THE
NATIONAL LAW REVIEW

Ohio Enacts New Cybersecurity Requirements for Insurers

Article By
Jennifer Orr Mitchell
Jared M. Bruce
Dinsmore & Shohl LLP
Publications

- Communications, Media & Internet
- Administrative & Regulatory
- Insurance Reinsurance & Surety

- Ohio

Friday, February 22, 2019

Senate Bill 273 goes into effect on March 20, 2019, and creates new requirements for Ohio insurance companies, including health insurance plans, to develop and implement specific information security programs to safeguard nonpublic business and personal information. Senate Bill 273 is based upon the National Association of Insurance Commissioners' Insurance Data Security Model Law (also referred to as "MDL-668"). With the enactment of Senate Bill 273, Ohio has become the second state to adopt a version of MDL-668, joining South Carolina. Senate Bill 273 is codified at new Ohio Revised Code Chapter 3965.

Development of Information Security Programs

Senate Bill 273 applies to all individuals or non-governmental entities required to be authorized, registered, or licensed under Ohio insurance laws (defined as "Licensees").[1] All Licensees will be required to develop, implement, and maintain a comprehensive written information security program, based on the Licensee's internal risk assessment, to safeguard the Licensee's nonpublic information, which is defined as business and personal information, the disclosure of which would harm the business or expose certain personal details of a customer.[2] Nonpublic information includes health information, financial information, or certain identifiers such as social security or bank account numbers. A Licensee's information security

program is required to be proportional "with the size and complexity of the Licensee, the nature and scope of the Licensee's activities including its use of third-party service providers, and the sensitivity of the nonpublic information used by the Licensee or in the Licensee's possession, custody, or control."[3] Only smaller Licensees that have fewer than 20 employees, less than $5 million in gross annual revenue, or less than $10 million in revenue are exempt from these requirements.

At a minimum, a Licensee's information security plan is required to do the following:

- Protect the security and confidentiality of nonpublic information and the security of the information system;
- Protect against any threats or hazards to the security or integrity of nonpublic information and the information system;
- Protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to any consumer; and
- Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.[4]

Senate Bill 273 also requires Licensees to include the following as a part of their information security program:

- Designate a party to act on behalf of the Licensee and be responsible for the information security program;
- Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including threats to the security of information systems and nonpublic information accessible to, or held by, third-party service providers, defined as entities contracted with a Licensee to maintain, process or store nonpublic information, to ensure their information security programs are adequate;
- Assess the likelihood and potential damage of internal or external threats based upon the sensitivity of the nonpublic information;
- Assess the sufficiency of safeguards in place to manage the threats described above;
- Implement information safeguards to manage the threats identified in its ongoing assessment; and
- Not less than annually, assess the effectiveness of the safeguards' key controls, systems, and procedures.[5]

Cybersecurity Event Notification Requirements

Senate Bill 273 requires Licensees to notify the Ohio Superintendent of Insurance upon the occurrence of a "cybersecurity event." A cybersecurity event is defined as "an event resulting in unauthorized access to, disruption of, or misuse of an information system or nonpublic information stored on an information system that has a reasonable likelihood of materially harming any consumer residing in this state or any material part of the normal operations of the Licensee."[6] The Licensee is required to notify the Ohio Superintendent of Insurance no later than three business days after the determination of the occurrence of a cybersecurity event if

the Licensee is domiciled in Ohio.[7] Additionally, Licensees are required to notify the Ohio Superintendent of Insurance in the event the cybersecurity event impacts 250 or more Ohio consumers and requires notification to be provided to any government body or agency.[8]

Cybersecurity event notices are required to include as much of the following information as possible:

- The date of the cybersecurity event;
- A description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of any third party service providers;
- How the cybersecurity event was discovered;
- Whether any lost, stolen, or breached information has been recovered and, if so, how this was done;
- The identity of the source of the cybersecurity event;
- Whether the Licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when such notification was provided;
- A description of the specific types of information (defined as “particular data elements, including types of medical information, types of financial information, or types of information allowing identification of the consumer acquired without authorization”);
- The period during which the information system was compromised by the cybersecurity event;
- The number of total consumers in Ohio affected by the cybersecurity event;
- The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;
- A description of efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur;
- A copy of the Licensee's privacy policy and a statement outlining the steps the Licensee will take to investigate and notify consumers affected by the cybersecurity event; and
- The name of a contact person who is both familiar with the cybersecurity event and authorized to act for the Licensee.[9]

In addition to these notification requirements, the Licensee is required to notify Ohio residents of the cybersecurity event in accordance with the existing requirements set forth at Ohio Revised Code § 1349.19.[10] The Ohio Superintendent of Insurance is required to receive a copy of any cybersecurity event notices sent to individuals.[11]

Certification of Compliance and Affirmative Defenses

Senate Bill 273 requires each insurer domiciled in Ohio to submit to the Ohio Superintendent of Insurance a written statement certifying compliance with all of the above information security program requirements by February 15 each year.[12] Insurers domiciled and licensed exclusively in Ohio may include this

information in their corporate governance annual disclosure form, which is required to be submitted to the Ohio Superintendent of Insurance by June 1 each year.[13] All records supporting compliance with Senate Bill 273 are required to be kept by the insurer for at least five years and are required to be available for inspection by the Ohio Superintendent of Insurance.[14]

Licensees that meet all of the requirements of Ohio Senate Bill 273 are deemed to have implemented a cybersecurity program that reasonably conforms to an industry-recognized cybersecurity framework for the purposes of Chapter 1354 of the Ohio Revised Code. This provides the Licensee with an affirmative defense to any cause of action based on a tort action brought under the laws of Ohio or in an Ohio court alleging the failure to implement reasonable information security controls resulted in a data breach concerning personal information or restricted information.[15]

Licensees subject to and compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy and security rules (45 C.F.R. Parts 160 and 164) are deemed to meet the bill's requirements. These Licensees can submit a written statement to the Ohio Superintendent of Insurance certifying their compliance with the HIPAA privacy and security rules. Licensees subject to HIPAA are still required to comply with the requirements regarding the notification of cybersecurity events.

Compliance Date

Licensees will have one year to come into compliance with the new requirements, with the exception of the certain provisions applicable to third party service providers, which will afford two years for Licensees to comply with those provisions.[16] The Ohio Superintendent of Insurance is authorized to adopt any new regulations required to carry out the requirements of Senate Bill 273.

The National Association of Insurance Commissioners' Insurance Data Security Model Law (MDL-668) is available here. Senate Bill 273 is available here.

---

[1] O.R.C. § 3965.01(M)

[2] *See*, O.R.C. 3965.01(O)

[3] O.R.C. § 3965.02 (A)

[4] O.R.C. §§ 3965.01 and 3965.02(A) and (B)

[5] O.R.C. § 3965.02(C).

[6] O.R.C. § 3965.01(E)

[7] O.R.C. § 3965.04(A)

[8] *Id.*

[9] O.R.C. § .04(B)(1)

[10] O.R.C. § .04(B)(2).

[11] *Id*.

[12] O.R.C. § 3965.02(I)

[13] *Id*.

[14] O.R.C. §§ 3965.03(C) and (D).

[15] O.R.C. § 3965.02(I)

[16] O.R.C. § 3965.02(F)