New Year, New Health Privacy Law? – What You Need to Know About NYHIPA

Alysa Z. Hutnik, Aaron J. Burstein, Alexander I. Schneider, Meaghan M. Donahue

January 29, 2025

A New York health privacy law has moved quickly through both chambers of the state legislature and is up for review by Governor Kathy Hochul. The New York Health Information Privacy Act ("NYHIPA") bears striking resemblance to similar laws in Washington, Nevada, and Connecticut, but also adopts novel provisions that could make this one of the most stringent privacy laws on the books in the U.S.

Scope and Applicability:

NYHIPA governs "regulated health information" – "*any information* that is reasonably linkable to an individual, or a device, and is *collected or processed in connection with* the physical or mental health of an individual." This specifically includes location or payment information, in addition to inferences drawn about an individual's mental or physical health, even when not based on sensitive information.

NYHIPA's definition of regulated health information is unique compared to other health privacy laws. In some ways it may be broader. For instance, it does not include a nexus to personal information (*see, e.g.*, "consumer health data" under Washington's My Health, My Data Act, which is defined as *personal information* that *identifies* a consumer's past, present, or future mental or physical health status). Additionally, NYHIPA does not include a carve out for publicly available data or data covered by the Gramm-Leach-Bliley Act, meaning that financial institutions, banks, and credit card companies could be impacted by this law. By contrast, in other ways it might be narrower. For example, NYHIPA's definition does not include reference to health care services or supplies/products, which is defined broadly by Washington and Nevada's laws to include any service or product provided to improve a person's health.

NYHIPA applies to businesses that 1) control the processing of regulated health information of residents of New York State, 2) control the processing of regulated health information of any person located in New York State when their information was collected, or 3) are located in New York State and process regulated health information.

Valid Authorization:

NYHIPA goes beyond consent requirements in similar laws by requiring *valid authorization* for *any processing* of regulated health information that is not strictly necessary to perform a list of services enumerated by the statute, such as providing the service requested by the consumer and conducting internal business operations. Notably, "conducting internal business operations" *explicitly excludes* activities related to marketing, advertising, or research and development.

Valid authorization as defined by NYHIPA is an extremely high bar, which may prove difficult for regulated entities to obtain. To collect or process regulated health information outside of a permissible purpose, regulated entities must:

- Make a request for valid authorization that is separate from any other transaction the regulated entity has with the consumer;
- Present consumers with a detailed disclosure, describing how regulated health information will be processed and how consumers can exercise their privacy rights;
- Allow consumers to provide or withhold authorization separately for *each category of processing activity*; and
- Obtain a consumer's written or electronic signature and establish an expiration date, after which the regulated entity must re-collect valid authorization.

Valid authorization also requires regulated entities disclose how the consumer can revoke authorization prior to expiration. If a consumer revokes their authorization, regulated entities must *immediately* cease all associated processing activities.

Similar laws in Washington and Nevada require valid authorization *only to sell* consumer health data – collecting and sharing merely require informed consent. Operationally, obtaining valid authorization may be an insurmountable challenge for businesses, so the fact that NYHIPA would require it for any collection or processing of regulated health information is notable.

Other requirements:

Health privacy policy: Similar to Washington and Nevada, NYHIPA requires regulated entities that process regulated health information for a permissible purpose to provide a notice detailing the collection and processing of the information. NYHIPA does not require this notice to be separate or distinct from other policies, as Washington does. However, if the regulated entity "materially alters" its processing activity, it must provide a notice separate from the privacy policy that explains the applicable changes.

Consumer Rights: NYHIPA provides consumers the right to access and delete their regulated health information via an "effective, efficient, and easy-to-use mechanism through an interface the consumer regularly uses[.]" Notably, consumers may engage an authorized agent to make these requests on their behalf, but the statute does not speak to whether the regulated entities may take steps to validate the identity of the requestor. While authorized agents are permitted to act on behalf of consumers in many comprehensive privacy laws, health privacy laws in Washington and Nevada do not provide this right. Regulated entities must fulfill deletion and access requests in no later than 30 days, and must pass deletion requests to downstream service providers or third parties.

Required contract terms: NYHIPA includes specific contract requirements for service providers, unique among the other health-specific state privacy laws. While the required contract terms largely mirror those required by the CCPA regulations, there are some differences, such as a requirement to notify a regulated entity in advance prior to transferring regulated health information to other service providers.

Security requirements: Different from Washington and Nevada, NYHIPA explicitly requires regulated entities to develop and maintain physical, technical, and administrative safeguards to protect

regulated health information, and also requires regulated health information be deleted pursuant to a public retention schedule no later than 60 days after it is no longer necessary to maintain for the purpose of collection and processing.

Enforcement:

NYHIPA provides the New York attorney general with enforcement authority, and also provides authority to promulgate implementing regulations. Potential rulemaking could offer clarity for regulated entities subject to compliance with this law, particularly related to open questions regarding the law's scope and applicability.

Conclusion:

Though NYHIPA shares many similarities with other health-related state privacy laws passed in the previous two years, its broad scope, ambiguous definitions, and stringent consent requirements may prove to create compliance challenges for regulated entities. Because of NYHIPA's potentially broad applicability, companies across the U.S. should closely monitor NYHIPA's progression.