AN A.S. PRATT PUBLICATION
JUNE 2025
VOL. 11 NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 11 **NUMBER 5** **June 2025**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2025–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, the editor(s), RELX, LexisNexis, Matthew Bender & Co., Inc, or any of its or their respective affiliates.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Will New York Be Next to Regulate Specifically Personal Health Information to Further, and Possibly Re-Write, a New Paradigm of State-Level Health Data Regulation?

By Scott T. Lashway, Matthew MK Stein, Cassandra L. Paolillo and Kayla LaRosa*

In this article, the authors compare the New York legislature's version of Washington's My Health Data Act to the Washington law.

The New York legislature has passed its version[1] of Washington's My Health My Data Act (WA MHMDA). Currently awaiting action by Governor Kathy Hochul, the New York Health Information Privacy Act (NY HIPA) would regulate personal health information not covered by HIPAA. If enacted, NY HIPA would take effect one year after it becomes law.

PRACTICAL CONSIDERATIONS

NY HIPA would impose significant restrictions on entities handling personal health data that is not regulated by HIPAA as "protected health information." Under the bill, a regulated entity could process or sell regulated health information only if it had a complaint authorization or if strictly necessary (as provided below) to achieve at least one of seven enumerated purposes. For valid authorization under NY HIPA, authorization must, among other things, be made (i) "separate[] from any other transaction," and (ii) "24 hours after an individual creates an account or thirst uses the requested produce or service." The bill's requirements for what constitutes authorization and how one can obtain it is complicated, to say the least. Otherwise, under the bill, the sale or processing of the data is "unlawful."

In brief, the intent behind both NY HIPA and Washington's law appears to be similar – to close the gap between widely-thought consumer expectations about the privacy protections provided by HIPAA and the actual outdated legal framework – but, NY HIPA's potential execution will be different. Indeed, in the absence of a broader federal law, it could set a new paradigm for state-level data regulation given New York's significance in regulating business.

---

* The authors, attorneys with Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C., may be contacted at slashway@mintz.com, mstein@mintz.com, clpaolillo@mintz.com and klarosa@mintz.com, respectively.

[1] https://legislation.nysenate.gov/pdf/bills/2025/s929.

Additionally, given the proposed law's breadth, its implications for the use of regulated data with emerging technology uses such as AI – whether in adtech, healthcare, or elsewhere – could be significant.

This article is a summary comparison between the currently passed NY HIPA and WA MHMDA.

WHAT DATA IS OR WOULD BE REGULATED?

Like other laws regulating data, WA MHMDA and NY HIPA (as enacted) regulate how and when certain types of data may be collected, used, or disclosed. Neither law regulates all data, and while both seek to regulate personal health information that is not covered by HIPAA, the Washington and New York legislatures use different definitions to define the type of data regulated under each: "consumer health information" in Washington, and "regulated health information" in New York. The definitions of regulated data provide the answer.

In NY HIPA, "regulated health information" is defined 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 refers to "individual[s]," without limiting that to New York residents, and if the information is about an unknown individual but linkable to a known device, then it is potentially within scope.

In contrast, in the WA MHMDA, "consumer health information" is defined as "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present, or future physical or mental health status." WA MYMDA defines "consumer" as (a) "a natural person who is a Washington resident; or (b) a natural person whose consumer health data is collected in Washington," and excludes "individual[s] acting in an employment context."

In other words, if person does not reside in Washington and their data is not collected in Washington, or if they are acting in an employment context, their data is definitionally not "consumer health information," and therefore not regulated by WA MHMDA. The legislative reports accompanying the WA MHMDA[2] as well as the Washington Attorney General's FAQs[3] about it do not explain what "collected in Washington" means, however. ("Collect" is defined; "in Washington" is not.) It is unknown currently if someone outside of Washington, whose data is collected on a cloud server in Washington, is a covered "consumer" for purposes of the WA MHMDA. But to be a consumer, and therefore to have their personal health information qualify as consumer health information, the person must have some nexus to Washington, even if the nexus is limited to where their data is collected. (WA MHMDA defines personal information as "include[ing], but is not limited to, data associated with a persistent

[2] https://app.leg.wa.gov/bi/tld/documentsearchresults?biennium=2023-24&name=1155&documentType=1.

[3] https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy.

unique identifier, such as a cookie ID, an IP address, a device identifier, or any other form of persistent unique identifier.")

So, data linkable to a device, but not a person, may still be consumer health information under WA MHMDA. In addition, note that NY HIPA does not contain language excluding individuals acting in an employment context. This point surely will be litigated and decided by the courts.

Both laws cover derived or inferential information, and both laws would cover some degree of location information. For Washington, it is location information "that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies." For NY HIPA, it is location information related "to an individual's physical or mental health."

Although NY HIPA potentially has broader scope based upon the clear ability to link to a device, not a person – as noted, the WA MHMDA definitions are ambiguous on this point – and the lack of a nexus requirement between the individual the data relates to and that state, the courts will need to determine whether one is broader than the other: "in connection with the physical or mental health of an individual" (NY HIPA) or "identifies the consumer's past, present, or future physical or mental health status" (WA MHMDA).

