MINTZ

My Health, My Data! Washington State Enacts Broad Health Data Privacy Protection Law

May 26, 2023 | Blog | By **Lara D. Compton**, **Kathryn F. Edgerton**, **Adam B. Korn**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

- Privacy & Cybersecurity

RELATED INDUSTRIES

Washington greatly expanded the protection for consumers' identifiable health information by enacting the "**My Health My Data Act**" (MHMDA), in an effort to close the gap between HIPAA protections and the laws protecting the privacy and security of other consumer health care data. While MHMDA resembles the California Consumer Privacy Act as amended by the California Privacy Rights Act (CCPA) and the Illinois Biometric Information Privacy Act (BIPA), it broadly applies to health information outside of traditional health care settings. Below we answer frequently asked questions about MHMDA's applicability and requirements.

1. **When Does The MHMDA Go Into Effect And Who Must Comply?**

The MHMDA goes into effect on March 31, 2024 for most regulated entities except "small businesses," which have until June 30, 2024 to comply. The MHMDA defines a small business as an entity that collects, processes, sells, or shares consumer health data of fewer than 100,000 consumers during a calendar year, or derives less than 50 percent of gross revenue from the collection, processing, selling, or sharing of consumer health data, and controls, processes, sells, or shares consumer health data of fewer than 25,000 consumers.

Under the MHMDA a "regulated entity" includes an entity that conducts "business in Washington, or produces or provides products or services that are targeted to consumers in Washington" and that determines the purpose and means of collecting, processing, sharing, or selling of consumer health data (Regulated Entity). Unlike the CCPA, there is not an exemption for nonprofit entities. Simply put, this bill will likely impact businesses that have traditionally fallen outside of HIPAA regulations, such as health tracking devices and corresponding mobile applications, grocery stores and other retailers that sell health-related supplements, and gyms, fitness studios, and other businesses that are quasi-health related.

Importantly, the MHMDA broadly **defines** what it means to "collect" data. The law specifically states that "collect" means "to buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any manner." Therefore, the MHMDA can apply broadly across industries.

2. **What Is Consumer Health Data?**

The MHMDA broadly **defines** consumer health data to include "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 can include "data associated with a persistent unique identifier, such as a cookie ID, an IP address, a device identifier, or any other form of persistent unique identifier" and specifically includes (among other things):

- gender-affirming care information;
- reproductive or sexual health information;
- biometric data (such as iris, retina, fingerprint, and voice);
- 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; and
- any information that a Regulated Entity or its respective processor processes to associate or identify a consumer with the 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).

Notably, the information protected by this law includes inferences that can be made from a consumer's information and activities. For example, in a manner similar to recent Office for Civil Rights Guidance (but with the force of law), this would include information gleaned from tracking technologies and other inferences that can be made from associating an identifier with other information in the recipient's

possession.

3. **Does The MHMDA Apply To All Identifiable Health Information?**

No. Similar to the CCPA, there are numerous information level exemptions to the law's applicability relating to protection by other laws and regulations, for example:

- protected health information subject to HIPAA and information de-identified or used and disclosed as a limited data set in accordance with HIPAA;
- personal information subject to Gramm Leach Bliley Act;
- health care information collected by health care providers or subject to privacy rules adopted by the office of the insurance commissioner;
- substance use disorder treatment information collected, used, or disclosed in accordance with 42 C.F.R. Part 2;
- identifiable research information protected by 45 C.F.R. Part 46.21 (Common Rule) or information collected as part of human subjects research pursuant to the good clinical practice guidelines issued by the international council for harmonization; and
- information originating from, intermingled with, and indistinguishable from information protected by HIPAA, RCW 70.02.010 (state health privacy), and 42 CFR Part 2.

4. **Does The MHMDA Apply To Employee Health Data?**

Unlike the CCPA, the MHMDA generally does not apply to employee information maintained by an entity in its role as an employer. The definition of consumer explicitly excludes individuals acting in an employment context.

5. **Are There Specific Security Requirements?**

Yes. Similar to HIPAA, Regulated Entities are required to establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect consumer health data, including internal enterprise-wide access controls designed to restrict access to consumer health data only to those employees, processors, or contractors that need access to further the purposes of the collection.

6. **What Requirements Apply To Vendors?**

Similar to HIPAA's business associate agreement requirement, Regulated Entities must enter into a written contract with data "processors" related to the use of consumer health data. Processors may only use and disclose data as set forth in the written contract and must assist Regulated Entities in establishing required security safeguards. Processors working outside the scope of their contracts are directly subject to the MHMDA. Additionally, a processor that receives notice of a consumer's deletion request must delete the consumer's health data from its records in accordance with the MHMDA.

