

# **Workplace Privacy, Data Management & Security Report**

## **Illinois Enacts Amendments to the Personal Information Protection Act**

By Jeffrey M. Schlossberg on June 8, 2016

Last month, Illinois Governor Bruce Rauner signed into law a number of amendments to the State's Personal Information Protection Act ("PIPA") that expand the definition of protected personal information and increase certain data breach notification requirements. The amendments, highlighted below, take effect January 1, 2017.

Currently, "personal information" is limited to an individual's first name or first initial and last name in combination with the individual's Social Security number; driver's license number or state identification card number; or account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

The amendments now expand the definition of "personal information" to include medical information, health insurance information, or unique biometric data. Importantly, beginning in January, PIPA will require entities that suffer a security breach to inform Illinois residents of the security breach *even if* the personal information was encrypted or redacted but the password/keys to unencrypt or underact that information is also acquired through the breach.

In addition, "personal information" will now 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, when either the user name or email address or password or security question and answer are not encrypted or redacted.

Under the new provisions, if notice is required and the breach of security involved an individual's user name or email address, the notice is required to direct individuals to promptly change their user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online account for which the individual uses the same user name or email address and password or security question and answer.

An entity in possession of personal information will be required to implement and maintain reasonable security

measures to protect the records from unauthorized access, destruction, or disclosure. Any entity that is in compliance with Section 501(b) of the Gramm-Leach-Bliley Act will be deemed in compliance with this provision. Similarly, a HIPAA covered entity or business associates subject to the privacy and security standards will also be deemed to be in compliance with PIPA. A covered entity or business associate that is required to provide notification of a breach to the Secretary of Health and Human Services under the HITECH Act must also provide such notification to the Illinois Attorney General.

As states continue to expand their breach notification statutes, compliance will continue to become more and more difficult.

Copyright © 2016, Jackson Lewis P.C.. All Rights Reserved.

STRATEGY, DESIGN, MARKETING & SUPPORT BY **LEXBLOG**