My Health My Data Act

Beyond Traditional Notions of Health Data

Agenda

1. Background: HIPAA Gap
2. Why MHMD Matters
3. What Data (and Whose) is Covered
4. Threshold
5. Obligations on Businesses
6. Consumer Rights
7. Enforcement

Background

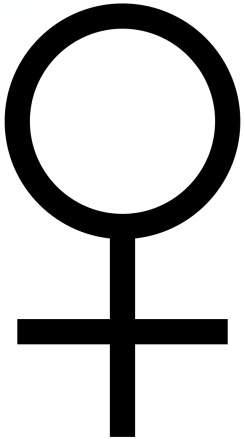
How Did We Get Here?

The HIPAA Gap

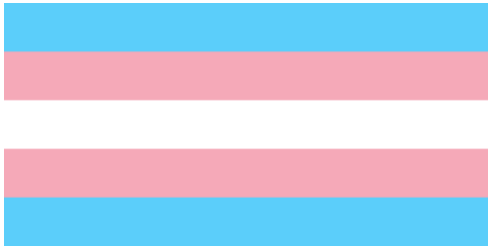
- HIPAA generally applies to “Covered Entities” and their “Business Associates”
  - Healthcare providers and their processors
- Does not include:
  - Fitbit
  - Apple Watch
  - Flo
  - Weight Watchers
  - Vitamins or supplements
- Not unprotected, but not focused on either

Reproductive and Gender-affirming Healthcare

- Reproductive or sexual health services
  - *Dobbs v. Jackson Women's Health*
  - Crisis pregnancy centers
- Gender-affirming care
  - Government actions restricting this for minors and, in some cases, adults
- Explicit inclusion in the MHMDA



Wikimedia



Wikimedia

Why It’s a Big Deal

Questions + lawsuits

Big Questions

- MHMDA goes after the entire HIPAA gap
- “Health data” defined very broadly (and vaguely)
- People without any connection to Washington
- All businesses with any health data
- Effective date: March 31, 2024
  - (Three-month reprieve for small businesses)
- No regulations
- Might end up reasonable, but…

Lawsuits Incoming

- Litigation will determine scope
- Private right of action
- Treble damages
- Businesses of any size
- Non-Washingtonians can sue

Bottom line: Getting to the answers will be messy

What does the MHMDA cover?

- The law regulates “health data” that belongs to “consumers”
  - Both terms are defined by statute
- Much of the MHMDA’s potential for overbreadth comes from how these two definitions are interpreted
  - “Health data” much broader than just details of medical treatment
  - “Consumers” not just limited to Washington residents

What is “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”
  - MHMDA provides 12 categories of data as examples
  - Exemptions for data covered by certain other laws
- Also includes information that can be used to *infer* details of an individual’s past, present, or future health
  - Potential for overbreadth arises from uncertainty around how attenuated an inference can be

Who are “Consumers”?

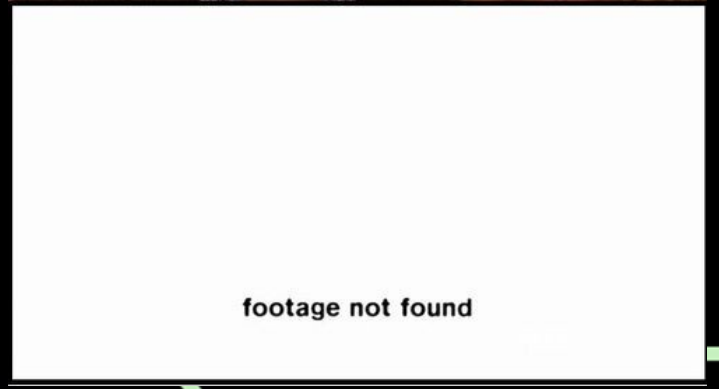
- A consumer is either:
  - A Washington resident, or
  - Any person whose “health data is collected in Washington”
- The MHMDA defines “collect” broadly to include performing any type of operation on data
  - This means any individual whose health data is stored or processed in Washington qualifies as a “consumer,” even if they have no connection to Washington at all
- Does not include individuals acting in an employment context

Compliance Obligations

Who Has to Do What?

Threshold

- Other state privacy law thresholds:
  - Lots of revenue
  - Lots of data
  - Selling lots of data
- The MHMDA does not have a threshold
- Non-profits included
- “Regulated entities” vs “small businesses”



Obligations

- Controllers (“Regulated entities”)
  - Health Data Privacy Policy (separate?)
  - Prominent link on website
  - Security / restrict access
  - Process for handling rights requests
  - Consent, consent everywhere!
- Processors
  - Contract
  - Deficiencies make you a controller

Consent: Collecting

- Affirmative act, no deceptive designs
- Needed (separately) for collection/processing, sharing, and selling
- Collection/Processing
  - (”Collection” means everything)
  - Need consent for a specific purpose OR
  - To the extent necessary to provide a product or service the consumer requested from the business
- Not *necessary* = consent is required

