions or to curtail a private cause of action that would otherwise  
12 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 known to  
17 and screened by a licensee and whose access to the nonpublic information held by the  
18 licensee and its information systems is determined by the licensee to be necessary and  
19 appropriate.

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

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

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

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

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



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

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

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

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

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

20           A. Knowledge factors, such as a password;

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

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

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

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

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

31                   (1) Social security number;

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

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

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

36                   (5) Biometric records; or

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

- 1           (1) The past, present or future physical, mental or behavioral health or condition  
2           of a consumer or a member of the consumer's family;  
3           (2) The provision of health care to a consumer; or  
4           (3) Payment for the provision of health care to a consumer.

insert →

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

- 8           A. Federal, state or local government records;  
9           B. Widely distributed media; or  
10           C. Disclosures to the general public that are required to be made by federal, state or  
11           local law.

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

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

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

23           **§2264. Information security program**

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

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

- 34           A. Protect the security and confidentiality of nonpublic information and the security  
35           of the information system;  
36           B. Protect against threats or hazards to the security or integrity of nonpublic  
37           information and the information system;  
38           C. Protect against unauthorized access to or use of nonpublic information and  
39           minimize the likelihood of harm to any consumer; and

(7)

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

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

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

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

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

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

- 17 (1) Employee training and management;
- 18 (2) Information systems, including network and software design, as well as  
19 information classification, governance, processing, storage, transmission and  
20 disposal; and
- 21 (3) Detecting, preventing and responding to attacks, intrusions or other system  
22 failures; and

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

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

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

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

- 34 (1) Place access controls on information systems, including controls to  
35 authenticate and permit access only to authorized individuals to protect against  
36 the unauthorized acquisition of nonpublic information;
- 37 (2) Identify and manage the data, personnel, devices, systems and facilities that  
38 enable the licensee to achieve its business purposes in accordance with their  
39 relative importance to business objectives and the licensee's risk management  
40 strategy;





- 1           (3) Restrict to only authorized individuals access at physical locations containing  
2           nonpublic information;
- 3           (4) Protect, by encryption or other appropriate means, all nonpublic information  
4           while it is being transmitted over an external network and all nonpublic  
5           information stored on a laptop computer or other portable computing or storage  
6           device or media;
- 7           (5) Adopt secure development practices for applications developed and used by  
8           the licensee and procedures for evaluating, assessing or testing the security of  
9           externally developed applications used by the licensee;
- 10          (6) Modify the information system in accordance with the licensee's information  
11          security program;
- 12          (7) Use effective controls, which may include multifactor authentication  
13          procedures, for individuals accessing nonpublic information;
- 14          (8) Regularly test and monitor systems and procedures to detect actual and  
15          attempted attacks on or intrusions into information systems;
- 16          (9) Include audit trails within the information security program designed to  
17          detect and respond to cybersecurity events and designed to reconstruct material  
18          financial transactions sufficient to support normal operations and obligations of  
19          the licensee;
- 20          (10) Implement measures to protect against destruction, loss or damage of  
21          nonpublic information due to environmental hazards, such as fire and water  
22          damage, or other catastrophes or technological failures; and
- 23          (11) Develop, implement and maintain procedures for the secure disposal of  
24          nonpublic information in any format;
- 25          C. Include cybersecurity risks in the licensee's enterprise risk management process;
- 26          D. Stay informed regarding emerging threats or vulnerabilities and use reasonable  
27          security measures when sharing information relative to the character of the sharing  
28          and the type of information shared; and
- 29          E. Provide its personnel with cybersecurity awareness training that is updated as  
30          necessary to reflect risks identified by the licensee in the risk assessment.
- 31          **5. Oversight by board of directors. If a licensee has a board of directors, the board**  
32          **or an appropriate committee of the board at a minimum shall:**
- 33                A. Require the licensee's executive management or the executive management's  
34                delegates to develop, implement and maintain the licensee's information security  
35                program; and
- 36                B. Require the licensee's executive management or the executive management's  
37                delegates to report to the board in writing at least annually the following information:
- 38                    (1) The overall status of the licensee's information security program and the  
39                    licensee's compliance with this chapter; and

9

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

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

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

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

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

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

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

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

30           B. The goals of the incident response plan;

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

33           D. External and internal communications and information sharing;

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

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

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

1           **9. Annual certification to superintendent.** By February 15th annually, an  
2 insurance carrier domiciled in this State shall submit to the superintendent a written  
3 statement certifying that the insurance carrier is in compliance with the requirements set  
4 forth in this section. An insurance carrier shall maintain for examination by the  
5 superintendent all records, schedules and data supporting this certification for a period of  
6 5 years. To the extent that an insurance carrier has identified areas, systems or processes  
7 that require material improvement, updating or redesign, the insurance carrier shall  
8 document the identification and the remedial efforts planned and under way to address  
9 such areas, systems or processes. The documentation required pursuant to this subsection  
10 must be available for inspection by the superintendent.

