STATE OF MAINE
DEPARTMENT OF PROFESSIONAL & FINANCIAL REGULATION
BUREAU OF INSURANCE

Janet T. Mills
Governor

Anne L. Head
DPFR Commissioner

Timothy N. Schott
Acting Superintendent

Bulletin 468

Maine Law Concerning Cybersecurity Events

(Supersedes Bulletin 462)

This Bulletin supersedes Bulletin 462 concerning the Maine Insurance Data Security Act (IDSA), which became effective January 1, 2022.[1] The purpose of this Bulletin is to explain the interaction between IDSA and Maine's omnibus cybersecurity breach law, the Notice of Risk to Personal Data Act (NRPDA).[2] This Bulletin also notifies licensees of some changes in the Bureau of Insurance's (Bureau) implementation of IDSA and offers guidance on compliance with IDSA and NRPDA.

IDSA establishes standards applicable to licensees of the Bureau for data security, investigation of cybersecurity events, and notification to the Bureau of these events.[3] NRPDA provides rules for notifying consumers and the Bureau of security breaches when IDSA does not apply.

Insurance Data Security Act

Scope. IDSA applies to all entities and persons who are licensed, authorized to operate, or registered, or who are required to be licensed, authorized, or registered pursuant to the Maine Insurance Code. IDSA 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.[4]

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.[5] 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 must cover data and

[1] P.L. 2021, c. 24, An Act To Enact the Maine Insurance Data Security Act (L.D. 51), enacted as 24-A M.R.S. §§ 2261 - 2272.

[2] 10 M.R.S. §§ 1346 – 1350-B.

[3] 24-A M.R.S. § 2262.

[4] 24-A M.R.S. § 2263(8).

[5] 24-A M.R.S. § 2264(1).

information in electronic and other formats. Licensees have been required to comply with Section 2264 since January 1, 2022.[6]

Licensees with fewer than ten employees are exempt from the requirements of Section 2264.[7] 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 IDSA.

Third-Party Service Providers. Licensees subject to Section 2265 must exercise due diligence in selecting third-party service providers.[8] 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 that access can be a route for unwanted intrusions on that information. This is true even if they provide services such as information technology maintenance and do not use personal information for their own purposes. As of 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 hold or have access to.

Annual Certifications. IDSA covers annual certifications concerning compliance with these requirements:

- *Maine Domestic Insurance Carriers.* Under § 2264(9), each Maine domestic insurance carrier must certify its compliance with IDSA's information security program requirements. This certification is mandatory. Maine domestic carriers can comply with this requirement by checking the appropriate box on the Domestic Insurer Compliance Certification form posted to our website. Maine domestic carriers that are not subject to HIPAA[9] and HITECH[10] should check the first box under part 3 of the form. A Maine domestic carrier that is subject to those federal laws should check the second box under part 3 of the form if its HIPAA/HITECH-compliant program for information security and breach notification treats all nonpublic information relating to consumers in this State in the same manner as protected health information. Otherwise, it should check the first box.

  IDSA imports the definition of "insurance carrier" from the Insurance Information and Privacy Protection Act.[11] It is important to understand what entities this definition applies to:

  - Entities that must be licensed in order to assume risk, such as insurers, nonprofit hospitals, medical or health care service organizations, health maintenance organizations, and multiple employer welfare arrangements;

[6] 24-A M.R.S. § 2272.

[7] 24-A M.R.S. § 2269(1).

[8] 24-A M.R.S. § 2264(6).

[9] 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.

[10] Health Information Technology for Economic and Clinical Health Act, Public Law 111-5.

[11] 24-A M.R.S. § 2204(15).

- Self-funded health plans subject to § 2848-A;
- Preferred provider arrangement administrators under § 2671; and
- Third-party administrators under § 1901, providing services for non-carrier entities.

The carrier 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 a carrier has identified areas, systems, or processes that require material improvement, updating, or redesign, the carrier, 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).

