Wisconsin Legislative Council
ACT MEMO

Prepared by: Margit Kelley, Senior Staff Attorney

September 9, 2021

2021 Wisconsin Act 73
[2021 Senate Bill 160]

Insurance Data Security

2021 Wisconsin Act 73 creates basic requirements relating to insurance data security. Very briefly, subject to certain exceptions, a person or entity that is licensed, registered, or authorized with the Office of the Commissioner of Insurance (OCI) must implement a comprehensive information security program by November 1, 2022, and must provide notice to certain persons in the event of a data breach.

INFORMATION SECURITY PROGRAM

First, an entity must conduct a risk assessment to identify reasonably foreseeable internal and external threats, assess the likelihood and potential damage of threats, and assess the sufficiency of policies, procedures, and other safeguards to manage threats, including the processes for detecting, preventing, and responding to attacks, intrusions, or other system failures.

Then, an entity must design an information security program to mitigate the identified threats, as appropriate for the size and complexity of the entity, the nature and scope of its activities, and the sensitivity of the nonpublic information in its possession or control. The security program may include access controls on information systems, encryption, multifactor authentication, physical access restrictions, audit trails, and other measures.

An entity must stay informed regarding emerging threats and vulnerabilities, and must periodically assess the effectiveness of the security safeguards, including key controls, systems, and procedures. The periodic assessment must occur at least annually. An entity must further monitor and adjust the program as needed to respond to changes in business operations, technology, and threats.

The plan must also include oversight of third-party service providers. In particular, an entity must make reasonable efforts to require third-party service providers to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that is accessible or held by the provider.

Lastly, if an entity has a board of directors, the board must oversee the development, implementation, and maintenance of the information security program. Executive management must also report, at least annually, to the board on risk assessment and control decisions, overall status, and recommendations for modifications to the information security program.

RESPONSE TO SECURITY ATTACK

An entity's information security program must include an incident response plan. Elements of the plan must address clear roles, responsibilities, and levels of decision-making during and following a cybersecurity event, remediation of identified weaknesses, reporting and documentation of an event, and plans for evaluation and revision following a cybersecurity event.

If a cybersecurity event involving an entity's information systems or nonpublic information has or may have occurred, the entity or a provider acting on its behalf must conduct a prompt investigation. The

investigation must include, at a minimum, an assessment of the nature and scope of the event, identification of any nonpublic information that may have been involved, and actions to restore the security of the information systems and prevent additional unauthorized acquisition.

Unless a data breach does not create a material risk of identity theft or fraud, an entity must notify each affected consumer and the consumer's current independent insurance producer of record within 45 days of learning about an unauthorized acquisition of nonpublic information. An entity must notify consumer reporting agencies without delay when notice is required for 1,000 or more consumers. The form for any notice sent to consumers must also be provided to OCI.

Lastly, an entity must notify OCI within three business days of determining that a cybersecurity event occurred, in circumstances where there is a reasonable likelihood of material harm to a consumer or to the entity's normal operations, or the event involves at least 250 consumers.

EXCEPTIONS

The act's requirements for implementation of an information security program do not apply to smaller entities that are below certain thresholds. In particular, an entity is not required to implement an information security program if it has less than $10 million in year-end total assets, less than $5 million in gross annual revenue, or has fewer than 50 employees.

The act's requirements for both implementation of an information security program and reporting of security attacks do not apply to entities that are governed by certain federal requirements. These include: an entity that is governed by the Health Insurance Portability and Accountability Act[1] (commonly referred to as HIPAA); a depository institution that is in compliance with federal guidelines for financial institutions under the Gramm-Leach-Bliley Act; a securities broker that is in compliance with the Financial Industry Regulatory Authority (commonly referred to as FINRA); and an entity that in compliance with federal Farm Credit Administration guidance and regulations.

An entity that ceases to qualify for either exemption must comply with the applicable requirements within 180 days of becoming subject to the act.

AGENCY OVERSIGHT AND RULEMAKING

An entity must certify to OCI, by March 1 of each year, that it is in compliance with the requirements relating to implementation of an information security program.

An entity must maintain records relating to the act's requirements for at least five years, and must produce the records to OCI upon demand. Records received by OCI under the act are confidential, except as may be used by OCI in furtherance of any regulatory or legal action.

OCI may promulgate administrative rules to implement the provisions of the act.

Effective date: November 1, 2021. An entity must have a comprehensive information security program in place by November 1, 2022. An entity's first annual certification to OCI for its information security program is due by March 1, 2023. An entity's oversight of third-party service providers must be in place by November 1, 2023.

MSK:jal

---

[1] An entity that is governed by HIPAA is required to notify OCI of a cybersecurity event, although otherwise exempted from the act.