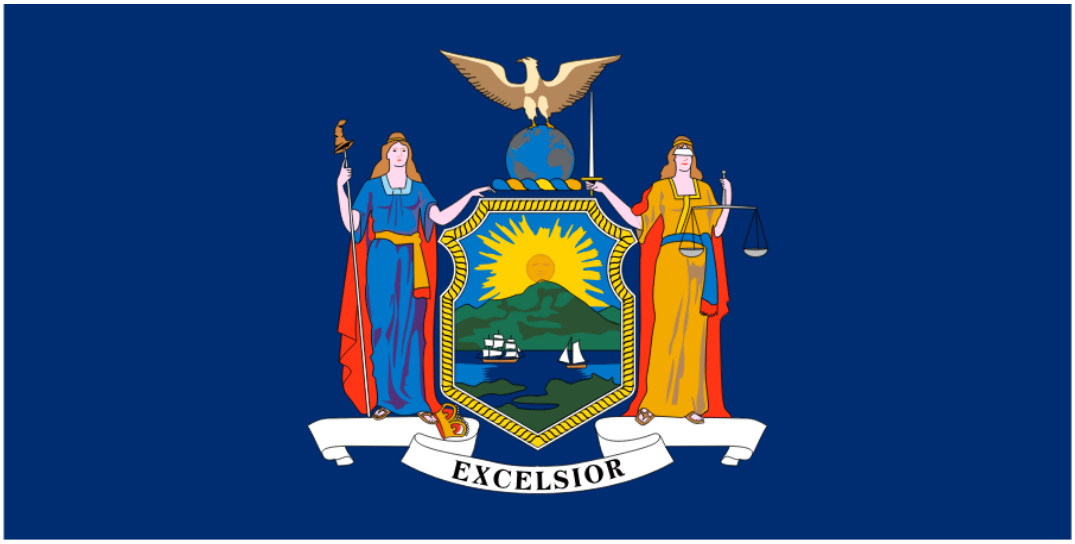
Ogletree Deakins

New York Health Data Requirements Potentially Ahead: Understanding the Newly Passed Health Information Privacy Act

March 10, 2025

By Jeffrey D. Coren and Zachary V. Zagger

New York lawmakers recently passed a wide-ranging health information privacy bill that would require entities to obtain consent to collect, use, or sell an individual's health information except for designated purposes. Notably, the bill broadly defines both regulated entities and regulated health information, and it would potentially impact companies nationwide that may not otherwise consider themselves to be collecting individuals' private health information.



Quick Hits

- New York lawmakers passed a health information privacy bill that, among other obligations, would require entities to obtain authorization to collect, use, or sell an individual's health information unless it is "strictly necessary" for certain purposes.
- The bill broadly defines regulated health information to include data that goes beyond traditional protected health information (PHI) and broadly defines regulated entities to include New York entities and

certain non-New York entities.

- While there is no private right of action, the bill would empower the state attorney general to seek significant penalties for violations.
- The governor must still sign the bill and it would take effect one year after becoming law.

On January 22, 2025, the New York State Legislature passed Senate Bill (S) 929, known as the New York Health Information Privacy Act (New York HIPA). The bill has not yet been sent to Governor Kathy Hochul's desk for signature. If signed, New York HIPA would take effect one year after becoming law.

In general, New York HIPA would place strict requirements on the collection or "processing" of individual health information or "any information that is reasonably linkable" to an individual's mental or physical health. It would require authorization to process regulated health information unless it is "strictly necessary" for a specific designated purpose. The bill would further give individuals a right to access and request deletion of their health information and require regulated entities to develop and maintain safeguards to protect health data.

New York HIPA is the latest of a series of state privacy laws being considered and passed in recent years, such as Washington State's recently enacted My Health My Data Act (MHMDA), which imposes a host of requirements for businesses in Washington concerning the collection of "consumer health data." That law is at the center of a recently filed and potentially precedent-setting class action alleging that advertising software attached to third-party mobile phone apps unlawfully harvested PHI in the form of location data from millions of users. Unlike Washington's MHMDA, New York HIPA would not provide a private right of action for individuals to file suit, but New York HIPA would empower the attorney general to enforce the law and allow for the imposition of stiff monetary penalties for violations.

Here is a breakdown of some key New York HIPA bill provisions.

Processing Regulated Health Information

New York HIPA, if enacted, would make it generally unlawful for a regulated entity to sell an individual's regulated health information to a third party or process such information without a valid authorization unless it is "strictly necessary" for specific purposes. The bill details the requirements for obtaining valid authorization and the permissible purposes for processing without authorization. New York HIPA broadly defines "processing" to include the collection, use, access, sharing, sale, monetization, analysis, and retention, among other actions, of an individual's regulated health information.

Notably, New York HIPA defines "regulated health information" broadly as "any information reasonably linkable" to an individual or device that "is collected or processed in connection with an individual's physical or mental health," including "location or payment information that relates to an individual's physical or mental

health" or "any inference drawn or derived about an individual's physical or mental health." This expansive definition could include a wide range of data points or information about individuals that might not typically be considered PHI, such as location data and payment information related to trips to the doctor or the gym.

New York HIPA also includes a broad definition of regulated entities. A "regulated entity" would include both entities located in New York that control the processing of regulated health information, and non-New York entities that control the processing of regulated health information of New York residents or individuals who are "physically present in New York."

