Illinois Health and Hospital Association

Amendment to Illinois PIPA's Breach Notification Requirement

Kathryn E. Brown, Staff Counsel
May 6, 2020

Effective January 1, 2020, Illinois' Personal Information Protection Act ("PIPA"), 815 ILCS 530, was amended to expand the breach notification requirements. See Public Act 101-0343 which enacts SB 1624.

Data Collectors that are required to notify more than 500 Illinois residents as a result of a single breach of the security system[1] must now also notify the Illinois Attorney General of such breach.[2] The notification to the Illinois Attorney General must be made in the most expedient time possible and without unreasonable delay but in no event later than when the data collector provides notice to consumers[3] and include:

- A description of the nature of the breach or unauthorized acquisition or use
- The number of Illinois residents affected by the incident at the time of notification; and
- Any steps the data collector has taken or plans to take relating to the incident.[4]

As well, if the date of the breach is unknown at the time the notice is sent to the Illinois Attorney General, the Data Collector must send the Illinois Attorney General the date of the breach as soon as possible.[5]

After receiving notice of the breach, the Illinois Attorney General may publish the name of the Data Collector that suffered the breach, the types of personal information compromised, and the date range of the breach.[6]

This breach notification requirement does not apply to Data Collectors that are regulated as Covered Entities or Business Associates under HIPAA and in compliance with Section 50 of PIPA.[7] Section 50 of PIPA states that:

---

[1] "Breach of a security system" or "breach" means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. "Breach of the security of the system data" does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure. 815 ILCS 530/5.
[2] 815 ILCS 530/10(e)(2).
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] 815 ILCS 530/10(e)(1).

> "Any covered entity or business associate that is subject to and in compliance with the privacy and security standards for the protection of electronic health information established pursuant to the federal Health Insurance Portability and Accountability Act of 1996 and the Health Information Technology for Economic and Clinical Health Act shall be deemed to be in compliance with the provisions of this Act, provided that any covered entity or business associate required to provide notification of a breach to the Secretary of Health and Human Services pursuant to the Health Information Technology for Economic and Clinical Health Act also provides such notification to the Attorney General within 5 business days of notifying the Secretary."[8]

Entities that are regulated as Covered Entities[9] and Business Associates[10] will still need to comply with the new breach notification requirement to the extent they are operating outside those functions that subject it to regulation as a Covered Entity or Business Associate.

For example, if an entity that is regulated as a Covered Entity happens to experience a breach of the security system related to its functions as an employer rather as a health care provider, health plan, or healthcare clearinghouse, then such entity would have to comply with PIPA's breach notification requirements, which could include notification to the Illinois Attorney General depending upon the number of records breached.

Given the recent trend of states introducing state privacy legislation that is similar to the European Union's General Data Protection Act ("GDPR") and the California Consumer Privacy Act ("CCPA"),[11] it is likely that more bills related to privacy will continue to be introduced in Illinois.

---

[8] 815 ILCS 530/50.

[9] "Covered Entity" means a 1) health plan, 2) healthcare clearinghouse, or 3) healthcare provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA. 45 C.F.R. § 160.103.

[10] 45 C.F.R. § 160.103.

[11] *See* Libbie Canter, *State Privacy Trends to Watch in 2020*, INSIDE PRIVACY (Jan. 16, 2020), https://www.insideprivacy.com/united-states/state-legislatures/state-privacy-trends-to-watch-in-2020/ (last accessed March 20, 2020).