Privacy Alert

February 2024

Washington's My Health My Data Act: Are You Ready?

Washington's My Health My Data Act (MHMDA) is set to go into effect on March 31, 2024 (June for small businesses), and the key question for businesses that interact with consumers is: Are you ready?

What's in scope?

MHMDA is different from California's Consumer Privacy Act (CCPA) and similar laws in that it is intended to broaden the types of consumers it protects, the entities it regulates, and the types of health data and related transactions that fall within its scope.

By its own description, MHMDA was enacted to bridge the gap and protect consumer health data that falls outside the scope of the Health Insurance Portability and Accountability Act (HIPAA). By closing "the gap between consumer knowledge and industry practice[, the Act will] provide stronger privacy protections" for consumer health data. MHMDA achieves this in three important ways.

First, the law defines "consumer health data" broadly to cover any "personal information that is linked or reasonably linkable to a consumer and that identifies a consumer's past, present, or future physical or mental health." This includes the following information:

- Individual health conditions, treatments, diseases or diagnoses
- Social, psychological, behavioral and medical interventions
- Health-related surgeries or procedures
- Use or purchase of prescribed medication
- Bodily functions, vital signs, symptoms or measurements of information described as health status
- Diagnoses or diagnostic testing, treatment or medication
- Gender-affirming care
- Reproductive or sexual health information
- Biometric data, including data related to a person's gait
- Genetic data
- Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies
- Data that identifies a consumer seeking health care services
- Any information that is used to associate a consumer with information about health status and that is derived or extrapolated from non-health data

What is out of scope?

The following data categories are generally considered out of scope for MHMDA:

- Protected health information (PHI) as defined under HIPAA
- Personal information governed by and collected, used, or disclosed under Gramm-Leach Bliley Act

Attorney Advertising

(GLBA), Fair Credit Reporting Act (FCRA), and Family Education Rights and Privacy Act (FERPA)

- Peer-reviewed scientific, historical or statistical research
- Employee data
- De-identified data
- Publicly available data

And while the attorney general's FAQs have clarified that simply collecting information on the purchase of toiletries does not fall within MHMDA's definition of "consumer health data," an inference drawn from those purchases could be considered consumer health data. This puts the burden on companies to understand how consumer purchase information is used.

Second, consumers protected by MHMDA include both Washington residents and individuals "whose consumer health data is collected in Washington."

Finally, "regulated entities" covered by MHMDA include out-of-state companies that are processors for companies or small businesses that are regulated by MHMDA. Unlike CCPA and similar laws, MHMDA also applies to nonprofits.

What does MHMDA require?

MHMDA has numerous requirements that differ from those of CCPA and similar U.S. state laws.

Privacy Notices. MHMDA requires regulated entities to maintain a "consumer health data privacy policy" that meets the related detailed content requirements. Under the most recent FAQs, the Washington AG clarified that the link to the MHMDA Consumer Health Privacy Policy must be a separate and distinct link on the regulated entity's homepage and may not contain additional information not required under the MHMDA. Still unclear, however, is whether the MHMDA requires a separate privacy policy for the collection and use of consumer health data or the notice itself can be embedded in an organization's broader privacy policy. Until further clarification is provided, preparing a separate policy or a separate MHMDA section in the existing policy that contains all mandatory content (as opposed to cross-referencing relevant provisions in the general privacy policy) would likely present the lowest risk.

Affirmative Consent Requirements. If you're covered by MHMDA, then you must obtain separate consent before collecting or sharing a consumer's health data. The only exception applies when collection or sharing is necessary to provide a product or service requested by the consumer. And MHMDA's definition of "consent" is a robust one, requiring "a clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and unambiguous agreement."

Other requirements include:

- **Authorization** for the sale of consumer health data that more closely resembles a HIPAA authorization
- **Contract** between the company and its processors restricting the processor to the use of consumer health data that is necessary to assist the company in providing the products or services requested by the consumer
- **Administrative, technical and physical** data security practices that satisfy reasonable standards of care within the company's industry to protect the confidentiality, integrity and accessibility of the consumer health data appropriate to the volume and nature of the consumer health data
- **Geofencing** (i.e., creating a virtual boundary that is 2,000 feet or less from the perimeter of a physical location) prohibited (since July 23, 2023) around an entity that provides in-person health care services when used to:
  - Identify or track the consumer seeking health care services
  - Collect consumer health data
  - Send notifications, messages or advertisements to consumers related to their health data or the health care services

What are consumers' rights?

Under MHMDA, consumers have the right to:

- Confirm whether the company is selling and sharing consumer health data
- Know the identities of all third parties and affiliates who receive a consumer's health data and be given an email address or other online mechanism to contact the third party

- Withdraw consent to the sharing, disclosing, processing and selling of consumer health data
- Delete consumer health data held by the company

Unlike most privacy laws around the world, the broad right to delete under MHMDA is not qualified or in any way limited by a company's legitimate need to comply with the law, legal processes or the defense of claims. This presents a novel compliance consideration.

Who can enforce MHMDA?

Under MHMDA, the Attorney General may pursue fines of up to $7,500 per violation through Washington's Consumer Protection Act. In addition, and more significant in the context of enforcement risk, MHMDA provides consumers a private right of action to seek damages for violations, creating a heightened risk for companies of defending class action litigation.

What should your company do to mitigate risk?

Consider taking the following steps to achieve compliance readiness before the upcoming deadline.

- **Identify** whether your company is collecting, using or disclosing consumer health data.
- **Identify what data is collected, used and processed** concerning your health-related products and services.
- **Determine the purposes** for using the applicable data and how and by whom the data is being processed (e.g., internal vs. vendor).
- **Differentiate between data that is necessary** to provide your products and services and the data being used that is beyond what is necessary to provide the requested health-related products or services.
- **Review and identify** whether appropriate limitations and restrictions are in the agreements with vendors that provide services and/or products that are necessary to fulfill consumers' requests.
- **Review and identify** whether appropriate limitations and restrictions exist in agreements with vendors such as third parties that are appropriate for the company's and/or vendor's use beyond the products or services requested by the consumer.
- **Implement proper limitations and restrictions into binding agreements** with all vendors that receive, access, process or create data that the company uses in providing a product and/or service that may implicate consumer health data.
- **Identify whether current notice and consent mechanisms** sufficiently comply with the requirements of MHMDA based on your assessment of the above practices.
- **Prepare and implement necessary policies and procedures** to comply with applicable MHMDA requirements that are not currently met by the company's existing privacy compliance practices and procedures, including appropriate administrative, technical and physical security practices.
- **Prepare and publish a consumer health privacy policy** and any updates to existing notices necessary to comply with MHMDA.

Related Professionals

Jessica B. Lee . . . . . jblee@loeb.com
Robyn Mohr . . . . . rmohr@loeb.com
Harry Valetk . . . . . hvaletk@loeb.com Eric
Eric Cook . . . . . ecook@loeb.com