NY HIPA also provides limited data-level exemptions for data regulated by HIPAA and the Federal Policy for the Protection of Human Subjects (the Common Rule). WA MHMDA has those data-level exceptions, and several others.

WHO IS OR WOULD BE REGULATED?

Neither law is straightforward as to the scope of regulated entities (the term used by both laws to describe entities subject to the law), so organizations with a nexus to New York will need to pay attention if NY HIPA becomes law. NY HIPA would apply to any entity that that satisfies any of these three requirements:

- Controls the processing of Regulated Health Information of New York residents,
- Controls the processing of Regulated Health Information of individuals physically present in New York while that person is in New York, or
- Is located in New York.

In contrast, Washington's law applies to entities that (a) "conduct[] business in Washington" or "target[] . . . consumers in Washington" and (b) "determine[] the purpose and means of collecting, processing, sharing, or selling of consumer health data."

NY HIPA appears to be more expansive than Washington's law, and being subject to the law would likely have greater consequences. While Washington is expansive because

entities that do not conduct business in Washington but otherwise target Washington residents can be subject, compliance for those entities is limited to information about individuals with a nexus to Washington based upon WA MHMDA's definitions of consumer and consumer health information discussed above. (And its reliance on "conducting business" and "targeting" implies that the subject entity intends its connection to Washington.)

The definition in NY HIPA is a study in contrasts. It would apply to entities "located in New York," but what that means is not defined. A sales or satellite office or even a single remote worker in New York state might be sufficient to mean "located," but that requires a deeper dive into New York law. An entity that is not "located" in New York and has no known connection to New York might take on compliance obligations if it unknowingly has regulated health information about a New York resident. And once an entity becomes subject to NY HIPA, NY HIPA appears to apply to regulated health information about any individual, even those with no connection to New York. (As a practical matter, New York is the fourth most populous state, so an obligation to comply with New York law may have the operational consequence of extending the bill's "authorization obligation" to residents of other states, even if not legally required to do so. This will have to be considered further given its significance from a compliance and legal risk or litigation perspective.)

ENFORCEMENT

Both the NY HIPA and WA MHMDA permit enforcement through the respective state's attorney general. However, the WA MHMDA arguably has an implied private right of action, according to those writing about the statute elsewhere, whereas NY HIPA is silent. (To be clear, WA MHMDA refers to a violation as a violation of Washington's consumer protection act, which suggests a private right of action. This will be tested in the courts.) Given the NY HIPA's broad definitions of "regulated health information" and its apparent application to businesses and individuals outside of New York, NY HIPA potentially would invite the New York attorney general to bring actions against entities from both within and outside the State of New York.

If the definitions of "regulated health information" and regulated entities are read by courts as broadly as the statutory text suggests may be possible, it seems likely that courts, for constitutional reasons or federalism concerns, may be asked to limit the New York Attorney General's reach for enforcement, providing (in a way) a limit to the breadth of the law.

PENALTIES FOR VIOLATION

NY HIPA provides for civil penalties of not more than $15,000 per violation or 20% of revenue obtained from New York consumers within the past fiscal year, whichever is greater. According to Washington's consumer protection action, WA MHMDA permits treble damages, which are capped at $25,000, and civil penalties, which are capped at $7,500 per violation.

PERMISSIBLE PROCESSING WITHOUT AUTHORIZATION

As an alternative to securing an individual's authorization (meeting certain statutory criteria), NY HIPA allows processing or sale of regulated health information if strictly necessary if you satisfy any of seven statutory purposes:

1. "Provid[e] or maintain[] a specific product or service requested by [the] individual,"
2. "Conduct[] the regulated entity's internal business operations, which excludes any activities related to marketing, advertising, research and development, or providing products or services to third parties,"
3. "Protect[] against malicious, fraudulent, or illegal activity,"
4. "Detect[], respond[] to, or prevent[] security incidents or threats,"
5. "Protect[] the vital interests of an individual,"
6. "Investigat[e], establish[], exercis[e], prepar[e] for, or defend[] legal claims," or
7. "Comply[] with the regulated entity's legal obligations."

In contrast, Washington exempts regulated entities (as defined above in section "Who is or would be regulated") when necessary to provide a requested product or service (which may be the same scope as the first strictly necessary purpose in NY HIPA), which ultimately may be broader than New York's permissible processing without authorization. WA MHMDA also states that the law does "not restrict" a regulated entity's ability "for collection, use, or disclosure of consumer health data" to the following:

- "Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any activity that is illegal under Washington state law or federal law,"
- "Preserve the integrity or security of systems" or
- "Investigate, report, or prosecute those responsible for any such action that is illegal under Washington state law or federal law."

In these situations, the WA MHMDA may provide a broader exemption in effect (although the law places the burden on the regulated entity to demonstrate the scope of the exemption).