11           **§2265. Investigation of cybersecurity event**

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

- 17           A. Determine whether a cybersecurity event has occurred;  
18           B. Assess the nature and scope of the cybersecurity event;  
19           C. Identify any nonpublic information that may have been involved in the  
20 cybersecurity event; and  
21           D. Perform or oversee reasonable measures to restore the security of the information  
22 systems compromised in the cybersecurity event in order to prevent further  
23 unauthorized acquisition, release or use of nonpublic information in the licensee's  
24 possession, custody or control.

25           **2. System maintained by 3rd-party service provider.** If a licensee learns that a  
26 cybersecurity event has or may have occurred in an information system maintained by a  
27 3rd-party service provider, the licensee shall complete the steps listed in subsection 1 or  
28 confirm and document that the 3rd-party service provider has completed those steps.

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

32           **§2266. Notification of cybersecurity event**

33           **1. Notification to superintendent.** Notwithstanding Title 10, chapter 210-B, a  
34 licensee shall notify the superintendent as promptly as possible but in no event later than  
35 72 hours from a determination that a cybersecurity event has occurred if:

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

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

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

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

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

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

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

13 A. The date of the cybersecurity event;

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

16 C. How the cybersecurity event was discovered;

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

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

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

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

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

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

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

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

1           L. A copy of the licensee's privacy policy and a statement outlining the steps the  
2           licensee will take to investigate and notify consumers affected by the cybersecurity  
3           event; and

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

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

8           **3. Notification to consumers.** A licensee shall comply with Title 10, chapter 210-B,  
9           as applicable, and, when required to notify the superintendent under subsection 1, provide  
10          to the superintendent a copy of the notice sent to consumers pursuant to Title 10, chapter  
11          210-B.

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

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

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

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

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

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

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

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

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

- 1           (1) The assuming insurer shall notify its affected ceding insurers and the  
2           superintendent of its state of domicile within 72 hours of receiving notice from its  
3           3rd-party service provider that a cybersecurity event has occurred; and
- 4           (2) The ceding insurers that have a direct contractual relationship with affected  
5           consumers shall fulfill the consumer notification requirements imposed under the  
6           laws of this State and any other notification requirements relating to a  
7           cybersecurity event imposed under this section.

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

17           **§2267. Power of superintendent**

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

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

27           **§2268. Confidentiality**

28           **1. Materials held confidential.** Documents, materials and other information in the  
29           control or possession of the bureau that are furnished by a licensee or an employee or  
30           agent acting on behalf of the licensee pursuant to section 2264, subsection 9 or section  
31           2266, subsection 2, paragraph B, C, D, E, H, J or K or that are obtained by the  
32           superintendent in an investigation or examination pursuant to section 2267 are  
33           confidential by law and privileged, are not subject to Title 1, chapter 13, subchapter 1, are  
34           not subject to subpoena and are not subject to discovery or admissible in evidence in any  
35           private civil action; however, the superintendent is authorized to use the documents,  
36           materials and other information in the furtherance of any regulatory or legal action  
37           brought as a part of the superintendent's duties and to share them on a confidential basis  
38           in accordance with section 216, subsection 5.

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

*no  
change  
in  
amend-  
ment*

14

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

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

10           **§2269. Application; exceptions**

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

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

19           3. Employee, agent, representative or designee also a licensee. An employee,  
20 agent, representative or designee of a licensee that is also a licensee is exempt from  
21 section 2264 and need not develop its own information security program to the extent that  
22 the employee, agent, representative or designee is covered by the information security  
23 program of the other licensee.

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

26           **§2270. Penalties**

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

29           **§2271. Rules**

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

33           **§2272. Effective date; implementation**

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

1 **SUMMARY**

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



OTP-A as voted by HCIFS

L.D. 1995

Date:

(Filing No. S- )

**HEALTH COVERAGE, INSURANCE AND FINANCIAL SERVICES**

Reproduced and distributed under the direction of the Secretary of the Senate.

