AN A.S. PRATT PUBLICATION
JULY-AUGUST 2023
VOL. 9 NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 6** **July - August 2023**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (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

(2023–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 articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

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

Washington Transforms Consumer Health Data Landscape with Passage of My Health My Data Act

By Meghan O'Connor and Kiana Baharloo*

In this article, the authors dive into the key concepts of a new privacy law enacted in Washington, including its broad application to businesses, wide-ranging scope, significant consent requirements, and private right of action.

On April 17, the Washington legislature passed the My Health My Data Act (MHMD),[1] and Governor Jay Inslee signed MHMD into law on April 27.

This article dives into the key concepts of this watershed legislation, including its broad application to businesses, wide-ranging scope, significant consent requirements, and private right of action. MHMD is the first state legislation to offer a comprehensive privacy approach specific to consumer health data. It brings in European and California-like privacy themes as well as some new obligations not yet seen in the US privacy landscape.

The MHMD Act comes after a string of recent privacy developments, including Iowa recently becoming the sixth state to pass a comprehensive data privacy law and increased health data-related enforcement from the Federal Trade Commission.

WHAT IS THE MHMD ACT?

Introduced early in January, MHMD creates protections for personal information related to an individual's health conditions or attempts to obtain health care services. MHMD acknowledges that consumer health data is among the most personal and sensitive categories of data and that the Health Insurance Portability and Accountability Act (HIPAA) leaves a gap for health data collected by non-HIPAA covered entities, including certain apps and websites. MHMD also clarifies that the intent is to "close the gap between consumer knowledge and industry practice by providing stronger privacy protections."

* The authors, attorneys with Quarles & Brady LLP, may be contacted at meghan.oconnor@quarles.com and kiana.baharloo@quarles.com, respectively.

[1] https://lawfilesext.leg.wa.gov/biennium/2023-24/Pdf/Bills/House%20Passed%20Legislature/1155-S.PL.pdf#page=1.

BROAD SCOPE OF ENTITIES SUBJECT TO MHMD

Unlike state comprehensive privacy laws (e.g., CCPA), there is no threshold for applicability based on revenue or number of consumers whose data is processed. Instead, the MHMD Act applies to "regulated entities" broadly defined as any legal entity that:

- Conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington; and
- Alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data.

"Regulated entities" are not limited to Washington-based businesses. However, the definition specifically excludes government agencies, tribal nations, and contracted service providers when processing consumer health data on behalf of the government agency. With the exception of these entities, MHMD does not provide full entity exemptions, including no exemption for non-profit entities.

Exemptions exist for specific types of data, such as protected health information under HIPAA, certain personal information for purposes federal human subjects protections, certain limited hospital data, data governed by the Gramm-Leach-Bliley Act, and data de-identified in compliance with HIPAA. The exemptions also include data originating from and intermingled to be indistinguishable with information maintained by a HIPAA covered entity or business associate.

What should HIPAA covered entities do? If the MHMD Act is signed, health and life sciences entities will need to carefully assess applicability and the scope of exemptions.

WHAT DATA IS COVERED BY MHMD?

The MHMD Act applies to "consumer health data" which is a broader definition than one might expect. The definition includes "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" which is similar to HIPAA. However, the definition also includes a non-exhaustive list of what is considered consumer health data, including: gender-affirming care information, reproductive or sexual health information, biometric data, genetic data, use or purchase of prescribed medication, and precise location data (all of which are further defined). Consumer health data also includes any information that a regulated entity (or its processor) processes to associate or identify a consumer with consumer health data that is derived or extrapolated from non-health information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).

The definition of "consumer" is also very broadly defined as not only Washington residents but also "a natural person whose consumer health data is collected in Washington." Note that "collection" is also broadly defined to include buying, renting,

accessing, retaining, receiving, acquiring, inferring, deriving, or otherwise processing consumer health data in any manner.

