9 November 2023

The Washington My Health My Data Act: Impacts, Challenges, & Practical Strategies

Mike Hintze
Hintze Law PLLC

Felicity Slater
Future of Privacy Forum

Privacy+ Security Forum

Speakers

Privacy+ Security Forum

Mike Hintze

Partner
Hintze Law PLLC

Felicity Slater

Policy Fellow
Future of Privacy Forum

Background & Overview

MHMDA Background

Timeline

- MHMDA first announced on October 21, 2022
- Drafted "at the request" of Washington Attorney General Bob Ferguson
- Direct response to the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization* (2022)
- Signed into law by Governor Inslee on April 27, 2023

Key Legislative Aims

- To increase legal protection for non-HIPAA-covered consumer health data
- More specifically, to create new protections for non-HIPAA-covered reproductive health data
- To protect individuals seeking care at clinics from geofencing-facilitated harassment.

--> In practice, MHMDA goes much further…

Broad scope of entities covered

Applies if an entity conducts business in Washington **or** produces or provides products or services targeted (available?) to Washington consumers

Directly applies to "regulated entities" (i.e., controllers), indirectly applies to "processors."

Applies to both commercial and non-profit entitles

Some provisions apply to all "persons," including individuals

Excludes data covered / protected by HIPAA, GLBA, FERPA, and several other statutes

- But that is a data-level exclusion, not an entity exclusion

Broad scope of data covered

Privacy+ Security Forum

a) "Consumer health data" means 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.
b) For the purposes of this definition, physical or mental health status includes, but ***is not limited to***:
   i. Individual health conditions, treatment, diseases, or diagnosis;
   ii. ***Social***, psychological, behavioral, and medical ***interventions***;
   iii. Health-related surgeries or procedures;
   iv. Use or purchase of prescribed medication;
   v. ***Bodily functions***, vital signs, symptoms, or measurements of the information described in this subsection (8)(b);
   vi. Diagnoses or diagnostic testing, treatment, or medication;
   vii. Gender-affirming care information;
   viii. Reproductive or sexual health information;
   ix. ***Biometric data***;
   x. Genetic data;
   xi. Precise location information that could ***reasonably indicate a consumer's attempt to acquire or receive health services or supplies***;
   xii. Data ***that identifies a consumer seeking health care services***; or
   xiii. Any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the data described in (b)(i) through (xii) of this subsection that is ***derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data*** by any means, including algorithms or machine learning).

"Biometric data" means data that is generated from the measurement or technological processing of an individual's physiological, biological, or ***behavioral characteristics*** and that identifies a consumer, whether individually or in combination with other data. Biometric data includes, but is not limited to … ***Imagery of the*** iris, retina, fingerprint, ***face***, hand, palm, vein patterns, and voice recordings, ***from which an identifier template can be extracted***;

"Health care services" means ***any service provided to a person to assess, measure, improve, or learn about a person's health***…

"Consumer health data" does not include personal information that is used to engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or a similar independent oversight entity that determines that the regulated entity has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

Broad scope of individuals covered

- "Consumer" means (a) a natural person who is a Washington resident; or (b) a natural person whose consumer health data is ***collected*** in Washington.
  - *Excludes an individual acting in an employment context*.
- "Collect" means to buy, rent, access, retain, receive, acquire, infer, derive, or otherwise ***process*** consumer health data in any manner.
- "Process" or "processing" means any operation or set of operations performed on consumer health data.

Overview of substantive requirements

Broad **extraterritorial** application
- Impacts non-Washington companies that have products / services available in WA
- Can apply to data about individuals outside of Washington state (for example, if the data is processed in Washington)

Opt-in (GDPR level) **consent** for any collection / use beyond what's necessary to provide a consumer-requested service

Even more burdensome "**authorization**" for a "sale" of consumer health data (including 3rd party advertising)

Notice via a separate "Consumer Health Data Privacy Policy"

Broad **access** right that includes list of 3rd parties and affiliates with which data was shared or sold

Broad **deletion** right that does not include typical exceptions (such as where retention is required by law, etc.)

Prohibition on certain uses of **geofencing**

Private right of action, in addition to Attorney General **enforcement**

Effective date of March 31, 2024, except:
June 30, 2024, for small businesses
July 22, 2023, for geofencing prohibition
Some ambiguity based on drafting issues

Compliance Challenges & Practical Strategies

Challenges of Obtaining Consent

Privacy+ Security Forum

Affirmative (opt-in) GDPR-level consent required to:

- Collect (process) or share consumer health data unless it is:
  - ***necessary*** to provide a consumer-requested product or service, or
  - for one of the ***security-related*** exempted purposes
- Process consumer health data beyond what is disclosed in a consumer health data privacy policy
  - Collect categories of consumer health data not disclosed
  - Collect, use, or share consumer health data for purposes not disclosed

Heightened "authorization" for "sale" of consumer health data which requires a written and signed authorization that:

- Includes the specific consumer health data to be sold
- Describes the purpose of the sale / use by the purchaser
- Specifies the name and contact information of the seller & purchaser
- Includes several other specified terms and disclosures
- Is valid for no more than one year
- Is revocable at any time by the consumer

(6)(a) "Consent" means a clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and unambiguous agreement, which may include written consent provided by electronic means.