**STATE OF MAINE**

**SENATE**

**129TH LEGISLATURE**

**SECOND REGULAR SESSION**

COMMITTEE AMENDMENT " " to S.P. 697, L.D. 1995, Bill, "An Act To Enact the Maine Insurance Data Security Act"

Amend the bill in section 1 in §2262 in the first paragraph in the first line (page 1, line 8 in L.D.) by inserting after the following: "and" the following: 'exclusive'

Amend the bill in section 1 in §2263 by striking out all of subsection 1 (page 1, lines 16 to 19 in L.D.) and inserting the following:

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

Amend the bill in section 1 in §2263 by striking out all of subsection 7 (page 2, lines 10 to 12 in L.D.) and inserting the following:

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

Amend the bill in section 1 in §2263 in subsection 10 by inserting at the end a new blocked paragraph to read:

"Nonpublic information" does not include a consumer's personally identifiable information that has been anonymized using a method no less secure than the safe harbor method under the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.'

Amend the bill in section 1 in §2264 in subsection 2 in paragraph B in the first line (page 3, line 36 in L.D.) by inserting after the following: "against" the following: 'reasonably foreseeable'

Amend the bill in section 1 in §2264 in subsection 6 in paragraph B in the last line (page 6, line 16 in L.D.) by inserting after the following: "accessible" the following: 'to'

Amend the bill in section 1 in §2264 in subsection 9 in the first line (page 7, line 1 in L.D.) by striking out the following: "February" and inserting the following: 'April'

17

1 Amend the bill in section 1 in §2265 by striking out all of subsection 2 (page 7, lines  
2 25 to 28 in L.D.) and inserting the following:

3 '2. System maintained by 3rd-party service provider. If a licensee learns that a  
4 cybersecurity event has or may have occurred in an information system maintained by a  
5 3rd-party service provider, the licensee shall either use its best efforts to complete the  
6 steps listed in subsection 1 or confirm that the 3rd-party service provider has completed  
7 those steps.'

8 Amend the bill in section 1 in §2266 in subsection 1 in the 3rd line (page 7, line 35 in  
9 L.D.) by striking out the following: "72 hours" and inserting the following: '3 business  
10 days'

11 Amend the bill in section 1 in §2266 in subsection 5 in paragraph A in subparagraph  
12 (1) in the 2nd line (page 9, line 32 in L.D.) by striking out the following: "72 hours" and  
13 inserting the following: '3 business days'

14 Amend the bill in section 1 in §2266 in subsection 5 in paragraph B in subparagraph  
15 (1) in the 2nd line (page 10, line 2 in L.D.) by striking out the following: "72 hours" and  
16 inserting the following: '3 business days'

17 Amend the bill in section 1 in §2266 in subsection 6 in the 6th line (page 10, line 13  
18 in L.D.) by striking out the following: "as soon as practicable" and inserting the  
19 following: 'no later than the time consumers must be notified under subsection 3 or'

20 Amend the bill in section 1 in §2269 in subsection 1 in the last line (page 11, line 12  
21 in L.D.) by inserting after the following: "contractors" the following: 'working for the  
22 licensee in the business of insurance'

23 Amend the bill in section 1 in §2269 by striking out all of subsection 2 (page 11, lines  
24 13 to 18 in L.D.) and inserting the following:

25 '2. Licensees subject to federal law. The following provisions apply to licensees  
26 subject to federal law.

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

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

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

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

18

1 B. A licensee that is a producer business entity owned by a depository institution and  
2 maintains an information security program in compliance with the standards for  
3 safeguarding customer information as set forth pursuant to the Gramm-Leach-Bliley  
4 Act, 15 United States Code, Sections 6801 and 6805 is considered to meet the  
5 requirements of section 2264 if:

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

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

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

16 Amend the bill by relettering or renumbering any nonconsecutive Part letter or  
17 section number to read consecutively.

### 18 SUMMARY

19 This amendment makes the following changes to the bill.

20 1. It clarifies the definitions of "authorized individual," "insurance carrier" and  
21 "nonpublic information."

22 2. It extends the time period for notification of a cybersecurity event from 72 hours  
23 to no later than 3 business days.

24 3. It changes the date that an insurance carrier annually certify compliance with the  
25 requirements for an information security program from February 15th to April 15th.

26 4. It clarifies the exemption for small business licensees and for certain licensees  
27 subject to federal law.

(19)