Pa. Insurance Data Security Act May Soon Become Law: Here's What It Could Mean

The Legal Intelligencer Cybersecurity Supplement

July 5, 2023

Krishna Jani, Coraleine Kitt, Anthony Gruzdis

This article was featured in The Legal Intelligencer on June 30, 2023. Subscription may be required.

The Pennsylvania Insurance Data Security Act (the act) was introduced on March 9 by Reps. Kevin J. Boyle and Tina Pickett. (2023 Bill Text PA H.B. 739). The legislation adopts a national model for insurer cybersecurity mandating that insurance entities implement new cybersecurity protections to better safeguard nonpublic information from nefarious threat actors. In recent years, insurance companies have been hot targets for malicious attackers because they collect and store vast amounts of personal information and other sensitive data about individuals. See Karen Hoffman, "Insurance companies increasingly fall prey to cyberattacks," SC MEDIA, (last visited June 9). Additionally, insurance companies often maintain lists of insured entities that carry cyber insurance. This particular aspect of the insurance business makes them attractive targets for cyber attackers because businesses that are cyber-insured are more likely to have the financial means to pay in the event of a ransomware attack. As a result, the bill aims to address the growing number of successful cyberattacks on insurance companies by requiring a comprehensive approach to implement effective cybersecurity measures.

What Would the Act Require of Insurance Companies?

The act would require Pennsylvania licensed insurance companies (licensees) to conduct a cybersecurity risk assessment of threats, information security systems, data that could be compromised, potential damage, and the control environment protecting the data. Licensees would be required to develop and implement a comprehensive written information security program using the results of the risk assessment. The act outlines specific standards and requirements for these information security programs.

First, licensees must establish administrative, technical, and physical safeguards to protect nonpublic information and the licensees' information systems. Second, licensees must designate one or more individuals, whether employees, affiliates, or external vendors, to oversee the information security program on behalf of the licensee. These designated individuals bear responsibility for the licensee's information security program. Additionally, Licensees must create an information security program tailored to mitigate identified risks, taking into account factors such as licensees' size and complexity, the nature and extent of Licensees' activities (including engagement with third-party service providers), and the sensitivity of nonpublic information under licensee's possession, custody, or control.

Additionally, the information security program should be designed to safeguard the security, confidentiality, and integrity of nonpublic information, as well as the security of information systems, protecting them against any threats or risks. Its purpose should be to prevent unauthorized access or use of nonpublic information and minimize potential harm to consumers. The act grants licensees the flexibility to determine the specific standards to be employed, guided by the outcomes of their risk assessment. However, it explicitly mandates the inclusion of audit trails within the information security program. These audit trails serve the purpose of detecting and responding to cybersecurity events, as well as reconstructing financial transactions to support the licensee's regular operations and obligations. Furthermore, the act imposes a requirement for licensees to provide cybersecurity awareness training to their personnel. This training should be regularly updated to address any risks identified through the company's risk assessment.

This act explicitly mandates the implementation of an incident response plan for licensees operating in Pennsylvania, especially for those that do not currently have one in place. As a crucial component of their information security program, each insurer would be obligated to create and sustain a written incident response plan. This plan's purpose would be to ensure swift and effective responses to cybersecurity events that may compromise the confidentiality, integrity, or availability of nonpublic information held by the insurer, the functionality of their information systems, or any critical aspects of the licensee's business operations.

Under the act, licensees would be required to submit an annual report to the insurance commissioner by April 15, along with maintaining appropriate documentation related to the report. In the event that a licensee becomes aware of a cybersecurity event, they would be required to promptly investigate the incident's extent and impact. Within five business days, the insurer must notify the insurance commissioner, providing specific details about the event's consequences. Additionally, the licensee must inform certain reinsurers, affected third-party service providers, and record-holding producers about the incident. The insurance commissioner is granted authority to investigate insurers and ensure their compliance with the act's requirements. Noncompliance may result in fines of up to $100,000 per calendar year, as well as potential license suspensions, revocations, or refusals to issue or renew an insurer's license, registration or authorization to operate in Pennsylvania.

Lastly, the bill repeals Section 7142 of Title 40 and introduces new provisions. These provisions grant the commissioner the authority to adopt exemptions from the National Association of insurance commissioners (NAIC) valuation manual through notices published in the Pennsylvania Bulletin. This change enables the adoption of the most current versions of the manual in a timely manner—and it is crucial for insurers to maintain accreditation with the NAIC because the NAIC accreditation program establishes and maintains standards to promote sound insurance company financial solvency regulation, the ultimate purpose of which is to protect consumers.

This law forms part of an overarching trend of states and localities, which have passed legislation requiring companies in a variety of sectors to undergo a cybersecurity risk assessment as a compliance measure.

How Does the Act Define 'Nonpublic Information?'

"Nonpublic information" is defined as information that is stored or maintained in an electronic system, is not publicly available information and is any of the following:

- Business-related information of a licensee that would cause a materially adverse impact to the business, operations, or security of the licensee if the information is tampered with, accessed, used, or subject to unauthorized disclosure.
- Information concerning a consumer that because of a name, number, personal mark, or other identifier, can be used to identify the consumer, in combination with any one or more of the following data elements:
- Social Security number;
- Driver's license number or nondriver identification card number;
- Financial account number, credit card number or debit card number;
- A security code, access code, or password that would permit access to a consumer's financial account;
- Biometric records information or data, except age or gender, in any form or medium created by or derived from a health care provider or a consumer that can be used to identify a particular consumer and that relates to any of the following:
- The past, present, or future physical, mental, or behavioral health or condition of a consumer or a member of the consumer's family;
- The provision of health care to any consumer; or
- Payment for the provision of health care to any consumer.

How Would the Notification Requirements in this Bill Work?

The act would require licensees to adhere to Section 3 of the Breach of Personal Information Notification Act, passed on Dec. 22, 2005, (P.L.474, No.94). In cases where the licensee is obligated to notify the commissioner under subsection (a), the Act would also require the Licensee to furnish a copy of the notice sent to consumers as per the provisions of the Breach of Personal Information Notification Act.

Where Is the Bill Now?

The bill unanimously passed both chambers of the General Assembly and was presented for Gov. Josh Shapiro's signature on June 8. As of June 12, the bill remains with the governor.

What Does this Mean for Insurance Companies?

Licensees in Pennsylvania should implement many of the measures that this bill would mandate if it became law, if they have not already. For instance, the proactive development of an incident response plan and internal employee training on cybersecurity best practices are effective methods of mitigating the risk of successful cyberattacks and resultant data breaches. By taking these practical steps, licensees can better protect themselves from falling prey to cyber attackers.

In conclusion, the Pennsylvania Insurance Data Security Act introduces comprehensive cybersecurity requirements for licensees, aiming to protect nonpublic information from malicious cyber threats. By mandating risk assessments, written information security programs, and incident response plans, the act provides a detailed approach for licensees to enhance their cybersecurity posture. The legislation aligns with a broader trend of states and localities enacting cybersecurity measures to safeguard sensitive data across various sectors. With potential penalties for non-compliance and a requirement to notify the Insurance Commissioner of cybersecurity events, the Act emphasizes the importance of taking a comprehensive approach to safeguarding internal systems and consumer data. Licensees in Pennsylvania should consider prioritizing the necessary information security measures outlined in the Act to mitigate the risk of damaging cyber incidents.

ATTORNEYS MENTIONED

Anthony Gruzdis

Coraleine Kitt, CIPP/US, CIPP/E