NEWS & INSIGHTS

# New cybersecurity requirements now in effect for (most) Pa. insurance carriers

BY: SETH A. MENDELSOHN | INSIGHTS | ARTICLE

JULY 24, 2023

Pennsylvania has joined nearly two dozen other states that have passed laws establishing cybersecurity regulations for insurance carriers operating in the state.  These regulations also will apply to certain small insurance companies now that the “small company exemption” has been repealed.

The Insurance Data Security Act will require all insurers, including certain small- and medium-sized insurers, to implement data security requirements including monitoring and reporting data breaches.

The Act, which has the support of Pennsylvania’s insurance industry, requires insurance companies operating in

Pennsylvania and licensed by the state to, among other items:

- Perform a risk assessment
- Develop, implement, and maintain an information security program
- Develop incident response plans
- Develop a corporate oversight program
- Develop a program to oversee vendors and exercise due diligence

Deadlines for compliance with the Act, effective December 11, 2023, are fast approaching. All these new requirements must be in place within a year of the effective date of the law, by December 11, 2024. And by December 11, 2025, all Pennsylvania insurance carriers must implement these requirements as to all third-party vendors that work with them.

The complex risk assessment must focus on foreseeable internal and external threats, assess likelihood for damage, assess licensees safeguard policies, procedures, and information systems. Insurance carriers then must implement safeguards and must perform this assessment annually.

A nuanced information security program must be a written plan based on the risk assessment. The program must identify specific safeguards to protect nonpublic information as well as information systems, be based on the company's complexity, and establish retention requirements for nonpublic information. The program also must include the specific designation of a person responsible for the program (this can be a vendor), and it must develop employee cyber risk training.

The Act also calls for the establishment of confidentiality protections, requires record retention for five years, and establishes penalties for non-compliance. The Insurance Commissioner is empowered to investigate any insurer to determine compliance. Exemptions to these requirements may apply to some small licensees. The new law is nearly identical to a model law from the National Association of Insurance Commissioners that 23 other states have passed and many multi-state carriers already follow. However, there are some slight differences. Understanding these and other differences is critical to compliance with the Act.

Saxton & Stump attorneys, along with our affiliate company Granite GRC, can help your insurance company grasp the nuances and work toward compliance with the new law. If you have questions about the new law or want to know how it will affect your business, please reach out to Seth Mendelsohn.

## Related People

Seth A. Mendelsohn

## Related Services and Industries

Insurance Law