

- HF 3842 (Elkins) Establishes enhanced data security standards for regulators and insurers to mitigate the potential damage of a data breach. The law applies to insurers, insurance agents and other entities licensed by the state department of insurance.
- The U.S. Treasury Department has urged prompt action by states to adopt the NAIC Insurance Data Security Model Law within the next 5 years or the administration will ask Congress to preempt the states.

## Background

In recent years, there have been several major data breaches involving large insurers that have exposed and compromised the sensitive personal information of millions of insurance consumers. This model was adopted by the NAIC in October 2017 following almost two years of extensive deliberations and input from state insurance regulators, consumer representatives, and the insurance industry. State adoption of the model is critical for state insurance regulators to have the tools they need to better protect sensitive consumer information.

## Key Points

- The model requires insurers and Commerce insurance licensees to develop, implement, and maintain an information security program based on its risk assessment, with a designated employee in charge of the information security program.
- This proposal is based on the National Association of Insurance Commissioners (NAIC) Data Security Model act.
- Phases in requirements for compliance with the information security program and oversight of third-party service providers.
  - Licensees determine the appropriate security measures to implement based on careful, ongoing risk assessment for internal and external threats.

- Requires licensees to investigate a cybersecurity event and notify the Department of a cybersecurity event.
- Allows the Commerce Department to determine compliance with the law, and provides state insurance regulators the authority to remedy data security deficiencies they find during an examination.
- Exempts licensees with fewer than twenty-five employees and agents of a licensee.
  - Licensees compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are exempt from the Information Security Program requirements, but are required to investigate cybersecurity events or and provide notification to the Department.

## Contact

Peter L. Brickwedde  
Assistant Commissioner  
Government & External Affairs  
651-539-1443 | [Peter.brickwedde@state.mn.us](mailto:Peter.brickwedde@state.mn.us)

