Robinson+Cole

Data Privacy + Security

July 2015

Connecticut Governor Signs New Comprehensive and Strict Data Security Law with Extensive Compliance Obligations for Companies, Including Breach Notification

On June 30, 2015, Connecticut Governor Dannel Malloy signed into law Substitute Senate Bill 949, "An Act Improving Data Security and Agency Effectiveness," which requires state government contractors to implement extensive data security measures when receiving personal and/or health information from a state agency and requires health care centers or other entities licensed to do health insurance business in the state, pharmacy benefits managers, third-party administrators, and utilization review companies to implement a comprehensive information security program (CISP), as well as amendments to Connecticut's data breach notification law. The law is considered one of the most stringent data security laws in the country.

The new law is quite extensive and requires specific compliance by government contractors, health insurers, health care centers, any entity licensed to do health insurance business in Connecticut, pharmacy benefits managers, third-party administrators, utilization review companies, and "any person who conducts business" in the State of Connecticut. It applies to all residents of the State of Connecticut, no matter where the information is held.

The requirements and deadlines for compliance with the law are outlined below.

Data Security Requirements

Effective **July 1, 2015**, any contractor that receives confidential information from a state agency through a written contract must implement "a comprehensive data-security program for the protection of confidential information" that it receives from the state agency.

Confidential information is defined to include "an individual's name, date of birth, mother's maiden name, motor vehicle operator's license number, Social Security number, employee identification number, employer or taxpayer identification number, alien registration number, government passport number, health insurance identification number, demand deposit account number, savings account number, credit card number, debit card number or unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation," and protected health information as defined in HIPAA. This broad definition

follows other recently enacted state laws that now include health information as a data element within the application of the law.

Section 1 of the law requires that, when a state agency shares confidential information with a contractor, the contract must include provisions that the contractor will protect the information, including the following:

- implement and maintain a comprehensive data-security program, which shall include as a minimum:
    - a comprehensive security policy
    - restrictions on access to the information, including physical restrictions and secure passwords
    - a process for reviewing the security program at least annually
    - an active and ongoing employee security awareness program that is mandatory for all employees with access to state confidential information that limits access to the confidential information to only authorized employees
- maintain state confidential information on a secure server, on secure drives, "behind firewall protections and monitored by intrusion detection software"
- restrict access to authorized employees
- implement and maintain security and breach investigation procedures
- notify the state and the Attorney General (AG) of a breach of the information
- cease using state information when requested by the state
- in the event of a breach or suspected breach of state information, provide a report to the AG and the state agency detailing the steps taken to mitigate the effects of the breach and the steps taken to ensure future breaches will not occur or why the contractor does not believe a breach occurred
- not store state information on a standalone computer or removable media
- not copy, reproduce, or transmit data except as necessary to perform services under the contract

Every contract between the state and a contractor shall include a proposed timetable for the Report about a breach or suspected breach, must be provided to the state and AG, and specify how the costs of investigation and notification of the breach will be apportioned.

The AG may investigate any violations and if the AG finds that a contractor has violated this section of the statute, the AG may bring a civil action in Hartford Superior Court against the contractor. Further, the statute specifically states, "Nothing in this section shall be construed to create a private right of action."

Finally, Section 1 provides that if the confidential information that is breached are education records, the contractor may be subject to a five-year ban from receiving access to the information by the State Department of Education.

Section 2 of the law allows the Secretary of the Office of Policy and Management to require additional protections as necessary, depending on the sensitivity of the data.

Section 4 is new and also effective **July 1, 2015**. It requires the Office of Policy and Management to develop a program to "access, link, analyze and share data maintained by executive agencies" and coordinate responses to queries for state data (including FOIA requests) and to assure that the privacy and confidentiality of the data will be protected.

Section 5, effective on **October 1, 2015**, is applicable to health insurers, health care centers,

or other entities licensed to do health insurance business in the state, pharmacy benefits managers, third-party administrators and utilization review companies and requires significant compliance obligations for protecting personal information of insureds, members, and enrollees.

The most significant requirement is that those entities must "implement and maintain a comprehensive information security program" (CISP) that must be in writing and is designed to safeguard the personal information of insurers and enrollees, which must be completed by **October 1, 2017**. The CISP must contain administrative, technical and physical safeguards that are appropriate to the size and complexity of the organization. The CISP must be updated at least annually.

The requirements of the CISP are similar to those of a Written Information Security Program required by the Massachusetts Data Security Regulations, touted to be the most stringent in the country. The CISP must include authentication protocols, including multifactor authentication methods, access restrictions, blocking and controls, password requirements, and encryption of all personal information. In addition, Section 5 requires the following:

- an employee must be designated to oversee the program
- a security risk assessment must be completed
- security policies and procedures are implemented
- employee discipline measures are adopted and imposed
- terminated, inactive, or retired employees are prevented from accessing personal information
- third parties be overseen and written contractual provisions be in place that the third party implement and maintain safeguards with very specific provisions required by the law

The company is required to certify annually to the Insurance Department that it maintains a compliant CISP commencing on **October 1, 2017**. The Insurance Commissioner and AG can request a copy of the CISP, and if it doesn't comply, can require the company to make changes to the CISP.

Breach Notification

The Connecticut breach notification law was also amended, requiring any company that discovers an actual or suspected breach of security to notify individuals of a compromise of their personal information without unreasonable delay, but "not later than ninety days after the discovery of such breach, unless a shorter time is required under federal law" (such as HIPAA which requires notification as soon as practicable, but not later than 60 days).

Significantly, the amended breach notification law requires any company that suffers a breach and notifies an individual of the breach must offer "appropriate identity theft prevention services, and if applicable, identity theft mitigation services" at no cost to the resident and for a period of not less than 12 months.

Kill Switch

Finally, following the lead from California, the amended law requires all new models of smartphones in the State of Connecticut offered for retail sale between **July 1, 2016** and **July 1, 2017** include software or hardware (or both) that can be downloaded at purchase that can kill or remotely wipe the smartphone to render it inoperable to an unauthorized user.

The new Connecticut law is significant for all businesses in the State of Connecticut and those outside the state that maintain the personal information of Connecticut residents and sets forth massive compliance obligations. The obligations are specific and onerous and will be a challenge for compliance.

To get more thoughtful and timely discussions of legal news and perspectives on various issues relating to data privacy and security, subscribe to our *Data Privacy + Security Insider* blog by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy + Security Team.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

---