Consent: Sharing

- Separate from collection consent
- Share: “release, disclose, disseminate, divulge, make available, provide access to, license, or otherwise communicate orally, in writing, or by electronic or other means”
  - Broad
  - Includes sharing with affiliates
- Cookies / pixels likely covered

~~Consent~~ Valid Authorization: Selling

- Separate from collection consent AND sharing consent
- Sell: “the exchange of consumer health data for monetary or other valuable consideration”
  - Cookies / pixels too?
- Plain English signed and dated document:
  - Specific health data to be sold
  - Name and contact of who is collecting and selling
  - Name and contact of buyer
  - Purposes
  - Procedural stuff
- 1 Year Expiration (and keep it 6 years after expiration)

Consumer Rights Under the MHMDA

Consumer Rights

Access

- Consumers can:
  - Confirm whether a controller is collecting, sharing, or selling their health data;
  - Access that data; and
  - Obtain a list of entities with whom their data was shared or sold (along with contact information)

Delete

- Businesses that receive deletion requests must:
  - Delete the data from its records (including archived/backup systems); and
  - Notify all entities with whom the data was shared of the deletion request
- Unclear whether consumers can request that only some of their health data be deleted

Withdraw Consent

- Functions as an opt-out right
- Allows consumers to opt-out of collection, sharing, and sale of health data they previously consented to

But wait, there's more!

- Consumers can also appeal a business' denial of a request
- No set time frame as long as consumer appeals within a "reasonable period of time" after the consumer learns of the denial
- Not much guidance as to how businesses should handle appeals
  - Must notify consumer of final decision within 45 days of receiving the appeal
  - Must provide a written explanation of the reasoning behind the final decision
- If the appeal is denied, must provide the consumer with contact information they can use to submit a complaint to the Washington AG

Rights Requests

- Businesses must establish a method to receive requests that is “secure and reliable” and takes into account:
  - “the ways in which consumers normally interact” with the business;
  - “the need for secure and reliable communication of such requests”; and
  - “the ability of the regulated entity or the small business to authenticate the identity of the consumer making the request”
- MHMDA lays out considerations, but leaves business with latitude to decide specifics

Other Requirements

- Businesses have 45 days to respond to requests
  - Can be extended by an additional 45 days “when reasonably necessary, taking into account the complexity and the number of the consumer’s requests”
- Businesses must attempt to “authenticate” requests upon receipt
  - No set process for authentication so long as it is “reasonable”
  - If authentication fails, business is “not required to comply with the request”

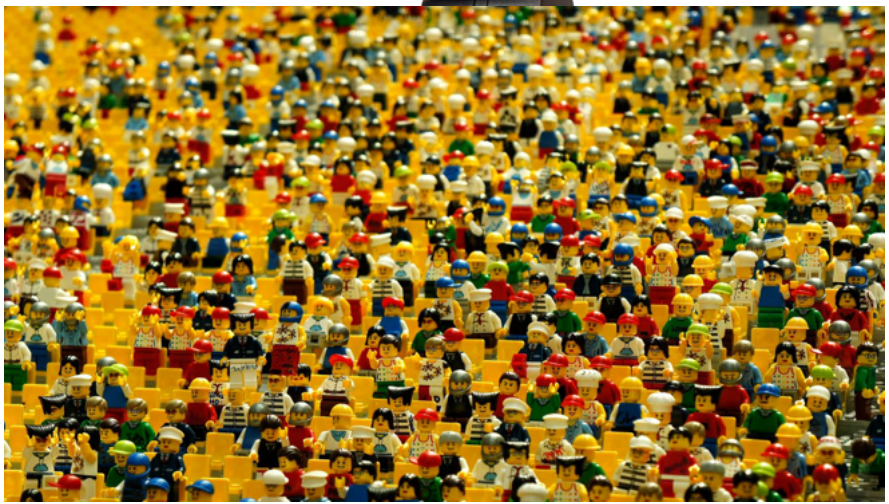
“Geofencing”

- Geofencing is using technology to “establish a virtual boundary around a specific physical location, or to locate a consumer within a virtual boundary”
- MHMDA includes a novel prohibition on “geofencing” if used to:
  - Identify or track consumers seeking health care services;
  - collect consumer health data from consumers; or
  - send notifications, messages, or advertisements to consumers related to their consumer health data or health care services

Enforcement

Enforcement

- Attorney General
  - Up to $7,500 per violation
- Private Right of Action
  - Treble damages
- Effective date(s)
  - Geofencing: July 22, 2023
  - March 31, 2024
  - Small businesses get until June 30, 2024



Key Takeaways

- Addresses the HIPAA Gap
- Broad and Vague
  - Beyond typical “health data”
  - People without connection to WA
- Consent
- Deletion Right Without (Almost) Any Exceptions
- Private Right of Action
- Questions? Litigate!

Q&A

Thank you!

Connect with us

on social media