Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Conn. Seeks To Tighten Data Privacy Requirements

Law360, New York (June 22, 2015, 12:04 PM ET) --

William J. Roberts

On June 1, 2015, the Connecticut Legislature passed S.B. 949, a comprehensive data privacy and security bill that tightens the state's data breach response requirements and imposes new obligations on state contractors and the health insurance industry. While Connecticut Gov. Dannel Malloy has yet to sign S.B. 949 into law, he is widely expected to do so shortly. A copy of S.B. 949 is available here. This article reviews the portions of the bill most pertinent to businesses operating in Connecticut or holding personal information of state residents.

Revisions to Breach Response Requirements

Current Connecticut law requires an entity that experiences a data breach to provide notice of such breach to the affected individuals and the Connecticut Attorney General's Office "without unreasonable delay." S.B. 949 amends this requirement by specifying that such notices must be provided no "later than [90] days after discovery of such breach, unless a shorter time is required under federal law." This amendment is striking in that it sets a maximum time period for notice that is much longer than the time periods set forth in other state or federal breach notification standards (e.g., the Health Insurance Portability and Accountability Act requires notice no later than 60 days following discovery of a breach).

Recognizing this apparent leniency, Connecticut Attorney General George Jepsen issued a press release that clarifies his office's enforcement approach. Specifically, Jespen clarifies that the 90-day reporting period is the "outside limit" for notifications and that "[t]here may be circumstances under which it is unreasonable to delay notification for 90 days." Jespen makes clear that his office will "continue to scrutinize breaches and to take enforcement action against companies who unreasonably delay notification — even if notification is provided less than 90 days after discovery of the breach." Thus, entities should continue to respond to breaches in a prompt manner and provide the necessary notices as soon as practicable.

In addition, S.B. 949 requires companies experiencing a breach involving Social Security numbers to provide affected individuals with free credit monitoring services and information on how such individuals may place a credit freeze on the individual's credit file. The free credit monitoring services

must be for a period of at least one (1) year. While this new requirement has been considered by many to be a significant change in the law, it may have limited implications in practice because the state attorney general has long expected (or even required) companies to provide such services when Social Security numbers were involved.

Notably, S.B. 949 appears to set a shorter time period for free credit monitoring than what is typically expected by the state attorney general's office. In many instances, the attorney general has insisted that companies offer no less than two years of free credit monitoring. Addressing this apparent lowering of expectations, Jespen announced in his office's press release that S.B. 949 "sets a floor for the duration of the protection" and that he retains the authority "to seek more than one year's protection — and to seek broader kinds of protection — where circumstances warrant."

Both of the modifications to Connecticut's breach reporting requirements are effective Oct. 1, 2015.

State Contractor Obligations

Effective July 1, 2015, S.B. 949 imposes significant new requirements for state contracts that authorize a state agency to disclose "confidential information" to a contractor. The bill defines "confidential information" as: (1) a person's name, date of birth or mother's maiden name; (2) any of the following numbers: motor vehicle operator's license, Social Security, employee identification, employer or taxpayer identification, alien registration, passport, health insurance identification, demand deposit or savings account, or credit or debit card; (3) unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation; (4) "personally identifiable information" and "protected health information," as defined in federal education and patient data regulations, respectively (i.e., Family Educational Rights and Privacy Act and HIPAA); and (5) any information that a state contracting agency tells the contractor is confidential. Confidential information does not include information that may be lawfully obtained from public sources or federal, state or local government records lawfully made available to the public. This definition is very broad and contractors should be cognizant that a large number of state contracts may be subject to the bill's new requirements.

If a state contract involves the sharing of confidential information, the contractor will be required to undertake significant efforts to protect the privacy and security of such information. Specifically, the contract must require the contractor to, at a minimum: (1) at its own expense, protect confidential information from being breached; (2) implement and maintain a comprehensive data security program to protect the confidential information; (3) limit access to the confidential information to the contractor's authorized employees and agents for authorized purposes as necessary to complete the contracted services or provide contracted goods; (4) maintain all confidential information obtained from the state (a) in a secure server, (b) on secure drives, (c) behind firewall protections and monitored by intrusion detection software, (d) in a manner where access is restricted to authorized employees and agents and (e) as otherwise required under state and federal law; (5) implement, maintain and update security and breach investigation procedures that are appropriate given the nature of the information disclosed and reasonably designed to protect confidential information from unauthorized access, use, modification, disclosure, manipulation or destruction; and (6) specify how the cost of any notification about, or investigation into, a breach is to be apportioned.

The bill includes numerous detailed requirements a contractor must adhere to, particularly with respect to the development of a data security program and the reporting of breaches. Compliance may be particularly burdensome for contractors in industries without a history of data privacy regulation or for small providers with limited financial or other resources. The bill includes a waiver provision which

allows the Office of Policy and Management ("OPM") to require additional protections or alternate security assurance measures for confidential information if the facts and circumstances warrant them after considering, among other factors, the type and amount of confidential information being shared, the purpose for which the confidential information is being shared, and the types of goods or services covered by the contract. Notably, the bill does not include the size or resources of the state contractor as factors OPM may consider when altering data security requirements.

Insurance Industry Data Security Programs

In response to the recent Anthem Inc. data breach, S.B. 949 imposes new requirements on health insurers, pharmacy benefit managers, utilization review companies and third-party administrators licensed do to business in Connecticut with respect to these entities' maintenance of comprehensive information security programs.

Specifically, each such entity must develop and implement a written security program no later than Oct. 1, 2017. The program must address a litany of administrative, physical and technical safeguards including, among others: (1) computer and Internet user authentication protocols; (2) access control measures; (3) risk assessments; (4) sanctions for employee violation of security policies or procedures; and (5) oversight of third parties that have access to personal information.

The extent of such safeguards must be appropriate in light of the scope and type of business, the amount of resources available, the amount of data compiled or maintained and the need for security of such data. The written security program must be updated at least annually.

While extensive, many of the affected companies will already be subject to very similar requirements imposed under HIPAA and thus will likely have most, if not all, of S.B. 949's elements already addressed in current policy. Nevertheless, insurers and others subject to this new requirement should review existing policies and procedures to determine sufficiency in light of the new requirements.

—By William J. Roberts, Shipman & Goodwin LLP

William Roberts is an associate in Shipman & Goodwin's Hartford, Connecticut, office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.