Given the broad definition of "collection," coupled with the number of businesses that process and retain personal information with large technology companies in Washington, the potential scope of MHMD reaches far beyond Washington. Hopefully we will see further guidance on MHMD that will set guardrails on the scope of applicability.

WHAT OBLIGATIONS DOES MHMD CREATE?

There are a number of pertinent MHMD obligations.

Consumer Rights

The MHMD Act creates privacy rights specific for consumer health data, similar to those seen in other state comprehensive privacy laws, such as the right to access, delete, and withdraw consent from the collection, sharing, or sale of such consumer health data. However, MHMD also introduces novel rights and more extreme requirements on common consumer privacy rights.

The MHMD's right to delete is an absolute right to delete, where upon receiving a request, a regulated entity must delete the consumer's health data within 30 days of authenticating the request. A consumer can request deletion at any time, and the right requires deletion of data from all parts of the regulated entity's network, including archived or backup systems, and flow down communication to affiliates, processors, contractors, and other third parties to whom the regulated entity shared consumer health data. Health and life sciences entities have a variety of legally required retention standards, which seem to conflict with this absolute deletion right as well as operational limitations. This will be a major concern with stakeholders as we watch MHMD implementation.

Restrictions on Collection and Sharing Consumer Health Data

MHMD includes specific restrictions on collecting and sharing consumer health data. Under MHMD, regulated entities may not collect or share consumer health data except (1) with consumer consent for the specified purpose, or (2) to the extent necessary to provide a product or service required by the consumer. Consents to collect or share must be obtained separately and prior to such collection or sharing. In addition, MHMD outlines specific consent content requirements.

Consumer Health Data Privacy Policy

MHMD requires companies to have a consumer health data privacy policy that clearly and conspicuously discloses required information (in addition to currently existing requirements for website privacy policies and HIPAA notices of privacy practices).

Restriction on Sale of Consumer Health Data

Regulated entities are prohibited from selling or offering to sell consumer health data without an authorization. An authorization must be written in plain language and outline a number of requirements, including the specific consumer health data being sold, name and contact information of the seller and purchaser, and the purpose of the sale (including how the sold data will be gathered and used by the purchaser).

Prohibition on Geofencing

MHMD makes it unlawful to implement a geofence around any facility providing in-person health care services where the geofence is used to:

(1) Identify or track consumers seeking health care services;

(2) Collect consumer health data from cosnsumers; or

(3) Send notifications, messages, or advertisements to consumers related to their consumer health data or health care services.

Geofence is defined as "technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, wifi data, and/or any other form of location detection to establish a virtual boundary around a specific physical location" within 2,000 feet from the perimeter of the physical location.

ENFORCEMENT AND PRIVATE RIGHT OF ACTION

Washington has tried several times to pass comprehensive privacy legislation and the issue of enforcement and a private right of action has historically killed every such effort. MHMD is enforceable through both the Washington Attorney General's office (as a violation of the Washington Consumer Protection Act governing unfair or deceptive trade practices and unfair competition) and a private right of action (via Washington's Consumer Protection Act), which makes MHMD the first privacy legislation with a private right of action since the 2008 adoption of Illinois' Biometric Information Privacy Act (BIPA).

WHAT'S NEXT?

Given the broad definitions of "consumer health data" and "consumer" as well as the broad scope of entities that could fall under MHMD and the potential for privacy causes of action, MHMD is poised to change the landscape of collecting and processing consumer health data. It is too early to tell if this will create a new best practice, but MHMD will certainly reach a broad swath of companies and may become the next BIPA-like opportunity for extensive privacy-related litigation and enforcement.

To meet their MHMD obligations, stakeholders should:

- Maintain a consumer health data privacy policy;
- Restrict collection and sharing of consumer health data to limited purposes without consumer consent;
- Provide and respond to consumer rights regarding consumer health data;
- Implement access controls and information security safeguards;
- Put in place data processing agreements;
- Not engage in sale of consumer health data without authorization; and
- Not implement geofencing in specific circumstances.