Legal Update Article

Connecticut Adds Significant Data Security Mandates for State Contractors, Certain Health Insurance Industry Businesses

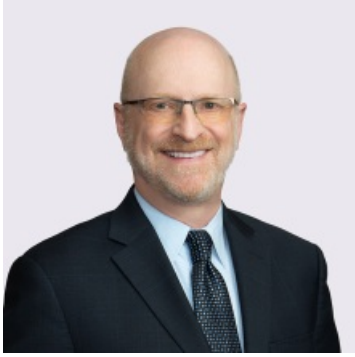
By Joseph J. Lazzarotti & Jeffrey M. Schlossberg

July 23, 2015

Meet the Authors

Joseph J. Lazzarotti

Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com



Jeffrey M. Schlossberg

(Jeff)
Principal
(631) 247-4614
Jeffrey.Schlossberg@jacksonlewis.com

Related Services

Privacy, Data and Cybersecurity

Connecticut has amended its breach notification statute to require that covered businesses provide one year of identity theft protection services to persons affected by certain breaches of their personal information.

Senate Bill 949 also establishes significant data security requirements for entities contracting with state agencies and entities in the health insurance and administration business (e.g., health insurance insurers, pharmacy benefits managers, and third-party administrators). In addition, the law mandates that smartphones sold in the state have hardware or software that will allow an authorized user to disable his or her phone's "essential features." Many such devices already contain this feature.

The law has implications beyond the businesses to which it applies directly. For example, professional service providers and other businesses working with covered state contractors or health insurance businesses in Connecticut might find that the new mandates apply to them by contract when they are asked to perform services that involve access to the same personal information triggering these requirements for the covered contractors and businesses. Moreover, employers regularly work with third-party administrators, pharmacy benefit managers, and other health insurance businesses in the administration of their group health plans for employees. These employers should consider ensuring that these entities are compliant with the new mandates.

Contractors Must Implement Data Security Program

Entities that have contracts with the state and receive "confidential information" from state agencies are required to implement and maintain a "comprehensive data-security program," including the use of security policies, annual reviews of such policies, access restrictions, and mandatory security awareness training for employees beginning July 1, 2015.

"Confidential Information" is defined broadly to include: name, date of birth, mother's maiden name, driver's license number, Social Security number, health insurance identification number, and bank and credit card account numbers. Confidential Information also includes protected health information under HIPAA (the Health Insurance Portability and Accountability Act), as well as any information that a state contracting agency identifies as confidential to the contractor.

These entities' policies, at the minimum, must restrict access to Confidential Information only to authorized contractor employees, maintain the Confidential Information in secure servers with firewall protections, and implement security and

breach investigation procedures. Their programs must be reviewed annually and include ongoing employee security awareness program. Further, the contractors must provide to the state Attorney General and the contracting agency a report detailing breaches or suspected breaches, including a plan to mitigate the effects of a breach, or report why the contractor believes no breach occurred.

Beyond safeguarding the data, the law adds limitations on how a contractor can use, maintain, and disclose the Confidential Information received from state agencies. For example, the contractor cannot store Confidential Information on stand-alone computers or notebooks or portable storage devices, such as USB drives. This provision has limited exceptions. Additionally, a contractor may not copy, reproduce, or transmit Confidential Information except as necessary to complete the contracted services. *Because of the way many businesses perform their services today (e.g., utilizing flash drives and allowing employees to work from home, perhaps with their own computers), the new mandates may require significant changes in current practices.*

Significantly, contractors who are "business associates" of a state agency as defined under HIPAA may have to do more than comply with the HIPAA privacy and security regulations. The HIPAA privacy and security rules establish a floor of protections that can be exceeded by more stringent protections at the state level. Although the Connecticut law provides that "nothing in [the law] shall be construed to supersede a contractor's obligations pursuant to" HIPAA, state contractors in Connecticut that are business associates will have to revisit their HIPAA policies and procedures to ensure compliance with the state mandates. Of course, state contracts could impose additional security obligations on the contractor, beyond what is provided in the statute.