7. **What Rights Do Consumers Have Under The MHMDA?**

A. *Consumer Notice:* The MHMDA requires a prominently placed link to a privacy policy on a Regulated Entity's webpage that includes:

- the categories of consumer health data collected and the purpose for which the data is collected, including how the data will be used;
- the categories of sources from which the consumer health data is collected;
- the categories of consumer health data that are shared;
- a list of the categories of third parties and specific affiliates with whom the Regulated Entity shares the consumer health data; and
- how a consumer can exercise the rights provided by the law.

B. *Consent and Authorization:* With limited exceptions, a consumer's affirmative opt-in consent is required before collecting or sharing consumer health data. "Sharing" under the MHMDA includes the disclosure of any health data to a third party ***or to a corporate affiliate***, with certain limited exceptions, such as fulfilling a consumer request. Further, a consumer can revoke consent upon request. The MHMDA makes it unlawful for any person or entity to sell consumer health data without first obtaining ***written authorization that is separate from consent obtained to collect or share consumer health data.***

C. *Access and Accounting of Disclosures:* Consumers have the right to access their consumer health data and confirm whether entities are using, disclosing, or selling health data. Consumers also have the right to know what third parties have had access to their data. Consumers are entitled to a list of all third parties and affiliates with whom an entity shared or sold the consumer health data and an active email address or other online mechanisms that the consumer may use to contact such third parties. While the concept of providing information about third-party recipients is not new, some other health information privacy laws, such as HIPAA, allow for exceptions to the general rule.

D. *Deletion:* Consumers have a broad deletion right under the MHMDA that must be pushed downstream to all service providers, contractors, third parties, and affiliates. Regulated Entities must comply with consumer deletion requests without undue delay, but in all cases within 45 days of receipt of a deletion

request. Regulated Entities may extend the response period once if reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the Regulated Entity informs the consumer of the extension within the initial 45-day response period and the reason for the extension. Further, Regulated Entities must establish a process to validate consumer identity in response to deletion requests and an appeals process for deletion request denials.

8. **Does The MHMDA Prohibit Geofencing?**

The MHMDA makes it unlawful to implement a geofence around an entity that provides in-person health care services if the geofence is used to identify or track consumers seeking health care services, collect consumer health data, or send notifications, messages, or advertisements to consumers related to their consumer health data or health care services.

9. **What Is The Potential Impact On Litigation?**

Similar to the CCPA and BIPA, the MHMDA includes a private right of action. Violations of the MHMDA are unfair and/or deceptive acts for purposes of applying Washington's existing Consumer Protection Act (CPA). As a result, consumers may seek injunctive relief and/or recover actual damages. These damages can include treble damages, capped at $25,000, as well as reasonable attorney's fees. Additionally, the MHMDA grants the Washington attorney general authority to investigate and prosecute claims under the CPA. While it is likely to take several years for the courts to interpret the MHMDA, we anticipate that the MHMDA will result in robust plaintiff litigation.

10. **What Should I Do If MHMDA Applies To My Business?**

Regulated Entities should consider the following next steps to prepare for the March 31, 2024, and June 30, 2024 (small businesses) compliance deadlines:

- confirm whether the MHMDA applies;
- perform data mapping to understand what data collected is actually subject to the MHMDA and how it flows into and out of the organization, taking into account what health information can be inferred from the data collected and shared;
- review data collection practices, terminate any impermissible geofencing, and update policies and procedures to prohibit unlawful geofencing;
- perform a security risk assessment and update policies and procedures to ensure compliance with security requirements;
- update contracts with vendors to include the MHMDA requirements;
- update data collection client/patient flows to include required consents and authorizations;
- update policies and procedures to address client/patient rights;
- evaluate operational and legal issues created by the deletion of data and consult with counsel regarding the relative risks of deletion versus denying a deletion request;
- evaluate the scope of consumer health data that will be subject to Washington's breach reporting statute and update incident response protocols, policies, and procedures accordingly; and
- train all employees regarding MHMDA compliance, preferably using a role-based approach.

Authors

Lara Compton

Kathryn F. Edgerton, Member

Katie Edgerton Professional Headshot Mintz

Kathryn F. Edgerton is a Member at Mintz and a Certified Information Privacy Professional (CIPP-US) who advises hospitals and other health-related organizations on a broad range of transactional, regulatory, and strategic issues. Her clients include physician organizations, long-term and behavioral health providers, telemedicine providers, home health providers, and medical spas.

Image not found or type unknown

Adam B. Korn