Wisconsin Insurance Data Cybersecurity Act becomes law

Zachary P. Bemis
608.284.2224
zbemis@gklaw.com

Josh Johanningmeier
608.284.2637
jjohanningmeier@gklaw.com

Sarah A. Sargent
414.287.9450
ssargent@gklaw.com

On July 15, 2021, Wisconsin Governor Tony Evers signed into law 2021 Act 73, the Wisconsin Insurance Data Security Law (Act 73).[1] Act 73 establishes specific data security requirements for the protection of nonpublic information of consumers and information systems for licensees regulated by the Wisconsin Office of the Commissioner of Insurance (OCI), including insurance companies, insurance agents and agencies, and public adjusters (licensees).

Act 73 outlines a licensee's obligations to prevent cybersecurity events from impacting consumers' nonpublic information and protecting the licensee's information systems. Generally, licensees are required to take preventative measures to combat and handle cybersecurity events through the performance of a risk assessment, implementation of an information security program (ISP) and development of an incident response plan.

Act 73 also requires licensees to provide notifications of cybersecurity events and the unauthorized acquisition of personal information to the OCI, consumers and others under various situations.

Act 73 contains several exemptions from applicability that licensees should review closely. Certain licensees that may already be subject to data security requirements under other regulatory requirements are exempt entirely from Act 73. Other licensees with less than $10,000,000 in year-end total assets, less than $5,000,000 in gross revenue or fewer than 50 employees are exempt from the requirements to establish an ISP but are subject to the breach notification requirements of Act 73.

Act 73 takes effect on Nov. 1, 2021, but mandates that required licensees implement an ISP by Nov. 1, 2022.

Prevention: Risk assessments, ISPs and incident response plans

By Nov. 1, 2022, licensees are required to conduct a risk assessment and develop, implement and maintain a comprehensive written ISP. The ISP must contain administrative, technical and physical safeguards for the protection of the licensee's information systems and nonpublic information.[2]

While Act 73 contains specific requirements for the development and implementation of an ISP, each licensee is responsible for tailoring the program based on the licensee's unique business and way it processes and maintains nonpublic information. Licensees that are not exempt are generally required to comply with the provisions of Act 73 requiring the establishment of an ISP and related provisions by Nov. 1, 2022. Specific steps that a licensee must take related to cybersecurity include:

[1] *Act 73 is modeled after the National Association of Insurance Commissioner's Insurance Data Security Model Law #668 (the NAIC Model Act).*

[2] *Wis. Stat. § 601.952(1).*

- **Risk assessment**: As the threshold step in developing an ISP, non-exempt licensees must conduct an initial risk assessment.
- **ISPs**: Based on the risk assessment, non-exempt licensees must design an ISP to mitigate identified threats and manage the risk of a cybersecurity event.[3] Importantly, Act 73 directs the ISP to be commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, and the sensitivity of the nonpublic information maintained by the licensee.[4]
- **Incident response plans**: As part of the ISP, licensees must also develop an incident response plan to promptly respond to, and recover from, a cybersecurity event.[5]
- **Third-party service provider oversight**: By Nov. 1, 2023, licensees are required to exercise due diligence when selecting third-party service providers.[6]
- **Oversight by board of directors**: Act 73 also requires a licensee's board of directors (if it has one), to exercise oversight of the licensee's ISP.
- **Annual certification of compliance**: Beginning in 2023, non-exempt licensees domiciled in Wisconsin are required to submit an annual, written certification to the OCI stating that the licensee is compliant with Act 73's ISP requirements.[7] These annual certifications will be submitted no later than March 1 of each year.