Like HIPAA, there is no private right of action under the Connecticut law for violations of its requirements. However, the law authorizes the state Attorney General to bring a civil action in the name of the state against a contractor who violates the statute.

Health Insurance Businesses Must Step Up Data Security

Beginning October 1, 2017, any health insurer, health care center, pharmacy benefits manager, third-party administrator, utilization review company, or entity that is licensed to do health insurance business in Connecticut must implement and maintain a "comprehensive information security program to safeguard the personal information of insureds." Examples of the safeguards the program must include are:

- secure computer and Internet user authorization protocols, e.g., control of user identification, a reasonably secure method of assigning a password, control of security passwords, restrictions on access only to active users, and blocking of access after multiple unsuccessful attempts to gain access;
- secure access control measures that include, but are not limited to, restriction of access to personal information only to those who require such data to perform their job duties, passwords that are not default passwords and are reset at least every six months, encryption of all personal information while being transmitted on a public Internet network or wirelessly, encryption of all personal information stored on a laptop computer or other portable device, and monitoring of

company security systems for breaches of security;
- designation of one or more employees to oversee the security program;
- identification and assessment of reasonably foreseeable internal and external risks to the security of the personal information;
- development of employee security policies;
- imposition of disciplinary action on employees for violating security policies;
- prevention of terminated employees from accessing personal information;
- annual review of the scope of the secure access control measures; and
- mandatory post-incident review.

Many of these entities are covered by the HIPAA privacy and security regulations, whether as covered entities (e.g., health insurance issuers) or business associates (e.g., pharmacy benefits managers, and third-party administrators). However, as with the application of the new rules for certain state agency contractors, some of Connecticut's requirements will go beyond the basic HIPAA regulatory mandates. For example, the Connecticut law requires passwords be changed at least every six months, something that is not expressly required under HIPAA. In addition, like the data security mandates in Massachusetts, the Connecticut law requires encryption of all personal information while being transmitted on a public Internet network or wirelessly and stored on a laptop computer or other portable device. Moreover, under the Connecticut law, the state's Insurance Commissioner or Attorney General may demand a copy of a covered businesses' written information security program (WISP) and require changes to the program that the Commissioner or Attorney General believes are necessary. In addition, beginning October 1, 2017, covered health insurance businesses must certify annually to the Insurance Department, under penalty of perjury, that they maintain a comprehensive information security program that complies with the law's requirements.

Smartphones Sold in Connecticut Must Include Disabling Feature

Starting in July 1, 2016 (through July 1, 2017), retailers of new smartphones in Connecticut must offer smartphones with either hardware or software that will allow an authorized user to disable the phone's "essential features" to an unauthorized user.

Implications

Businesses covered by the new requirements must take stock of their current operations, policies, and procedures to determine whether they are in compliance. This takes time and only after careful assessment and analysis. Turning this task over to the company's "IT guy" is likely not the best approach. The security programs contemplated by these new mandates (and those in other states, such as California, Florida, Maryland, Massachusetts, and Oregon) go beyond the functioning of an organization's electronic information systems. The role of IT is no doubt critical, but these mandates require consideration of administrative and physical safeguards, as well as technical safeguards. They envision careful assignment of access to personal data based on particular need. They seek broad awareness of the safeguards throughout an organization that is accomplished through training and other measures. They mandate incident response planning, a function involving key decision makers in an organization so they know what to expect and their responsibilities in the event of a data breach. They require organizations to obligate

their third-party service providers to adhere to similar standards. In short, they contemplate a wholesale, enterprise-wide, regularly reviewed approach to securing personal information that changes and develops with the organization.

Data security laws often reach beyond the entities directly affected by them. This is because to provide their services, directly covered entities will have to work with other businesses that would need access to the personal information driving the laws' mandates. Accordingly, the safeguards flow downstream, at least through contract.

This is a general summary of the changes. Because of the complexities involved in this area, businesses would be well-served to address specific scenarios with the assistance of counsel.