(b) "Consent" may not be obtained by:

(i) A consumer's acceptance of a general or broad terms of use agreement or a similar document that contains descriptions of personal data processing along with other unrelated information;

(ii) A consumer hovering over, muting, pausing, or closing a given piece of content; or

(iii) A consumer's agreement obtained through the use of deceptive designs.

For consent to collect or share: "Consent required under this section must be obtained prior to the collection or sharing, as applicable, of any consumer health data, and the request for consent must clearly and conspicuously disclose: (a) The categories of consumer health data collected or shared; (b) the purpose of the collection or sharing of the consumer health data, including the specific ways in which it will be used; (c) the categories of entities with whom the consumer health data is shared; and (d) how the consumer can withdraw consent from future collection or sharing of the consumer's health data."

Consent for sharing must be separate from consent to collect (process).

“Share” means share (not the ad-specific definition of the CCPA) but with exclusion for processors, M&A, & extremely limited circumstances involving 3rd party with a direct consumer relationship

“Sale” is the CCPA definition. Given how onerous and non-scalable the authorization requirement is, this could be seen as, in effect, a prohibition on any (3rd party) health-related targeted advertising. Could also affect analytics, etc.

Security exception is surprisingly broad, allowing the collection, use, or disclosure of consumer health data, without consent, “to 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.”

Consent compliance strategies

- Be sure the “consumer health data privacy notice” is sufficiently broad and future-proofed to capture current and anticipated categories of data and purposes for collection, use, and disclosure
- Determine what is “necessary” to provide the consumer-requested product or service
  - Strictly necessary vs. reasonably necessary
  - What else might fall into the “security” exception?
- Investigate leveraging existing consent mechanisms (e.g., cookie consent, etc.). Are the sufficient? Or a good starting point?

Consumer rights challenges

Right to know / right of access

- Confirmation that entity is collecting, sharing, or selling consumer health data
- Access to consumer health data
- List of all third parties and affiliates with whom the entity has shared or sold the consumer health data
  - Plus an active email address or other online mechanism that the consumer may use to contact these third parties

Right to delete

- Lacks common exceptions found in other privacy laws
- Includes data archives and backups (but with longer deadline – 6 months)
- Includes a passthrough deletion requirement to all processors, affiliates, and third parties with which the consumer health data has been shared

No exception from deletion where retention is necessary to comply with law, enforce agreements, defend against claims, etc.

Consumer rights compliance strategies

- Leverage existing DSR mechanisms / processes
- Implement new processes, as needed, to track and provide details on third party and affiliate sharing
- Develop policies for resolving conflicts with deletion requests (e.g., where there are obligations to retain data)
- Ensure data can be deleted from all data locations, including backups
- Consider whether new processes are needed to receive pass-though deletion requests from entities that provided the data

Notice challenges

Privacy+ Security Forum

[Separate] “consumer health data privacy policy” containing specified disclosures, including:

- A list of the ***categories*** of consumer health data collected
- A list of the ***categories*** of *third parties* and ***specific*** *“affiliates”* with which consumer health data is shared.
- Several other disclosures that are likely already in the entity's general privacy statement

Linked from ~~the homepage~~ every page.

- For apps, from the download page (e.g., app store) & from within the app
- Must it be linked “directly” or could a link from within the general privacy statement suffice?

Privacy Policy | California Privacy Notice | Your California Privacy Choices | Washington Privacy Notice | Terms of Use | Accessibility Services

Close

By continuing to use this site, you consent to our use of technologies that analyze and monitor activity on our website, may record your activity on this site for compliance and other purposes, and sometimes provide you with tailored advertising. To learn more please visit our Privacy Policy and Terms of Use.

"Homepage" means “the introductory page of an internet website and *any internet webpage where personal information is collected*. In the case of an online service, such as a mobile application, homepage means the application's platform page or download page, and a link within the application, such as from the application configuration, "about," "information," or settings page.”

"**Affiliate**" means a legal entity that shares common branding with another legal entity and controls, is controlled by, or is under common control with another legal entity.

