Insights, News & Events

NEW YORK ON VERGE OF ENACTING SWEEPING HEALTH DATA PRIVACY LAW: ANSWERS TO YOUR KEY QUESTIONS AND 6 STEPS TO PREPARE

Insights
Jan 23, 2025

In a major development for all businesses handling health data, New York lawmakers passed a sweeping health data privacy bill yesterday that could have far-ranging consequences across the country. S929, also known as the New York Health Information Privacy Act (NYHIPA), now awaits the signature of Governor Kathy Hochul. If she signs it into law, any entity that processes health information concerning individuals who are physically present in New York – even if the organization itself is beyond the state borders – will face stringent new consequences within six months or so. Below is an in-depth overview of the key provisions and answers to your key questions about what your organization should consider doing now.

What is the Background of This Proposed Law?

NYHIPA is the latest in a wave of state-level health data legislation aiming to plug gaps left by the federal Health Insurance Portability and Accountability Act (HIPAA). Although the new law is one "A" short of HIPAA, it pulls a ton more weight than its federal counterpart and even goes further than its counterparts in other states.

Just a year and a half ago, Washington was the latest state to enact a comprehensive health information privacy law called the My Health My Data Act (MHMDA). While NYHIPA shares some conceptual similarities with MHMDA and other state laws protecting consumer health data, New York's approach introduces several distinctive requirements that could greatly impact how health-related services collect, use, store, and share data.

Related People

Omeed Askari-Behbahani
Associate
858.964.1587

Melissa Camire
Partner
212.899.9965

Why is This Proposed Law So Significant?

Needless to say, anyone familiar with NYHIPA will tell you it's earth shattering among healthcare privacy laws if for nothing other than its broad definitions of "regulated entity" and "regulated health information" (discussed in detail below). For comparison, most of us are familiar with the federal privacy law, HIPAA. But most folks don't know that HIPAA applies to a very narrow set of entities and very specific circumstances (although, it is set to undergo a major overhaul this year).

- For example, HIPAA generally does not protect your health information contained in your personnel file at work.
- Nor does HIPAA typically protect students' health information kept in school records (e.g., immunization records, medical accommodation requests).

In contrast, NYHIPA imposes significant new obligations on businesses of all kinds and sizes that interact with health data in virtually any form – from telehealth platforms, credit card processors, and fitness apps to wearable device manufacturers, employers, and schools.

What Entities Does the Act Cover?

Crucially, NYHIPA's reach is not limited to New York-based organizations. Any entity that processes or collects health information of a New York resident or health information linked to someone "physically present" in New York is subject to the new rules. This extraterritorial approach goes further than NYHIPA's counterparts in other states and signals that organizations without a physical presence in New York must still consider whether their services are accessed by New York consumers.

For example, Washington's MDMHA applies only to entities that do business in Washington or target Washington consumers, and that have control to determine the purpose and means of processing the consumer health data they collect, share, and/or sell. In contrast, NYHIPA applies to *any entity* that controls the processing of "regulated health information" belonging to any person physically present in New York, or New York residents located anywhere in the country. For example, if a New York resident is attending university at in San Diego, any of that student's health care

Usama Kahf, CIPP/US

Partner

949.798.2118

Service Focus

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

Related Offices

New York

data collected by the school in San Diego is likely subject to NYHIPA.

Will This Act Get Signed into Law? And When Would it Be Effective?

Though we have no indication yet about whether Governor Hochul will sign the Act, many businesses are bracing for its likely enactment and its operational and compliance impacts. If Governor Hochul signs the Act, NYHIPA could take effect as soon as 180 days thereafter — leaving a tight window for organizations to align their data practices with the law's provisions.

What Data Does the Act Protect?

One of the Act's most significant features is its broad definition of "regulated health information," or "RHI." The Act defines RHI as "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." The definition even includes location and payment information related to someone's physical or mental health.

Consequently, this expansive definition captures a wide variety of data types, including without limitation:

- Information provided by consumers to telehealth platforms;
- Data processed or generated by wellness or fitness applications and smart devices (e.g., wearable heart-rate monitors, smart watches, and smart phones);
- User-generated content on websites or apps that might indicate health conditions or personal health practices;
- Health information provided to schools, colleges, and universities; and
- Health information provided to employers in New York, and employers with remote workers living in New York.

