Ogletree Deakins

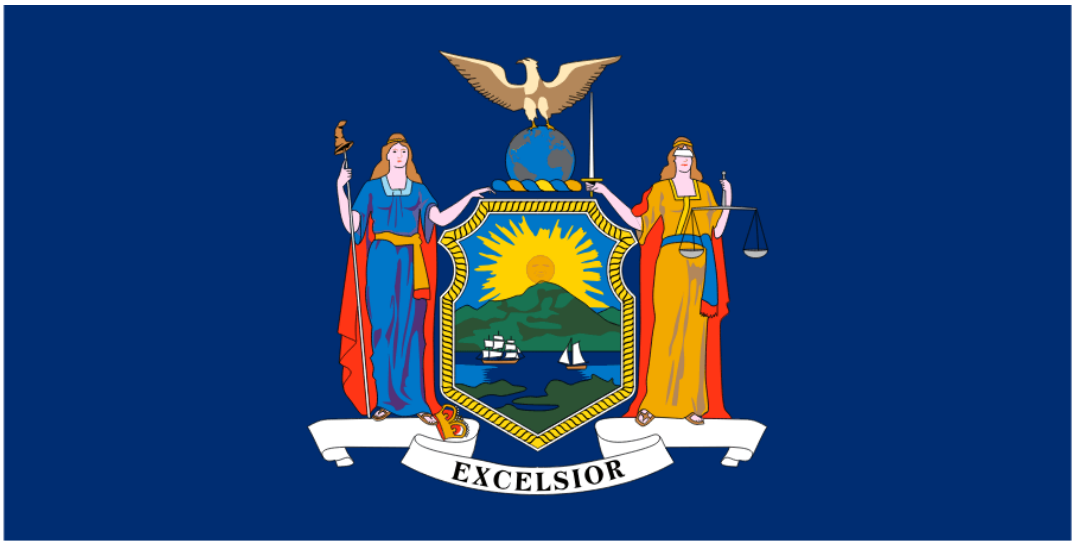
New York Amends Data Breach Notification Law to Enhance Notification Requirements, Expand Definition of 'Private Information'

January 14, 2025

By Benjamin W. Perry, Jeffrey D. Coren, and Yomaris Sanchez-Orona

On December 24, 2024, New York Governor Kathy Hochul signed into law amendments to New York's private-sector data breach notification law (General Business Law § 899-aa) and government agency data breach notification law (New York State Technology Law § 208).

The private-sector changes include a thirty-day deadline for businesses to notify New York residents impacted by a data breach, and both laws now have an expanded definition of "private information" that includes medical and health insurance information. The new notification requirements are effective immediately, whereas the expanded definition of "private information" will become effective on March 21, 2025, for both laws.



Quick Hits

- Businesses must now notify New York residents impacted by a data breach within thirty days after a data breach has been discovered.
- The state's Department of Financial Services must now be notified of a data breach along with other regulatory agencies.
- The definition of "private information" was expanded to include a person's medical information and health insurance information.

Notification Requirements

Effective immediately, persons or businesses that are required to notify New York residents of a data breach must provide notification within **thirty days** after discovery of the breach. This same thirty-day timeframe also applies to the obligation for service providers to notify the data owner or licensee of a data breach. Previously, the New York data breach notification law required only that disclosure of a breach be made as expediently as possible and without unreasonable delay, but it did not provide a specific deadline. The amendments further removed language in the law that allowed businesses to delay notification consistent with "any measures necessary to determine the scope of the breach and restore system integrity," although notification may still be delayed based on the legitimate needs of law enforcement. Both of these changes eliminate the flexibility businesses were previously afforded in the timing of data breach notifications.

The amendments also expand data breach notice requirements to regulatory agencies. The New York State Department of Financial Services (NYDFS) must now be notified of a data breach, in addition to the previously existing requirement to notify the state's attorney general, the New York Department of State, and the state police. Such agency notices must still include the timing, content, and distribution of the notices, the approximate number of affected persons, and a template of the individual notice. This requirement to notify NYDFS is also separate from the disclosure requirements for covered entities under the NYDFS cybersecurity regulations (23 NYCRR Part 500).

The thirty-day notification requirement, however, does not apply to data breach notification obligations for government agencies or entities. These public entities are still only required to notify affected individuals "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement … or any measures necessary to determine the scope of the breach and restore the integrity of the data system." In other words, although private-sector businesses now have a strict thirty-day deadline to report data breaches, state governmental agencies and entities still enjoy wider discretion in the timing of their same notification obligations.

Expanded Definition of 'Private Information'

The amendments further expand the definition of "private information" under both the private-sector and public-sector data breach notification laws. Effective March 21, 2025, private information under both laws

will also include:

- **medical information**, including the individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; and

- **health insurance information**, including the individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application or claims history, including the individual's appeals history.

The expanded definition of "private information" means that a data breach involving medical or health insurance information may now trigger notification requirements under New York law. Notably, the New York data breach notification laws are distinct from other state and federal laws that govern medical or health insurance information in certain contexts, such as the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule, the Federal Trade Commission's Health Breach Notification Rule, and the recently adopted New York State Department of Health's hospital cybersecurity regulations. As a result, in some instances, a data breach involving medical or health insurance information may now implicate overlapping legal obligations and notification requirements.

Key Takeaways

Businesses may want to consider reviewing their incident response plans and other data security policies and practices to comply with New York's updated data breach notification requirements.

Ogletree Deakins' Buffalo office, New York office, and Cybersecurity and Privacy Practice Group will continue to monitor developments and provide updates on the Cybersecurity and Privacy, Healthcare, and New York blogs as additional information becomes available.

Follow and Subscribe

LinkedIn | Instagram | Webinars | Podcasts

AUTHORS

Benjamin W. Perry

Shareholder, Nashville

[Jeffrey D. Coren]

Of Counsel, Buffalo

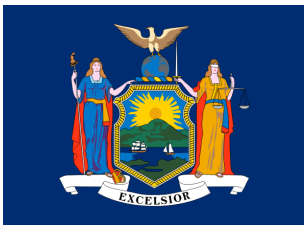
[Yomaris Sanchez-Orona]

Associate, Buffalo

TOPICS

Cybersecurity and Privacy , Healthcare , New York , State Developments

RELATED ARTICLES



February 13, 2025

New York Federal Court Ruling Highlights a Potential Pitfall in Settlement Agreement Enforcement

February 11, 2025

Keeping Cool: Understanding Nevada OSHA's Heat Illness Prevention Guidance

RELATED PODCAST

December 17, 2024

Top Issues for U.S. Employers in Germany

RELATED ARCHIVED WEBINAR

November 20, 2024

Pay Transparency Update: Additional State Laws Take Effect Soon