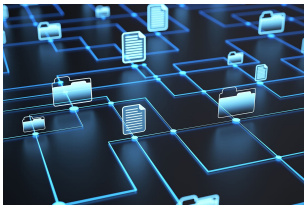

Thank You Michigan, Next! A Third State Adopts the NAIC Insurance Data Security Model Law

Feb 19, 2019

Categories:

Blogs
Technology Blog

On December 28, 2018, the former Michigan Governor, Rick Snyder, signed into law House Bill 6941 (the "Bill") amending the Insurance Code by adding Chapter 5A – Data Security (Sections 550 – 565). Michigan became the third state, after South Carolina and Ohio, to adopt a version of the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law.

Details

The Bill becomes effective on January 20, 2021, and codifies new data security obligations for insurance companies, including the following requirements:

- Create, maintain, and monitor an information security program based on the results of a risk assessment in order to safeguard nonpublic business and personal information. Follow-up risk assessments must be performed at least once a year.
- Develop a written incident response plan to respond to a cybersecurity event as defined by the Bill.
- Certify compliance to the Director of the Department of Insurance and Financial Services (DIFS) by submitting a written statement by February 15 of each year. Records supporting this certificate must be maintained for five years.
- Investigate and assess the nature and scope of a cybersecurity event. This obligation extends to outside vendors or service providers acting on behalf of the insurance company.
- Notify DIFS of a cybersecurity event no later than ten business days after the determination that the incident occurred. There are additional notification requirements to affected consumers, national consumer reporting agencies, and statewide media if the cybersecurity event exceeds certain threshold requirements.

FBT Gibbons

Further, the board of directors must require the insurance company's executive management to develop, implement, and maintain the information security program. Management must then provide the board with an annual report detailing the overall status of the program as well as material matters relating to it, including information on cybersecurity events, risk assessments, and recommendations for changes.

Exclusion

Insurers with fewer than 50 employees, less than $10 million in gross annual revenue, or less than $25 million in year-end total assets are excluded from the information security program requirements, and HIPAA-compliant insurers are deemed to also be compliant with the Bill's obligations.

Confidentiality of Cybersecurity Documents

Materials acquired by DIFS in compliance with the Bill would not be subject to the Freedom of Information Act, subpoena, or discovery, or admissible in evidence in any private civil action. DIFS would be authorized to use this information to fulfill its duties but otherwise could not make any of the information public without the consent of the insurance company.

Who is Next?

Other states are also in the race to adopt their versions of the Insurance Data Security Model Law. In early 2018, Rhode Island introduced Senate Bill S2497, but it was postponed indefinitely. Nevada also introduced Senate Bill 21 that is now set for review by the Nevada Senate Commerce and Labor Committee in the third week of February, 2019. The Washington State Office of the Insurance Commissioner presented its legislative agenda, stating that the legislation will adopt the NAIC model law during the 2019 calendar year.

For questions and assistance regarding this topic, please feel free to contact any member of our Privacy and Data Security Team.

FBT Gibbons

FBT Gibbons