With only four express exemptions, NYHIPA does not apply to:

- Information processed by any level of government;

- The already-protected health information governed by HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH);
- The three types of entities (and their business associates) subject to HIPAA and HITECH to the extent those federal laws already provide privacy protection (meaning NYHIPA will fill any gaps); and,
- Information collected as part of a clinical trial and governed by the Federal Policy for the Protection of Human Subjects, a.k.a. "the Common Rule."

Because NYHIPA explicitly avoids listing finite categories of covered health data, businesses need to examine any data that might directly or indirectly relate to an individual's health status, bodily functions, or mental well-being. Determining whether your organization handles regulated health information is the essential first step in assessing your compliance obligations.

Will There Be Stricter Limits on Processing Health Data?

Yes, most definitely. Under NYHIPA, unless an individual provides explicit authorization (discussed below in Section 4), a company may only process regulated health information if it is "strictly necessary" for one of seven enumerated permissible purposes. This stricter standard goes beyond the "necessary" or "compatible" use frameworks found in other privacy laws. Here, processing must align with one of these seven specific justifications:

- **Providing or Maintaining a Specific Product or Service**
  The data use must be essential for delivering or supporting the particular product or service that the individual has requested. For instance, a telemedicine app may collect and process users' vitals if it is "strictly necessary" for a remote consultation.
- **Performing Internal Business Operations**
  This category is meant to cover operational tasks like billing, accounting, or quality assurance. However, companies should note that the law constrains what counts as "strictly necessary" internal functions. Ancillary marketing uses, for example, would not qualify.
- **Preventing Fraud or Protecting Against Illegal Activity**
  If the data processing is essential to detect or prevent

fraud related to the health services provided, an entity may rely on this permissible purpose. Nevertheless, "strict necessity" will limit the ability to collect or share health data for more generalized fraud detection programs that are not directly tied to the product or service in question.

- **Detecting or Responding to Security Incidents**
  Protecting systems from security threats can justify data processing. For instance, using health-related data logs to investigate and mitigate a ransomware attack could fall within this permissible purpose, provided the processing is no broader than required for security.

- **Protecting the Vital Interests of an Individual**
  In emergency situations — for example, life-threatening scenarios where an individual cannot provide consent — the law permits data processing to ensure the immediate safety or essential medical care of that individual.

- **Preparing for or Defending Legal Claims**
  Data processing is justified if a regulated entity is investigating, establishing, exercising, preparing for, or defending a legal claim.

- **Complying with a Court Order or Other Legal Obligation**
  This catch-all category refers to any specifically authorized use under state or federal law. Businesses may process regulated health information to the extent required by law, regulation, court order, or other valid legal or regulatory processes. Organizations should ensure they do not exceed the narrow scope of what is legally mandated and carefully confirm that the data processing is indeed "strictly necessary" to carry out the organization's legal obligations.

If processing regulated health information does not align with one of these seven categories, NYHIPA requires that the individual provide a valid authorization (explored in the next section). In practice, these enumerated permissible purposes significantly narrow the range of health data activities an organization can engage in without first obtaining explicit permission.

What are the Consent Requirements? And What About the 24-Hour Waiting Period?

NYHIPA introduces one of the most stringent consent frameworks in U.S. privacy law. When a company's

processing of regulated health information exceeds the permissible purposes set out above, it must secure what the law refers to as a "valid authorization." Key points to note include:

- **High Bar for Authorization**: This valid authorization is a formal, written (or equivalently documented electronic) standalone agreement through which the individual expressly consents to the collection, use, or sharing of their health data. Further, when requesting authorization for multiple categories of processing activities, the consumer must have the option to provide or withhold authorization separately for each category of processing. Organizations must ensure they present the authorization request in a clear, conspicuous manner and in plain language that details the scope of data use.
- **24-Hour Waiting Period**: In a unique twist, NYHIPA prohibits obtaining this authorization until at least 24 hours after an entity's initial interaction with a consumer. This waiting period is intended to prevent individuals from feeling rushed or confused when consenting to share sensitive health information. Organizations will therefore need to design user flows and data collection strategies that respect this mandatory pause.
- **Opt-In vs. Opt-Out**: Unlike some state privacy laws that merely require an opt-out mechanism for certain uses of personal data, NYHIPA generally mandates opt-in authorizations for any collection, use, or disclosure of regulated health information that does not fall under the seven permissible purposes.
- **Authorization Request Limit**: If a consumer revokes or withholds authorization for a particular processing activity, organizations may not again request authorization for that processing activity for a period of 12 months from the date the individual withheld or revoked authorization.
- **Contracts & Waivers Void**: Any contract provisions or waivers that are inconsistent with NYHIPA are considered void and unenforceable. Organizations should review their policies and procedures and update accordingly.

