OFFICE OF LEGISLATIVE RESEARCH
Objective Research for Connecticut's Legislature

ResearchReport

Insurance Data Security Law

By: Alex Reger, Associate Analyst
October 25, 2021 | 2021-R-0150

Issue

Provide a brief overview of the Insurance Data Security Law (CGS § 38a-38, as amended by PA 21-157).

Summary

Connecticut's insurance data security law generally requires entities licensed by the Insurance Department to (1) develop and implement information security programs to protect sensitive private data and (2) investigate cybersecurity events (i.e., unauthorized access of private information) and report them to impacted consumers and the insurance commissioner.

The law, which is substantially similar to the National Association of Insurance Commissioners' insurance data security model law, was originally passed in 2019 (PA 19-117 § 230). Shortly after adoption, the legislature delayed its effective date from October 1, 2019, to October 1, 2020 (PA 19-196 § 8). Due to the COVID-19 pandemic, the Governor further delayed the act's effective date until October 1, 2021 (EO 9E and corresponding department bulletin IC-43). PA 21-157 codified the October 1, 2021, effective date, and enacted numerous changes, including clarifying the law's scope and changing to which entities the notification requirements apply.

Under the law, the insurance commissioner may investigate any licensee to ensure compliance with the law. After notice and a hearing, the commissioner may also suspend or revoke a license and fine the licensee up to $50,000.

Information Security Program

The law broadly requires licensees to develop, implement, and maintain an information security program commensurate with the licensee's business complexity (e.g., the size, nature, scope, and sensitivity of the data it holds). The program must be developed in coordination with a risk assessment the law requires licensees to conduct.

Among other things, the program must (1) establish a data retention schedule and method of destroying data once it is no longer being used, (2) create procedures to routinely assess a business' risk, (3) require the business to consider cyber security risk in their risk management process, and (4) identify and implement measures to control access to private data (CGS § 38a-38(c)).

HIPAA Exclusions and Grace Period for Small Businesses

The law applies to most entities licensed by the department but deems in compliance any business that maintains a federal Health Insurance Portability and Accountability Act (HIPAA)–approved information security program.

Additionally, the law establishes a grace period for certain small businesses to comply with the information security program requirements. Although most businesses must comply by October 1, 2021, licensees with at least 10, but fewer than 20 employees, have until October 1, 2022. The law exempts licensees with fewer than 10 employees (CGS § 38a-38(c)(10), as amended by PA 21-157, § 3).

Cybersecurity Events

Investigation

The law requires licensees to investigate any suspected cybersecurity event, including events occurring to third-party contractors, and to the extent possible (1) assess its nature and scope, (2) identify any private information that may have been involved or compromised, and (3) restore system security to prevent further data breaches. Licensees subject to a cybersecurity event must maintain related records for at least five years, and produce those records to the commissioner upon demand (CGS § 38a-38(d)).

Notification Requirements

The law establishes notification requirements if private information is breached in a cybersecurity event. Specifically, it requires domestic insurers and Connecticut insurance producers to report a

cybersecurity event if it is reasonably likely that the event will materially harm their business or a Connecticut consumer. Additionally, any department licensee must report an event if it impacts at least 250 Connecticut residents and (1) the licensee is required by federal or state law, or other governmental or supervisory regulation, to report the event or (2) it is reasonably likely the cybersecurity event will materially harm any Connecticut consumer or the licensee's business (CGS § 38a-38(e), as amended by PA 21-157, § 3).

Notice to Commissioner. The entities described above must notify the insurance commissioner as soon as possible, but within three business days after they first determined that the cybersecurity event occurred. The notice must include as much of certain specified information as possible about the event, including a description of the compromised data, how and when the event was discovered, its source, and any efforts being taken to remediate the situation that allowed the event to occur.

Notice to Consumers and Identity Protection Services. The insurance data security law generally requires licensees to notify consumers in accordance with the state's existing data breach notification law. This law requires covered businesses suffering data breaches to:

1. notify consumers within 60 days of a data breach, and
2. provide consumers with two years of identity theft prevention or mitigation services at no cost to them (CGS § 36a-701b, as amended by PA 21-59).

Enforcement

The law grants the commissioner powers to investigate any licensee for compliance, and if necessary, enforce the law's provisions. Among other things, this requires him to provide alleged violators with notice and an opportunity for a hearing to show why the commissioner should not take enforcement action, including by suspending or revoking a license. Additionally, the act allows the commissioner to impose a civil penalty of up to $50,000 for each violation and bring a civil action to recover it if necessary.

Additional Information

- **State Cybersecurity Law:** In addition to the insurance data security law, other Connecticut laws generally require businesses to safeguard data, computer files, and other documents containing personally identifiable information (CGS §§ 42-470 to 42-472d).
- **Cyber Threats and Cybersecurity:** OLR Report 2019-R-0047 provides a(n) (1) overview of cyber threats; (2) summary of Connecticut's cybersecurity strategies, action plans, and

resources for public utilities, state government, businesses, and individuals; and (3) overview of certain state cybersecurity laws.

- **An Act Concerning the Insurance Department's Recommendations Regarding the General Statute (PA 21-157):** The public act summary provides a synopsis of all the changes to the insurance data security law passed this session.

- **Cybersecurity Laws in Other States:** The National Conference of State Legislatures provides information on data security laws in other states for both the public and private sectors.

AR:kl