REPORT ON LEGISLATION BY THE CIVIL RIGHTS COMMITTEE

A.2141	**M. of A. Rosenthal**
S.929	**Sen. Krueger**

AN ACT to amend the general business law, in relation to providing for the protection of health information.

New York Health Information Privacy Act

THIS LEGISLATION IS APPROVED

I. INTRODUCTION

It is a truism that modern life is increasingly—and perhaps predominantly—lived online, where personal information can easily and irretrievably be subject to theft, exposure, or manipulation. In this context, there is a passive if begrudging acceptance that no personal information is safe from prying eyes.

Still, even now, most people take it as an article of faith that health information is the exception, assuming that it is protected from disclosure behind a robust legal curtain. The Health Information Portability and Accountability Act ("HIPAA"),[1] a federal law that regulates how and to whom protected medical information is disclosed, is widely known as the cornerstone of medical confidentiality, ensuring that patients have control over who can access their medical records.

As important as HIPAA is, its scope is limited to information generated within traditional healthcare settings: hospitals, clinics, doctors' offices. But personal health information is not confined solely to medical records. HIPAA cannot reach beyond the clinic doors to protect data generated elsewhere, such as lifestyle apps, browser histories, and social media accounts. For third parties, the data contained in such digital repositories can be lucrative: companies routinely purchase private healthcare data for advertising purposes, often without consumers' knowledge or consent.[2]

[1] Public Law 104-191 (1996).

[2] *See, e.g.*, Lily Hay Newman, *Health Sites Let Ads Track Visitors Without Telling Them*, WIRED (Feb. 6, 2022), https://www.wired.com/story/health-site-ad-tracking/#:~:text=The%20tool%20shows%20what%20information,across%20the%20web%20for%20marketin; Matt Schwartz, Justin Brookman, & Margaret Oates, *Report: Companies Continue to Share Health Data Despite*

About the Association
The mission of the New York City Bar Association, which was founded in 1870 and has over 20,000 members, is to equip and mobilize a diverse legal profession to practice with excellence, promote reform of the law, and uphold the rule of law and access to justice in support of a fair society and the public interest in our community, our nation, and throughout the world.

The Supreme Court's decision in *Dobbs v. Jackson Women's Health*—overturning *Roe v. Wade* and unleashing a swarm of state laws that target deeply personal healthcare choices—deepened concerns over the vulnerability of consumer data to abuse and manipulation, underscoring the need for more robust protection of personal healthcare information.

In most cases, an abortion will leave a digital paper trail. Phone records to clinics, internet searches, ride-sharing histories—these and other sources can be scraped and pieced together to identify abortion-seeking patients or people who facilitate these procedures. This is not an idle or remote threat: prosecutors have already leveraged app-generated data to criminalize or penalize people seeking an abortion or those who aided them.[3]

The potential misuse of private healthcare information extends beyond reproductive health. An increasing number of states are banning gender-affirming care and implementing other anti-LGBTQ+ measures. The vast expansion of surveillance is aiding in efforts to target and discriminate against trans people, exploiting gaps in data privacy for healthcare information.[4]

Recognizing the dangers posed by the exposure of healthcare information, the New York legislature has passed legislation to make it harder for bad actors to weaponize such data: the New York Health Information Privacy Act ("NYHIPA").

II. PRE-EXISTING PROTECTIONS FOR HEALTH INFORMATION

Prior to NYHIPA, New York had already acted to protect private health information.

In 2023, the State enacted a law, known as HMH Part U,[5] that created a foundation for the protection of healthcare-related data. HMH Part U prohibited large communications companies and apps headquartered in New York from complying with out-of-state warrants seeking information related to reproductive health. It further forbade geofencing—the practice of creating virtual markers around particular geographic locations—around all healthcare facilities in New York. Finally, it stopped New York law enforcement agencies from purchasing health-related data

---

New Privacy Laws, CONSUMER REPORTS (Jan. 15, 2024), https://advocacy.consumerreports.org/research/report-companies-to-share-health-data-despite-new-privacy-laws/. (All websites last accessed Dec. 2025)

[3] *See, e.g.*, John Yang, Kaisha Young, & Marconja Zor, *Court Cases Targeting Abortion Highlight Digital Privacy Concerns*, PBS NEWS (Aug. 5, 2023), https://www.pbs.org/newshour/show/court-cases-targeting-abortion-highlight-digital-privacy-concerns#:~:text=Yes%2C%20authorities%20have%20used%20web%20searches%2C%20text,and%20he's%20using%20text%20messages%20as%20evidence; Jolynn Dellinger & Stephanie K. Pell, *The Criminalization of Abortion and Surveillance of Women in a Post-Dobbs World*, THE BROOKINGS INSTITUTION (Apr. 18, 2024), https://www.brookings.edu/articles/the-criminalization-of-abortion-and-surveillance-of-women-in-a-post-dobbs-world/#:~:text=Florida's%20six%2Dweek%20ban%20features,surveillance%20technologies%20at%20their%20disposal.

