



Janet T. Mills
Governor

STATE OF MAINE
DEPARTMENT OF PROFESSIONAL
AND FINANCIAL REGULATION
BUREAU OF INSURANCE
34 STATE HOUSE STATION
AUGUSTA, MAINE
04333-0034

Eric A. Cioppa
Superintendent

Bulletin 462

Maine Insurance Data Security Act

The Maine Insurance Data Security Act is effective January 1, 2022.¹ The Act establishes standards applicable to licensees of the Bureau of Insurance for data security, investigation of cybersecurity events, and notification to the Bureau of these events.² The purpose of this Bulletin is to guide licensees on how to comply with the Act.

Scope. The Act applies to all entities and persons who are licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the Maine Insurance Code. The Act does not apply to purchasing groups or risk retention groups chartered and licensed in other states or to licensees acting in their capacity as assuming insurers and not domiciled in Maine.³

Information Security Program. Licensees must develop, implement, and maintain a comprehensive written information security program that is commensurate with the licensee's size and complexity, the nature and scope of its activities, and the sensitivity of the nonpublic information that the licensee uses or is in the licensee's custody, possession, or control.⁴ The licensee must base its information security program on the licensee's risk assessment. This means that any licensee that must develop an information security program must also conduct an assessment of the risks that it faces. The information security program's safeguards must also address the licensee's use of third-party service providers. This is especially important because third-party service providers often have access to sensitive information and because the access can be a route for unwanted intrusions on that information. The information security program must cover data and information in electronic and other formats. Licensees must comply with Section 2264 by January 1, 2022.⁵

¹ P.L. 2021, c. 24, An Act To Enact the Maine Insurance Data Security Act (L.D. 51).

² 24-A M.R.S. § 2262.

³ 24-A M.R.S. § 2263(8).

⁴ 24-A M.R.S. § 2264(1).

⁵ 24-A M.R.S. § 2272.



PRINTED ON RECYCLED PAPER

OFFICES LOCATED AT 76 NORTHERN AVENUE, GARDINER, MAINE 04345
www.maine.gov/insurance

Phone: (207) 624-8475

TTY: Please call Maine Relay 711

Consumer Assistance: 1-800-300-5000

Fax (207) 624-8599

Licensees with fewer than ten employees are exempt from the requirements of Section 2264.⁶ This headcount includes independent contractors, but only if they work for the licensee in the business of insurance. For example, someone whose only work for a licensee is providing landscaping or snowplowing services is not considered an independent contractor under the Act.

Third-Party Service Providers. Licensees subject to Section 2265 must exercise due diligence in selecting third-party service providers.⁷ By January 1, 2023, a licensee must require its third-party service providers to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that the third-party service providers either have access to or hold.

Annual Certifications. The Act requires annual certifications concerning compliance with these requirements:

- *Maine Domestic Insurers.* Under § 2264(9), each Maine domestic insurer must certify its compliance with the Act's information security program requirements. The insurer must maintain all records, schedules, and data supporting each certification for the Superintendent's examination for five years from the date the certification is submitted. An insurance holding company system may submit one statement certifying compliance on behalf of all domestic insurers in the holding company system. If an insurer has identified areas, systems, or processes that require material improvement, updating or redesign, the insurer, either directly or through an affiliate, must document the problems it has identified and the remedial efforts that are planned and underway, and must make that documentation available for inspection by the Bureau. Information furnished to the Bureau under Section 2264(9) is confidential under Section 2268(1).
- *HIPAA- and HITECH-Compliant Licensees.* A licensee subject to HIPAA⁸ and HITECH⁹ that maintains a program for information security and breach notification that treats all nonpublic information related to Maine consumers in the same manner as protected health information is deemed to meet the requirements of Section 2266.¹⁰ This does not apply to the notification requirement under Subsection 2266(1).
- *Producer Business Entity Licensees.* An insurance producer business entity that is owned by a depository institution and maintains an information security program in compliance with the standards for safeguarding consumer information of 15 U.S.C. §§ 6801 and 6805 is also deemed to have complied with Section 2264 under certain circumstances.¹¹ The licensee must, on request, produce evidence satisfactory to the Superintendent independently validating that the parent depository institution has adopted an information security program that satisfies the federal standards for safeguarding consumer information.

⁶ 24-A M.R.S. § 2269(1).

⁷ 24-A M.R.S. § 2264(6).

⁸ Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 and related privacy, security, and breach notification regulations pursuant to 45 C.F.R. Parts 160 and 164.

⁹ Health Information Technology for Economic and Clinical Health Act, Public Law 111-5.

¹⁰ 24-A M.R.S. § 2269(2)(A).

¹¹ 24-A M.R.S. § 2269(2)(B).

A licensee must submit its certification by April 15th each year and may use the omnibus certification form that will be posted on the Bureau's website or submit its own certification using the language in the posted form. If a licensee no longer qualifies for the HIPAA or bank subsidiary safe harbor, it must notify the Superintendent within three months after that change in status.

Cybersecurity Event Investigations. When a licensee learns that a cybersecurity event has or might have occurred, the licensee must conduct a prompt investigation in accordance with the Act.¹² The licensee may designate an outside vendor or service provider to act on its behalf. The investigation must cover at least the following, as applicable:

- determining whether a cybersecurity event occurred;
- assessing the nature and scope of the cybersecurity event;
- identifying any nonpublic information involved in the cybersecurity event; and
- taking steps to restore the security of the information in order to prevent further unauthorized acquisition, release, or use of nonpublic information in the licensee's possession, custody, or control.