- *Non-Carrier Licensees and Non-Domestic Carriers.* Unlike the mandatory certification that applies to Maine domestic risk-bearing entities defined as insurance carriers in 24-A M.R.S. § 2204(15), the two certifications available to other licensees are optional. Each provides a safe harbor to a licensee entity that elects to use it, but licensees may comply instead with Section 2266 or 2264 as described below:
  - *HIPAA- and HITECH-Compliant Licensees.* A licensee subject to HIPAA and HITECH 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. This safe harbor does not exempt the licensee from the notification requirement under Subsection 2266(1).[12]
  - *Bank-Owned Producer Business Entities*. 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 under the Gramm-Leach-Bliley Act (GLBA) at 15 U.S.C. §§ 6801 and 6805 is also deemed to have complied with Section 2264 under certain circumstances.[13] 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.

A licensee must submit its certification by April 15 each year. The Bureau has replaced the previous omnibus certification form with two certification forms. One is for domestic insurance carriers only, and includes an option to elect the HIPAA/HITECH safe harbor. The other form is for non-domestic carriers and other licensees, domestic or non-domestic, that elect the HIPAA/HITECH or bank subsidiary GLBA safe harbor.

[12] 24-A M.R.S. § 2269(2)(A).

[13] 24-A M.R.S. § 2269(2)(B).

Carriers and other licensees may submit their own certifications using the language in the posted forms. A licensee no longer qualifying for the HIPAA/HITECH or bank subsidiary safe harbor must notify the Superintendent within 180 days after that change in status.[14]

As mentioned above, licensees that have fewer than ten employees are exempt from IDSA's information security program requirements. This includes, for example, producers and adjusters working on a bona fide basis on their own. These licensees also do not have to file the HIPAA/HITECH certification or the GLBA certification. Licensees, such as producers or adjusters, who are employed by another licensee, such as an agency or adjusting firm, do not need to file their own HIPAA/HITECH or GLBA certification forms. An employer meeting the ten-employee threshold would file the forms on their behalf in the employer's name.

The following table presents this information graphically:

Annual Certifications (due before or on April 15)			
Type of Licensee or Risk-Bearing Entity	**IDSA Citation and Description**		
	§ 2264(9) Maine domestic insurance carrier	§ 2269(2)(A) Licensee is subject to/compliant with HIPAA/HITECH	§ 2269(2)(B) Licensee is a producer business entity owned by a GLBA-compliant depository institution
Domestic risk-bearing entity, such as insurer, nonprofit hospital, medical or health care service organization, health maintenance organization, or multiple employer welfare arrangement	Yes	Not applicable because this option is included in the § 2264(9) form	No
Foreign/Alien insurance carrier	No	Yes	No
Licensee with fewer than ten employees	No	No	No
Licensee with ten or more employees	Yes	Yes	Yes
Producer – solo or employed by another entity	No	No	No
Risk retention group chartered and licensed in Maine	Yes	Not applicable	No
Risk retention group chartered and licensed in a state other than Maine, or a risk purchasing group	No	No	No
Title 39-A self-insured group or individual self-insurer	No	No	No
Title 30-A risk pool	No	No	No

[14] 24-A M.R.S. § 2269.

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 IDSA.[15] 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.[16]

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.[17]

Notification of a Cybersecurity Event. Notification is an important part of IDSA. It covers notification to the Superintendent and, in conjunction with NRPDA, 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 of the event, if:

- The licensee is an insurer domiciled in Maine.
- The licensee is a producer whose home state is Maine.
- A nonresident 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
  b. the event has a reasonable likelihood of materially harming any Maine resident or a material part of the licensee's normal operations.[18]

Licensees notifying the Superintendent of cybersecurity events under IDSA must use the form and process announced on our website.[19] A licensee that has reported a cybersecurity event has an ongoing obligation to update its initial and any further notifications.

---

[15] 24-A M.R.S. § 2265(1).

[16] 24-A M.R.S. § 2265(2).

[17] 24-A M.R.S. § 2265(3).