Investigations and notifications

Act 73's requirements for investigations of cybersecurity events and breach notifications are applicable to all licensees. Act 73 adopts the National Association of Insurance Commissioners (NAIC) Model Act's requirement that licensees investigate cybersecurity events and provide notifications in certain instances. Importantly, Act 73 also specifies that the OCI is the exclusive state agency to which licensees must report notifications of unauthorized acquisitions of personal information, including consumer notifications.[8] This subtle deviation from the NAIC Model Act centralizes requirements for consumer notifications by licensees with the OCI, a mandate that should ease compliance for licensees by providing regulation by a single state agency familiar with the insurance industry.[9] With regard to cybersecurity events, Act 73 requires:

- **Investigations of cybersecurity events**: Act 73 requires all licensees—including licensees exempt from the ISP requirements—to conduct prompt investigations of cybersecurity events.[10]
- **Notifying OCI**: Act 73 requires licensees to notify the OCI within three business days of certain information breaches/cybersecurity events. Under Act 73, a licensee may be required to provide a notification to the OCI if:

    1. The licensee is domiciled in Wisconsin and there is a reasonable likelihood of materially harming a consumer or a material part of the normal operations of the licensee; or
    2. A cybersecurity event involves the nonpublic information of at least 250 Wisconsin residents and (a) the cybersecurity event has a reasonable likelihood of materially harming a consumer or a material part of the normal operations of the licensee or (b) the licensee is required to report the event to another government body under state or federal law.[11]

[3] *Wis. Stat. § 601.952(3).*

[4] *Wis. Stat. § 601.952(3)(a).*

[5] *Wis. Stat. § 601.952(5).*

[6] *Wis. Stat. § 601.952(6).*

[7] *Wis. Stat. § 601.952(8).*

[8] *Wis. Stat. § 601.951.*

[9] *In contrast, under the NAIC Model Act licensees would be subject to the insurance regulator for certain notices and the state Attorney General or consumer protection regulator for consumer notices.*

[10] *Wis. Stat. § 601.954(3).*

[11] *Wis. Stat. § 601.954(2)(a).*

- **Notifying OCI regarding third-party service providers**: Further, licensees are required to notify the OCI of cybersecurity events involving third-party service providers no later than three days after the earlier of the date the licensee is notified of the event or the date the licensee has knowledge of the event.[12]
- **Notifying consumers**: Licensees must make reasonable efforts to notify each consumer whose nonpublic information has been acquired without authorization.[13] The notice must be provided in a reasonable time, but not later than 45 days after knowledge of the acquisition. A form of the notice provided to consumers must also be provided to the OCI.
- **Notifying producers of record**: Licenses are required to provide notification to the producer of record of any consumers whose nonpublic information has been acquired without authorization or affected by a cybersecurity event within 45 days of learning of the event.[14]

Additional provisions of Act 73

- **Confidentiality**: Act 73 provides broad confidentiality protections for documents, materials and other information in the possession or control of the OCI that are obtained under Act 73.[15]
- **Private causes of action**: In short, Act 73 doesn't create new claims or duties, but existing claims may be supported by evidence of failures to comply with its requirements. Act 73 as a whole may not be construed to create or imply a private cause of action for violation of its provisions, but also declares that it does not "curtail a private cause of action that otherwise exists" in the absence of Act 73.[16] Additionally, the failure to comply with the notification obligations is "not negligence or a breach of any duty, but may be evidence of negligence of a breach of a legal duty."[17]
- **OCI enforcement**: The OCI has the authority to investigate any licensee to determine compliance with Act 73 and take enforcement actions.[18] Enforcement is provided under the OCI's existing authority which allows for enforcement orders, civil forfeitures, license suspensions or revocations, or criminal penalties.[19]

For more information on the Wisconsin Insurance Data Security Law, or to learn how Godfrey & Kahn can help, contact Zach Bemis, Josh Johanningmeier or Sarah Sargent.

[12] *Wis. Stat. § 601.954(3).*

[13] *Wis. Stat. § 601.954(2)(a).*

[14] *Wis. Stat. § 601.954(2)(i).*

[15] *Wis. Stat. § 601.955.*

[16] *Wis. Stat. § 601.951(4).*

[17] *Wis. Stat. § 601.954(2)(g).*

[18] *Wis. Stat. § 601.956.*

[19] *Wis. Stat. § 601.64.*