If a licensee learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, the licensee must either use its best efforts to conduct an investigation using the steps described above or confirm that the third-party service provider has completed those steps.¹³

Each licensee must maintain records concerning each cybersecurity event for at least five years from the date of the event, and must produce such records to the Superintendent upon demand.¹⁴

Notification of a Cybersecurity Event. Notification is an important part of the Act. It covers notification to the Superintendent and, in conjunction with Maine's Notice of Risk to Personal Data Act,¹⁵ to consumers.

Notification to the Superintendent. As promptly as possible but in no event later than three business days after determining that a cybersecurity event has occurred, a licensee must notify the Superintendent that of the event, if:

- The licensee is an insurer domiciled in Maine.
- The licensee is a producer whose home state is Maine.
- The licensee reasonably believes that the cybersecurity event involves nonpublic information of 250 or more Maine residents and either:
 - a. state or federal laws require that a notice concerning the cybersecurity event be provided to a government body, self-regulatory agency, or another supervisory body; or

¹² 24-A M.R.S. § 2265(1).

¹³ 24-A M.R.S. § 2265(2).

¹⁴ 24-A M.R.S. § 2265(3).

¹⁵ 10 M.R.S. Ch. 210-B.

- b. the event has a reasonable likelihood of materially harming any Maine resident or a material part of the licensee's normal operations.¹⁶

Licenses notifying the Superintendent of cybersecurity events must use the form and process to be announced on the Bureau's website.¹⁷ A licensee that has reported a cybersecurity event has an ongoing obligation to update its initial and any further notifications.

Notification to Consumers. The Act requires each licensee to comply with the applicable provisions of Maine's Notice of Risk to Personal Data Act.¹⁸ The licensee must also provide the Superintendent with templates of any consumer notifications required under that law.

Notification Involving Third-party Service Providers. When a cybersecurity event involving an information system maintained by a third-party service provider affects licensees, the licensees must treat such event as requiring notice to the Superintendent, if the licensees have actual knowledge of the event.¹⁹ However, a licensee may allow the third-party service provider to provide the required notice to the Superintendent.

Notification to Ceding Insurers. If a cybersecurity event involves a reinsurer that does not have a direct contractual relationship with the Maine residents affected by the event, the reinsurer is not responsible for providing notice to the affected consumers. Instead, the reinsurer must notify its domiciliary regulator and the affected ceding insurers within three business days after determining that a cybersecurity event has occurred, or after receiving notice from a third-party service provider that a cybersecurity event has occurred.²⁰ Ceding insurers that have a direct contractual relationship with affected Maine residents must comply with the consumer notification requirements of the Act and the Notice of Risk to Personal Data Act.

Notice by Insurers to Producers of Record. If the cybersecurity event involves nonpublic information that is in the possession, custody, or control of an insurer or its third-party service provider, the insurer must notify each affected consumer's producer of record, if the consumer accessed services through an independent insurance producer and the insurer has current producer-of-record information for the consumer. This notice must be given no later than the notice to the affected consumer, unless otherwise directed by the Superintendent.²¹

The Act specifically allows licensees to agree with other licensees, third-party services providers, or other persons to meet the investigation requirements of Section 2265 or the notice requirements of Section 2266.²² For example, an insurer producer business entity may comply

¹⁶ 24-A M.R.S. § 2266(1).

¹⁷ 24-A M.R.S. § 2266(2).

¹⁸ 24-A M.R.S. § 2266(3).

¹⁹ 24-A M.R.S. § 2266(4).

²⁰ 24-A M.R.S. § 2266(5).

²¹ 24-A M.R.S. § 2266(6).

²² 24-A M.R.S. § 2266(4).

with these requirements on behalf of the producers that it employs, and a law firm may do so for its client.

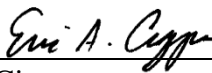
Confidentiality. The Act recognizes the need for some balance between consumers' need to have some information about cybersecurity events involving licensees that they do business with and licensees' need to protect the confidentiality of the processes that they use to secure their information systems. The Act therefore treats as confidential the information security program information that the Superintendent obtains from licensees under Section 2264(9), as described above; some of the cybersecurity event information that licensees must report to the Superintendent under Section 2266(2); and information obtained in an investigation or examination under Section 2267.²³

It is worth explaining what is confidential and not confidential in the notification required under Section 2266(2). The information covered by Subsections 2268(1)(B), (C), (D), (E), (H), (J), and (K) is confidential. This includes the mechanism of the cybersecurity event, how the licensee discovered the event, whether and how the licensee recovered the information at issue, the identity of the attacker, the period of compromise, the results of any forensic review of the event, and the licensee's steps to remediate the vulnerability. The information covered by Subsections 2268(2)(A), (F), (G), (I), (L), and (M) is public. This includes the fact that a cybersecurity event has happened, the reporting licensee's identity, whether reports have been filed with law enforcement officials, the types of affected information, the number of affected people, the affected licensee's privacy policy and investigation and notification steps, and the licensee's contact person are public information.

When the information described in Section 2268(2) is in the Superintendent's possession or control, it is not only confidential but also not subject to subpoena or discovery nor admissible in evidence in any private civil action. This status does not prevent the Superintendent from using this information in any regulatory or legal action made as part of the Superintendent's duties, nor from sharing this information under Section 216(5).

Last, Bureau staff will add a page to our website with information about the Act, including the certification form and notification form mentioned at pages 2 and 3. Anyone interested in receiving further announcements about the Act is encouraged to sign up at the "Get Notified" box on the Bureau's home page, www.maine.gov/pfr/insurance.

October 4, 2021



Eric A. Cioppa
Superintendent of Insurance

NOTE: This Bulletin is intended solely for informational purposes. It is not intended to set forth legal rights, duties, or privileges, nor is it intended to provide legal advice. Readers should consult applicable statutes and rules and contact the Bureau of Insurance if additional information is needed.

²³ 24-A M.R.S. § 2268(1).