ROPES & GRAY

ALERT

Health Care

June 14, 2016

Five Key Amendments to the Illinois Personal Information Protection Act and Their Implications for Health Care Providers, Medical Device Companies, and Digital Health Companies

Attorneys
Deborah Gersh
Jennifer L. Romig
John Saran
Sara Helene Shanti

On May 6, 2016, Gov. Bruce Rauner signed House Bill 1260 amending the Illinois Personal Information Protection Act ("PIPA") in response to the increasing threat of electronic personal information being compromised. In the fall of 2015, Gov. Rauner had vetoed the proposed amendments to PIPA after taking issue with certain elements that he viewed as departing from similar laws in other states, and which could place burdensome costs on businesses and hurt Illinois' economic competitiveness.[1] PIPA's amendments take effect on January 1, 2017, and will make Illinois one of the most progressive states for the regulation of breach reporting and the protection of electronic personal information. As such, health care providers, medical device companies, and digital health companies that collect, maintain, disclose, or "otherwise deal[s] with nonpublic" electronic personal information should be aware of, and be prepared to comply with, the amended PIPA.[2]

Five Key Amendments to PIPA

1. Expansion of the Personal Information Definition: The definition of "Personal Information" was significantly expanded to include the individual's first name or first initial and last name and any one of the following: (i) Medical information (including any information regarding an individual's medical history, mental or physical condition, diagnosis, or medical treatment by a healthcare professional, *including such information provided by such individual to a website or mobile application*); (ii) Health insurance information (including a policy or subscriber number, any other unique identifier, and any related medical information in an application, claims history, or appeals record); and (iii) unique biometric data (including fingerprints, retina or iris images, or other unique physical representation or digital representation of biometric data).

   The definition of "Personal Information" was further expanded to include a user name or email address in combination with a password or security question and answer that would permit access to an online account.

2. Erosion of Encryption Exception: The definition of "Personal Information" previously only captured computerized data that was unencrypted. However, the amended PIPA's definition of "Personal Information" *includes encrypted or redacted data where the keys to unencrypt or unredact or otherwise read the name or data elements are available*.

3. Expanded Notice Obligations: The amendments to PIPA added an additional notice requirement for the data breach of Personal Information that consists of a user name or email address in addition to a password or security question answer that can allow access to an online account. *Such notice must inform the person that his or her information has been breached and that he or she thus should change his or her user name, password,*

[1] For example, the previous proposed amendments included consumer marketing information and geolocation information as protected personal information and required a 30-day Attorney General notice requirement. *See* Gov. Bruce Rauner, Letter to the Illinois Senate, Aug. 21, 2015, *available here*.
[2] PIPA at 815 ILCS 530/5, Section 5.

security question or answer, as applicable, or take protective steps to safeguard other online accounts using the same log-in information.

4. Data Security Requirements: Any data collector that owns, maintains, stores, or licenses records that contain Personal Information concerning an Illinois resident must implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

   In the event such data collector discloses Personal Information to a third party pursuant to a contract, such contract must contain provisions requiring such third party to implement and maintain similar reasonable security measures.

5. Interaction with HIPAA and GLBA: A data collector that has implemented security standards in compliance with the Gramm-Leach-Bliley Act ("GLBA") is now deemed to comply with the above security requirements. Furthermore, any covered entity or business associate subject to HIPAA that complies with the privacy and security standards for the protection of electronic health information will be considered to be in compliance with the requirements of PIPA, *provided that* if the covered entity or business associate must notify the Secretary of the Department of Health & Human Services (the "Secretary") of such data breach, it must also notify the Illinois Attorney General within five days of notifying the Secretary.

Implications for Health Care Providers, Medical Device Companies, and Digital Health Companies

The obligation to notify the Illinois Attorney General within five days of providing notice to the Secretary is significant since we understand that the Illinois Attorney General, who also has the authority to enforce HIPAA, intends to continue focusing on data privacy and security enforcement in the coming years. As a result, health care providers, medical device companies, and digital health companies should ensure that all Personal Information in their possession is subject to the same HIPAA protections and security standards regardless of whether such Personal Information is also deemed to be protected health information under HIPAA. Given the increase in enforcement and potential for increased fines and penalties, covered entities and business associates should consider whether to automatically report a security incident without the benefit of undertaking a risk assessment to determine whether such incident actually rises to the level of a breach, or whether in fact there is a low probability of compromise of the data, in which case such incident would not rise to the level of a reportable breach.

To the extent health care providers, medical device companies, and digital health companies take the position that they are not covered entities or business associates under HIPAA, and, given the expanded definition of "Personal Information," including the addition of the broad "Medical information," companies should take inventory of the data elements collected from individuals and determine whether such data is nevertheless subject to PIPA. Companies that deal with such electronic information will need to implement reasonable security measures to protect the Personal Information, and must also have contracts in place requiring third parties who receive Personal Information to safeguard such information with reasonable security measures. It is unclear what the Illinois Attorney General will expect regarding the implementation of "reasonable security measures" by data collectors, but the Illinois Attorney General may look to GLBA, PCI, FCRA and HIPAA standards, and/or utilize its 2012 guidance, *Information Security and Security Breach Notification Guidance*.[3]

Please let us know if you have any questions on PIPA's new amendments or how to comply with its security and breach notification requirements.

[3] Illinois Attorney General, *Information Security and Security Breach Notification Guidance*, Jan. 27, 2012. Such 2012 guidance has detailed recommendations for i) physical and electronic safeguards, including PCI standards for transmission of payment information and employee training; ii) information security program standards based upon GLBA and FCRA guidance; iii) steps for responding to data breaches; and iv) satisfying notification requirements in the event of a breach of Personal Information. However, we have not seen an indication from the Illinois Attorney General to date whether data collectors should use the 2012 guidance or wait for new guidance.