Designated Purposes

New York HIPA also sets forth the designated purposes for collecting or processing an individual's health information without specific authorization. The collection or processing would need to be "strictly necessary" for:

1. providing a product or service that the individual has requested;
2. conducting internal business operations, excluding marketing, advertising, research and development, or providing products or services to third parties;
3. protecting against fraud or illegal activity;
4. detecting and responding to security threats;
5. protecting the individual's "vital interests"; or
6. investigating or defending a legal claim.

Requests for Authorization

Under the bill, an authorization request must be separate from any other transaction, and individuals must be allowed to withhold authorization separately for each kind of processing. A "valid authorization" must also include several specific disclosures, including "the nature of the processing activity" and "the specific purposes for such processing."

Individual Rights

New York HIPA would further require regulated entities to provide an "easy-to-use mechanism" for individuals to request access to and delete their regulated health information. Regulated entities would be required to provide access to or delete health data within thirty days of a request. If using a service provider, regulated entities would be required to communicate the request to a service provider within thirty days "[u]nless it proves impossible or involves disproportionate effort."

Exemptions

The bill exempts certain information from its provisions, including:

- "information processed by local, state, and federal governments, and municipal corporations";
- PHI governed by federal regulations under the Health Insurance Portability and Accountability Act (HIPAA);
- covered entities governed by HIPAA; and
- certain information collected as part of clinical trials.

Notably, the bill does not exempt entities subject to the Gramm-Leach-Bliley Act. Further, the bill does not exempt "business associates" under HIPAA with respect to "regulated health information" that goes beyond traditional PHI.

Security Safeguards

Under New York HIPA, regulated entities would be required to develop and maintain reasonable safeguards to protect the security, confidentiality, and integrity of regulated health information. They would also be required to securely dispose of such information according to a publicly available retention schedule.

The bill does not address the obligations of a regulated entity in the event of a data breach. New York's data breach notification law (General Business Law § 899-aa), however, was recently amended to expand the definition of "private information" to include medical information and health insurance information, and to impose a thirty-day deadline for businesses to notify New York residents impacted by a data breach.

Service Providers

The bill would require any processing of health information by service providers on behalf of regulated entities to be governed by a written agreement. That agreement would need to include specific obligations for the service provider, such as ensuring confidentiality, protecting the data, and complying with individual rights requests.

Contracts and Waivers

Any contractual provision or waiver inconsistent with New York HIPA would be declared void and unenforceable, meaning individuals would not be able to waive their rights under the law.

Enforcement

New York HIPA would empower the state attorney general to investigate alleged breaches of the privacy requirements and bring enforcement actions. Such actions could result in civil penalties of up to $15,000 per violation or up to 20 percent of the revenue obtained from New York consumers within the past fiscal year, whichever is greater. The bill would also give the attorney general the ability to enjoin violations, seek restitution, and obtain the disgorgement of profits "obtained directly or indirectly" by any violations. Unlike Washington State's MHMDA, the bill does not include a private right of action for individuals to sue for violations.

Next Steps

New York HIPA underscores the state's focus, and a broader focus of states across the country, on protecting the privacy of health information. Like Washington's MHMDA, New York HIPA would broadly define regulated health information as any information reasonably tied to an individual or device and related to an individual's physical or mental health, including location and payment information. The bill therefore seeks to protect a broader scope of health data than what has been historically viewed as PHI under HIPAA.

New York HIPA has potential far-reaching implications for businesses nationwide that collect or process data of New York residents or individuals located in New York. If the bill is signed into law, such businesses may wish to review and consider changes to their data processing practices, data handling policies, employee training programs, contractual agreements with service providers, and customer agreements. Additionally, they may want to review their websites with respect to collecting user information and providing consumers with opt-outs.

Notably, however, New York HIPA must still be delivered to and signed by Governor Hochul, who may seek to negotiate changes to the bill before signature or effectuate changes later through chapter amendments. The governor has shown a propensity to use such chapter amendments, which refer to changes by the governor that are approved by the legislature through subsequent legislation after the law has been signed. In addition, if enacted, the bill provides that the attorney general can promulgate rules and regulations to enforce the law.

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

Follow and Subscribe

LinkedIn | Instagram | Webinars | Podcasts

AUTHORS

[Jeffrey D. Coren]

Of Counsel, [Buffalo]

[Zachary V. Zagger]

Senior Marketing Counsel, [New York]

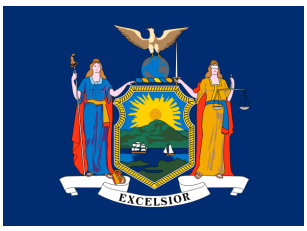
TOPICS

[Cybersecurity and Privacy] , [Healthcare] , [New York] , [State Developments]

RELATED ARTICLES

March 10, 2025

South Carolina House and Senate Introduce Legislation on Diversity, Equity, and Inclusion



March 6, 2025

New York's Proposed Employment Contract Reforms: What Employers Need to Know

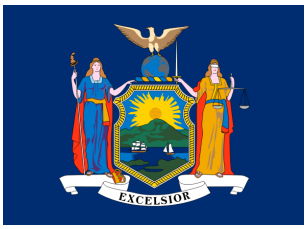
RELATED PODCAST

December 18, 2024

Nevada's New Safety Rules: Can Employers Beat the Heat?

RELATED ARCHIVED WEBINAR

January 21, 2025



New York’s Groundbreaking Paid Prenatal Leave Law: How to Prepare