[4] *See* René Kladzyk, *Policing Gender: How Surveillance Tech Aids Enforcement of Anti-Trans Laws*, PROJECT ON GOVERNMENT OVERSIGHT (June 28, 2023), https://www.pogo.org/investigations/policing-gender-how-surveillance-tech-aids-enforcement-of-anti-trans-laws.

[5] *See* General Business Law § 394-f. The provision was enacted as part of the FY2024 Health and Mental Hygiene (HMH) Article VII legislation (A.8807-A/S.8307-A).

from third parties and imposed warrant requirements for law enforcement agencies to access any healthcare information.

Since its passage, however, gaps and shortcomings in HMH Part U's protections have become clear. The law only applies to actors in New York; it does not reach out-of-state entities with information pertaining to New Yorkers or information generated in New York. For example, if a Texas law enforcement official serves a subpoena on Uber at a location within Texas for health information that was generated in New York, HMH Part U cannot prevent Uber's compliance.

III. THE NEW YORK HEALTH INFORMATION PRIVACY ACT

NYHIPA would build on the protections set forth in HMH Part U by giving New Yorkers more control over their health data and limiting the instances in which companies can process covered healthcare information.

A. What NYHIPA Covers

NYHIPA's reach is broad and specifically designed to patch the holes in HMH Part U, covering any entity that "(a) controls the processing of regulated health information of an individual who is a New York resident, (b) controls the processing of regulated health information of an individual who is physically present in New York while that individual is in New York, or (c) is located in New York and controls the processing of regulated health information."[6] Under this broad definition, the healthcare information of those who travel to New York to undergo a medical procedure that would be unlawful elsewhere is protected.

Likewise, the type of health data the law covers is defined broadly as any information that can be tied to an identifiable person or device and that is collected or processed in relation to a person's medical or mental healthcare. The legislation explicitly defines payment or location information related to an individual's medical and mental healthcare, including any inferences one can draw from such information, as regulated data under the act. This definition is much broader than that of protected health information under HIPPA.

B. What NYHIPA Does

NYHIPA closes many of the gaps left open under HMH Part U. Among its provisions, the legislation puts strict limitations on whether and when an entity can process[7] health information. Other than when an individual provides valid consent—for which the law sets out robust requirements—covered entities can only use private health data when doing so is strictly necessary to perform a list of seven activities. These include protecting against malicious, fraudulent, or illegal activity and responding to or preventing security incidents. While "internal business operations" is one of the permitted uses of private health data, the legislation specifically excludes

[6] A.2141 / S.929 (2025), https://www.nysenate.gov/legislation/bills/2025/S929.

[7] The legislation uses the terms "process" or "processing," which are again defined broadly as any "operation or set of operations performed on regulated health information, including but not limited to the collection, use, access, sharing, sale, monetization, analysis, retention, creation, generation, derivation, recording, organization, structuring, storage, disclosure, transmission, disposal, licensing, destruction, deletion, modification, or deidentification of regulated health information." *Id*.

"any activities related to marketing, advertising, research and development, or providing products or services to third parties."[8]

This would significantly reduce the amount of private health information companies collect in the first instance. Thus, even if an official from a hostile state compelled a company to produce health information generated in or pertaining to New York, there would simply be less that company could turn over.

NYHIPA also addresses the risk that extraterritorial legal process could be used to access private health data by giving individuals more control over their own health information. The law would create a default expectation that regulated entities destroy an individual's covered health information within 60 days,[9] unless that person requests that it be preserved for longer. The law also grants individual rights of access and deletion to health information in the possession of regulated entities. Under NYHIPA, people can access what information has been collected about them and demand that it be deleted within 30 days. A hostile state actor cannot obtain what no longer exists.

C. CONCLUSION

As explained above, people receiving medical care in New York are currently vulnerable, as out-of-state entities can access their sensitive information. Both chambers of the legislature have already passed NYHIPA. For the foregoing reasons, the Civil Rights Committee urge Governor Hochul to sign the New York Health Information Privacy Act as swiftly as possible.

Civil Rights Committee
Evan Henley, Co-Chair

December 2025

Contact
Elizabeth Kocienda, Director of Advocacy | 212.382.4788 | ekocienda@nycbar.org
Mary Margulis-Ohnuma, Senior Policy Counsel | 212.382.6767 | mmargulis-ohnuma@nycbar.org

[8] *Id.*

[9] NYHIPA exempts protected health information in the possession of HIPAA-covered entities from the 60-day deletion requirement. Such entities would still be required to retain protected health information for at least six years.