June 25, 2021

Connecticut Enhances Data Breach Notification Law

On June 16, Connecticut Gov. Ned Lamont signed House Bill No. 5310, titled "An Act Concerning Data Privacy Breaches" (the act). The act, which goes into effect October 1, amends Conn. Gen. Stat. § 36a-701b, Connecticut's existing breach notification law, and significantly expands the definition of "personal information," in addition to other enhancements described below. Helpfully, the new act deems persons who provide notice to affected Connecticut residents under the Health Information Technology for Economic and Clinical Health (HITECH) Act to be in compliance with the act.

Definition of Personal Information Expanded

Previously, Connecticut law defined "personal information" as an individual's first name, or first initial and last name, in combination with any one or more of the following data categories:

- Social Security number
- Driver's license number
- State identification card number
- Credit or debit card number
- Financial account number, in combination with any required security code, access code or password that would permit access to such financial account

The act expands Connecticut's definition of "personal information" to align more closely with laws in other states by including the following data categories:

- Individual taxpayer identification number (e.g., Social Security number)
- Identity protection personal identification number issued by the IRS
- Passport number, military identification number or other identification number issued by the government that is used to verify identity
- Medical information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional
- Health insurance policy number or subscriber identification number, or any other unique identifier, issued by a health insurer to identify the individual
- Biometric information consisting of data generated by electronic measurements of an individual's unique physical characteristics and used to authenticate or ascertain the individual's identity, such as a fingerprint, voiceprint, or retina or iris image

- User name or email address, in combination with a password or with a security question and answer that would permit access to an online account

Timing for Required Notification Reduced

The act shortens the maximum allowable amount of time for breach notification from not later than 90 days to not later than 60 days after the discovery of a breach.

The act clarifies that if additional Connecticut residents impacted by a breach are identified after the 60-day period, they must be notified as "expediently as possible."

One of the most significant changes under the act is the elimination of what some interpreted as an option to defer notification, pending completion of an investigation to determine the nature and scope of the incident, to identify the individuals affected, or to restore the reasonable integrity of the affected data system.

Additional Requirements for Login Credential Breach and Notification

The act includes additional requirements in the event of a login credential breach. In such event, notice must be provided to the affected Connecticut resident that enables them to:

- promptly change their password and/or security question and answer; or
- take other steps to secure the affected account and all other accounts for which they use the same e-mail and password or the same security question and answer.

HIPAA and HITECH Act Exemptions

Under the act, any person who provides notice to affected Connecticut residents in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the HITECH Act does not need to send separate notices to comply with the requirements of the act, so long as such person is in compliance with the HITECH Act's privacy and security standards. If a HITECH Act notice is required, however, then notice must also be provided to the Connecticut Attorney General no later than the time the HITECH Act notice is provided to the affected Connecticut residents.

Investigation Materials Exempt From Public Disclosure

Under the act, documents, materials and information provided to the Connecticut Attorney General in response to an investigative demand issued in an investigation of a security breach are exempt from public disclosure under subsection (a) of Section 1-210 of Connecticut's Freedom of Information Act, Conn. Gen. Stat. § 1-210 (2013), provided that the Connecticut Attorney General may make such documents, materials and information available to third parties in furtherance of its investigation.

Conclusion

Persons who own, license or maintain the personal information of Connecticut residents should review their existing data breach response protocols, or seek counsel, to ensure compliance with Connecticut's amended breach notification law when it goes into effect October 1.

Authors

Richard D. Harris

Partner

Hartford, CT | (860) 275-0294

New Haven, CT | (203) 752-5094

rdharris@daypitney.com

Susan R. Huntington

Partner

Hartford, CT | (860) 275-0168

Washington, D.C. | (202) 218-3909

shuntington@daypitney.com