THOMPSON COBURN LLP

insights

Illinois strengthens, expands scope of personal information protections

With the passage of the Illinois Personal Information Protection Act (HB1260) last month, Illinois substantially broadened the definition of personally identifiable information, and imposed requirements on data collectors for the protection of Illinois residents' information. The Act, known as PIPA, takes effect on January 1, 2017.

One of the biggest changes in PIPA is a broadening of the definition of "protected personal information." PIPA now defines protected personal information to include an individual's first name or first initial and last name in combination with medical information or health insurance information (which are further defined in the statute), or unique biometric data (e.g., "fingerprint, retina, or iris image, or other unique physical representation or digital representation of biometric data"). Notably, a company will be required to provide notice of a breach involving "any information regarding an individual's medical history, mental or physical condition…" Arguably, this could be interpreted to require notice of a breach of an incident report describing the fact that an employee fell, cut their arm and required stitches. The simple statement that the employee fell and required stitches could be considered a description of their "physical condition" requiring notification. While states should be lauded for their efforts to protect their residents in the event of a data breach, if organizations are required to inform individuals whenever information about a paper cut is breached, consumers may ignore such communications and miss important notices regarding breaches of highly sensitive information that truly create a risk of harm.

PIPA also clarifies the existing encryption safe-harbor provisions to expand notification requirements. With the new law, notification may now be required where personal information is encrypted or redacted but the keys to decrypt or otherwise read the data have been acquired.

Adding usernames

PIPA joins other states by requiring notice if a breach includes a username or email address in combination with a password or security question and an answer (i.e., information that would permit access to an online account).

Notification of a breach of usernames and password information can be provided via e-mail. Notices must direct the user to "promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer."

Implementing safeguards

The new law also requires companies that deal with records containing Illinois residents' personal information to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure." Similarly, any contract requiring the disclosure of personal information from an Illinois resident must include a provision requiring the recipient of the information to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure." Of course, similar to many other laws, PIPA does not define "reasonable security measures."

PIPA does contain a safe harbor provision for those companies that are subject to, and in compliance with, certain federal laws. For instance, under the new law, if an entity is subject to, and in compliance with, the Gramm-Leach-Bliley Act Safeguards Rule, that entity is deemed to be in compliance with PIPA. Entities required to comply with the Privacy and Security Rules for the protection of electronic personal health information under the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) are deemed to be in compliance with PIPA. It should be noted, though, that those entities required to provide notice to the U.S. Department of Health and Human Services (HHS) of a breach under HITECH must now provide notification to the Illinois Attorney General within five business days of notifying HHS.

For assistance with data security compliance and with the latest developments in state breach notification laws, please contact Thompson Coburn's Cybersecurity group.

authorsTest