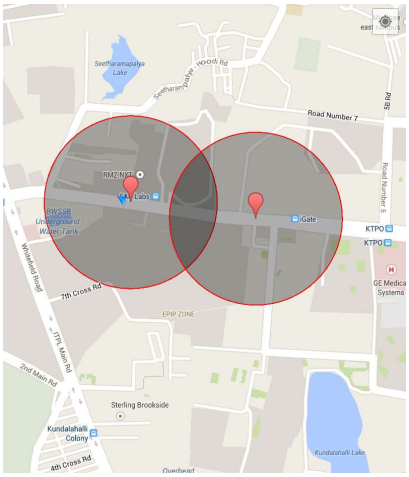
Notice compliance strategies

- Different options for the "consumer health data privacy policy"
  - Complete separate notice document
  - Separate section or, or appendix to, the general privacy statement
  - Requirements integrated throughout a general privacy statement
- Different options for the link on every page
  - Add a specific "Consumer Health Data Privacy Policy" link that points to a separate notice document
  - Add a specific "Consumer Health Data Privacy Policy" link that points directly to a separate section of the general privacy statement
  - Use existing link to the general privacy statement, but add a prominent link to the consumer health data privacy policy at the top of the privacy statement
  - Use existing link, and have the required disclosures integrated throughout the general privacy statement

Geofencing prohibition

Prohibition on geofencing around locations that provide in-person health care services where such geofence is used to:

1. identify or track consumers seeking health care services;
2. collect consumer health data from consumers; or
3. send notifications, messages, or advertisements to consumers related to their consumer health data or health care services.



Geofence prohibition is narrower than earlier version of bill, but still very broad. Recall how broad the definition of “health care services” is (including any services “to assess, measure, improve, or learn about a person's health”). So could cover any retailer with a pharmacy, or that sells running shoes, or that sells food and provides nutrition tips, etc.

“Geofence" means a virtual boundary that is 2,000 feet or less from the perimeter of the physical location.

Geofencing challenges and strategies

Privacy+ Security Forum

- Lots of gray that calls for making risk-based decisions
  - What locations are providing in-person "health care services"
  - Which geofencing scenarios fall into the three prohibited uses?
    - What data collected by a geofence is "consumer health data"?
    - Can you identify from that data whether the person is seeking health care services?
    - Do any of the uses fall into the "security" exception?
  - What is the interaction of "geofence" and "precise location information" definitions?
- Location-based, health-related tracking, profiling, and advertising may be among the riskiest activities under the Act

Consumer health data includes: "Precise location information that could ***reasonably indicate a consumer's attempt to acquire or receive health services or supplies.***"

"Precise location information" is a defined term that means location information that "directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet."

Geofence is defined as a "virtual boundary around a specific physical location, or to locate a consumer within a virtual boundary. For purposes of this definition, "geofence" means a virtual boundary that is 2,000 feet or less from the perimeter of the physical location."

The interplay between the 2,000 foot geofence boundary and the 1,750 foot radius precision in the definition of "precise location information" is open to interpretation but potentially captures a pretty large area.

Overview of compliance strategies

Privacy+ Security Forum

- Leverage existing measures already in place for GDPR, CCPA, etc.
  - Focus on what is different, additive
- Risk-based data categorization and compliance measures
- Understand the motivations and the obstacles for the enforcers
  - Washington State Attorney General
  - Private litigants / plaintiffs' attorneys
- Stay vigilant and nimble as we learn more
  - Guidance from the Office of the Attorney General
  - What others in industry are doing
  - AG enforcement actions, plaintiff claims & litigation, and court decisions

What's coming next?

Other health privacy state legislation

- **In 2023, we've seen 'My Health, My Data'-influenced health privacy bills pass into law at least three other U.S. states:**
  - New York SB 6224
    - enacted on May 3rd, 2023 (as part of Budget Bill A 3007C)
    - took effect July 2, 2023
  - Connecticut SB 3,
    - enacted on June 3rd, 2023
    - took effect October 1, 2023
  - Nevada SB 370
    - enacted on June 16th, 2023
    - will take effect on March 31, 2024

Looking forward

- **Looking ahead, a few major policy questions:**
  - Will subsequent health data privacy laws follow Nevada and Connecticut in adopting use-focused definitions of “consumer health data?”
  - Will legislators and enforcers add nuance to their treatment of health inferences?
  - Are we going to see distinctions regarding the sensitivity of different forms of health information (ex. has allergies vs. has cancer)?

Resources

- Hintze Law multi-part blog series on MHMDA https://hintzelaw.com/hintzelaw-blog/2023/4/9/wa-my-health-my-data-act-pt1-overview
- FPF Policy Brief on MHMD(A): https://fpf.org/wp-content/uploads/2023/04/FPF-Legislation-Policy-Brief_-The-Washington-My-Health-My-Data-Act-Public-Version.pdf
- Felicity Slater, FPF, "A new paradigm for consumer heath data privacy in Washington State" https://fpf.org/blog/a-new-paradigm-for-consumer-health-data-privacy-in-washington-state/
- MHMDA statute https://lawfilesext.leg.wa.gov/biennium/2023-24/Pdf/Bills/House%20Passed%20Legislature/1155-S.PL.pdf
- Office of the Attorney General FAQs https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy

Questions & Contacts

Privacy+ Security Forum

Mike Hintze

Partner
Hintze Law PLLC

mike@hintzelaw.com

Felicity Slater

Policy Fellow
Future of Privacy Forum

fslater@fpf.org