Preparing for compliance: Ohio's Insurance Data Security Law

April 1, 2019

Ohio is the second state in the country to adopt cybersecurity legislation modeled after the National Association of Insurance Commissioner's (NAIC) Insurance Data Security Model Law. The Ohio law, Senate Bill 273 (S.B. 273), went into effect on March 20, 2019, and applies to insurers authorized to do business in Ohio. Companies have one year to put the security measures into place.

Like NAIC's model law, Ohio's law requires insurance providers to take several steps to protect nonpublic personal information. Requirements include conducting risk assessments, submitting annual compliance certifications to the insurance superintendent and having a written information security program.

Information to help you and your clients understand the new legislation is listed below.

Who is required to comply with Ohio's insurance data security law?

Ohio's insurance data security law applies to "licensee" insurance companies. A licensee is any person licensed, authorized or registered, or required to be licensed, authorized or registered, under the insurance laws of Ohio. R.C. 3965.01(M).

Smaller insurance companies are exempt from certain requirements under the law, such as the adoption of a written information security program. Smaller companies are those with any one of the following criteria: less than 20 employees, less than $5 million in gross annual revenue or less than $10 million in assets. R.C. 3965.07(A). HIPAA-compliant companies are also exempt from certain requirements. R.C. 3965.07(B).

What are insurers required to do under the new law?

Here are some of the key requirements:

- **Written information security program.** A licensee must implement a comprehensive written information security program. The program should be based on the company's own risk assessment and take into account the nature and scope of the company's activity, including its use of third-party servicing. As part of this program, each licensee must include an incident response plan.
- **Annual risk assessment.** A licensee must conduct an annual review of the security program's key controls, systems and procedures. The assessment should assess the likelihood and potential damage of reasonably foreseeable security threats.
- **Prompt investigation.** If a licensee learns that a "cybersecurity event" (R.C. 3965.01(E)) has or may have occurred, the licensee or an outside service provider must conduct a prompt investigation and oversee measures to restore the security of the information systems compromised in the event.
- **Oversight of third-party service providers.** A licensee must require its third-party service provider to implement appropriate security measures to secure the nonpublic information that is accessible or held by that provider. Furthermore, if a licensee learns that a cybersecurity event may have occurred in a third-party service provider's information system, the licensee must conduct an investigation or make reasonable efforts to confirm and document that the third-party provider conducted an investigation and restored security.
- **Cybersecurity event notification.** In certain instances, a licensee must notify the superintendent of insurance of a cybersecurity event no later than three business days after determination the event occurred. This requirement only applies if certain thresholds are met, such as the reasonable likelihood of material harm to consumers or if the nonpublic information involves 250 or more Ohio consumers. R.C. 3965.04.
- **Annual certification.** Insurers domiciled in Ohio must annually submit a written statement to the superintendent of insurance, certifying that the insurer is in compliance with the requirements set forth in the law. Each insurer shall maintain all records supporting this certificate for a period of five years and have them available for inspection upon demand by the superintendent during that period.

What else should I know about the Ohio law?

S.B. 273 also includes the same safe harbor provisions as Ohio's general data breach law. (See R.C. 1354.01, et seq.) Under both laws, satisfaction of the statutory requirements gives a covered entity (or licensee) an affirmative defense to any cause of action alleging that the failure to implement reasonable information security controls resulted in a data breach concerning nonpublic information. An insurance licensee that meets the requirements of S.B 273 is deemed to have implemented a cybersecurity program that reasonably conforms to an industry-recognized framework under Ohio's general data breach law.

Authors

Anne Marie Sferra

Partner & Litigation Practice Group Chair

Columbus
614.227.2394
asferra@bricker.com