[18] 24-A M.R.S. § 2266(1).

[19] 24-A M.R.S. § 2266(2).

Notification to Consumers. IDSA requires each licensee to comply with the applicable provisions of NRPDA.[20] 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.[21] 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.[22] Ceding insurers that have a direct contractual relationship with affected Maine residents must comply with the consumer notification requirements of IDSA and NRPDA.

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.[23]

IDSA specifically allows licensees to agree with other licensees, third-party service providers, or other persons to meet the investigation requirements of Section 2265 or the notice requirements of Section 2266.[24] For example, an insurer producer business entity may comply with these requirements on behalf of the producers that it employs, and a law firm may do so for its client.

Confidentiality. IDSA 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. IDSA 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.[25]

---

[20] 24-A M.R.S. § 2266(3).

[21] 24-A M.R.S. § 2266(4).

[22] 24-A M.R.S. § 2266(5).

[23] 24-A M.R.S. § 2266(6).

[24] 24-A M.R.S. § 2266(4).

[25] 24-A M.R.S. § 2268(1).

The information covered by Subsections 2266(2)(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 2266(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).

Notice of Risk to Personal Data Act

NRPDA applies to "security breaches." A security breach is the unauthorized acquisition, release or use of a person's computerized personal information that compromises the security, confidentiality, or integrity of that information.[26] "Personal information," for purposes of NRPDA, means a person's first name or first initial and last name when combined with any of the following: the person's Social Security number; driver's license or state-issued identification card number; account, credit card, or debit card number if the number could be used without other identifying information, access codes, or passwords; or account passwords, personal identification numbers, or other access codes.[27]

A person who suspects a breach of their security system must, in good faith, reasonably and promptly investigate the likelihood of misuse of the personal information and notify any Maine resident whose information has been or is believed to have been acquired by an unauthorized person. This notice must be given as expediently as possible and without unreasonable delay, but in no event more than 30 days after the person became aware of the breach and identifies its scope. If a law enforcement agency has delayed notification because of an investigation into the breach, the notice must be made within 7 days after the agency has lifted that embargo.[28]

The Superintendent enforces NRPDA as to any person licensed or regulated by the Bureau of Insurance. Bureau-regulated entities must notify the Superintendent of breaches when they notify their customers.[29]

---

[26] 10 M.R.S. § 1347(1).

[27] 10 M.R.S. § 1347(6).

[28] 10 M.R.S. § 1348.

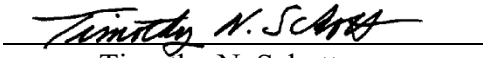
[29] 10 M.R.S. §§ 1348(5) and 1349(1).

NRPDA gives a safe harbor for any person complying with the security breach notification requirements of any other Maine or federal law if that law is at least as protective as NRPDA's notification requirements.[30]

NRPDA requires notification to the Superintendent whenever it is reasonably possible that misuse of personal information will occur, even if the system breach affects only one Maine resident. However, if a nonresident licensee has reason to think that a breach of its systems will affect at least 250 Maine residents, even though the licensee has not yet completed its investigation, it should notify the Superintendent under IDSA. Nonresident licensees should notify the Superintendent of breaches of their systems as required by and defined in NRPDA only if they are confident those events will not meet the criteria of section 2266(1).[31] We have posted a notification form for NRPDA-covered notifications on our website. This form largely tracks the IDSA form, including indications where we will give confidential treatment to responses.

Bureau staff have posted information about these laws on our website, including the certification forms and notification form mentioned in this Bulletin. Anyone interested in receiving further announcements about this topic is encouraged to sign up at the "Get Updates" box on the Bureau's home page.

July 19, 2023



Timothy N. Schott
Acting 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.

[30] 10 M.R.S. § 1350(4).

[31] The requirements are that the nonresident licensee must reasonably believe that the cybersecurity event involves nonpublic information of 250 or more Maine residents and either 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 the event has a reasonable likelihood of materially harming any Maine resident or a material part of the licensee's normal operations.