HINSHAW

Alerts

Iowa Becomes the Latest State to Adopt the NAIC Model Cybersecurity Law

May 11, 2021
Hinshaw Privacy & Cyber Bytes

On April 30, 2021, Iowa Governor Kim Reynolds signed into law the Iowa Insurance Data Security Act, making Iowa the latest state to adopt the National Association of Insurance Commissioner's model cybersecurity law. Effective January 1, 2022, the Act establishes investigation procedures, data security program standards, and notification requirements for Iowa Insurance Division-regulated licensees (licensees) to protect the security and confidentiality of non-public information and the security of the licensees' information systems. Licensees with fewer than 20 employees are exempt, as are licensees with less than $5 million in gross annual revenue or less than $10 million in year-end total.

Covered licensees must develop, implement, and maintain a comprehensive written information security program that considers their size, complexity, the scope of their activities, and the results of a required risk assessment. The risk assessment may be conducted by an employee, affiliate, or outside vendor. It must identify internal and external threats, along with the probability and potential for damage that those threats could cause. Because risk assessment is an ongoing obligation under the Act and changes in technology must be continually monitored, a licensee's security program will need to be reviewed and updated with some frequency to stay compliant.

The Act also mandates oversight by a licensee's board of directors or an appropriate board committee, as well as at least annual written reports to the board concerning the overall status of the licensee's information security program, compliance with the Act, cyber events and violations, and related issues.

All insurers domiciled in the state must submit annual reports to the Commissioner of Insurance (Commissioner) by April 15th, certifying that the licensee is in compliance with the Act. Licensees must also maintain records of the past five years in the event the state requests to review compliance with the Act.

If a cybersecurity event occurs, licensees must notify the Commissioner within three business days:

- identifying the nature of the event; and
- declaring if the licensee reasonably believes that the incident affects more than 250 consumers—and has a reasonable likelihood of materially harming

Attorneys

Jason J. Oliveri

Service Areas

Privacy, Security & Artificial Intelligence

any consumer or a material part of the licensee's business operations.

In addition, consumers must be notified when required by Iowa's breach notification law.

The Act also addresses cyber event notice requirements for producers, third-party service providers, and reinsurers. The Commissioner is responsible for establishing the rules and procedures to enforce the Act and may commence an investigation if it learns that a cybersecurity event has or may have occurred. A licensee that violates the Act could be subject to a fine of up to $10,000 or more depending on if it knew or should have known of the violation. There is no private right of action under the Act.

Information provided to the Commissioner in connection with the Act is considered confidential and is not subject to discovery or admissible in any private civil action. Neither the Commissioner nor any other person who receives such information may be permitted or required to testify in a private civil action concerning the information.

Licensees are required to be in compliance when the law becomes effective on January 1, 2022.