What are the Revocation and Data Deletion Obligations?

NYHIPA stands out for its unprecedented approach to revoking consent. If an individual decides to revoke a

previously granted authorization, the covered entity must "immediately cease all processing activities" related to that authorization, except to the extent necessary to comply with the organization's legal obligations (e.g., Medicare retention requirements). This likely requires businesses to delete or segregate the individual's data at once, rather than within the more typical 30-to-45-day compliance window seen in other privacy frameworks.

In addition, the law stipulates separate timelines for other consumer rights — such as the right to request access or deletion of existing health data — with a general 30-day requirement to respond. While this 30-day period is still stringent, it is the immediate cessation requirement upon revocation that could pose the greatest operational challenges. Covered entities may need to restructure their data retention systems to ensure they can promptly isolate and delete data once a consumer withdraws consent.

How Will the Law Be Enforced and What are the Potential Penalties?

NYHIPA has significant penalties for non-compliance. As enacted, the New York Attorney General has enforcement authority and can leverage both investigative powers and civil penalties of up to $15,000 per violation or 20% of revenue obtained from New York consumers within the prior fiscal year, whichever is greater.

Notably, the Act does not provide a private right of action to individuals. Some observers suggest that, given recent legislative trends, the New York Legislature may lean toward providing an avenue for individuals to bring suit directly against non-compliant entities, although this is not yet certain. Whether or not future regulations or amendments to the Act grant a private right of action to consumers remains a high-stakes question.

Organizations should be prepared for active enforcement once the law takes effect. Regulators in other states with similarly sweeping privacy laws have signaled aggressive enforcement, and New York is likely to follow suit. Thus, establishing a clear compliance roadmap and training relevant staff will be critical steps in avoiding enforcement actions, financial penalties, and reputational harm.

What are the Practical Steps We Can Take to Prepare?

With NYHIPA now approved by the New York Senate and Assembly, organizations handling health data should begin readiness initiatives even before Governor Hochul signs the Act into law. Below are six practical steps to consider:

- **Data Mapping**: Conduct an internal audit to identify all sources of regulated health information, how it is used, and where it is stored. Understanding these data flows is the foundational step for any compliance program.
- **Policy and Procedure Overhaul**: Update privacy policies, notices, and employee handbooks to reflect NYHIPA's narrower lawful processing grounds and the new authorization requirements. If your existing policies reference HIPAA or other privacy standards, clarify how NYHIPA's stricter rules differ.
- **Consent Management**: Implement or refine consent management tools to handle the 24-hour waiting period and maintain records of when and how authorizations are granted or revoked. This may include updating user interfaces, forms, and workflows to incorporate clear notice and adequate delays.
- **Technical Adjustments**: Ensure systems can respond quickly to revocation requests by suspending or terminating data processing, as well as by deleting or segregating revoked data immediately. Many organizations may need new infrastructure or processes to comply with this stringent requirement.
- **Employee Training**: Provide comprehensive training for any employees who handle regulated health information, ensuring they understand the law's permissible purposes, consent requirements, and the gravity of immediate deletion obligations.
- **Monitoring Future Developments**: As with any legislation, final amendments or regulatory guidance could alter key provisions of NYHIPA. Keep an eye on official updates and subscribe to our FP Insights to ensure your compliance strategy remains accurate and current.

Conclusion

Although the legislation still awaits the Governor's signature, the margin of support in the state legislature suggests that New York is poised to join the ranks of states with robust

consumer health privacy laws. Organizations that begin their compliance preparations now will be better positioned to adapt swiftly should the legislation become law. In an environment of rapidly evolving privacy standards, proactive planning can help mitigate legal risk and demonstrate a commitment to consumer trust.

Fisher Phillips will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox. You can also visit FP's U.S. Consumer Privacy Hub for additional resources to help you navigate this area. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, any attorney in our New York City office, or any member of our Privacy and Cyber team.