My Health My Data: Washington's Health Data Privacy Revolution

Aaron J. Burstein, Alysa Z. Hutnik

April 26, 2023

On April 27, 2023, Washington Governor Jay Inslee signed into law the My Health My Data Act (MHMD). The law has an effective date of July 23, 2023, but the deadline to comply with most of its requirements is March 31, 2024.* While the 2023 state legislative season may see the addition of four comprehensive privacy laws (Iowa, Indiana, Montana, and Tennessee), My Health My Data (HB 1155) could have the most far-reaching impact on businesses.

Although limited to "consumer health data," MHMD's actual scope is much broader than many might anticipate based on the title of the law. It imposes stringent notice, consent, and HIPAA-style authorizations to the collection, sharing, and sale of "consumer health data," a term that captures a potentially vast array of data. MHMD also creates a private right of action, allowing consumers to bring claims under Washington's Consumer Protection Act, in addition to authorizing enforcement by the state attorney general.

MHMD also fits a broader trend toward intense scrutiny of health information practices under state privacy laws, through FTC enforcement actions, and in private class actions.

This post takes a look at some of the key requirements and open questions under MHMD, and offers a few tips to help stay ahead of increasingly strict health privacy regulations.

MHMD's Broad Scope

- **"Consumers" and "Consumer Health Data."** "Consumers" under MHMD are Washington residents "in an individual or household context." MHMD expressly excludes individuals in an employment context (but not expressly in a business-to-business context).

Significantly, the definition of "consumer" also includes "a natural person whose consumer health data ***is collected in Washington***." "Collection," in turn, includes inferring, deriving, buying, acquiring, "***or otherwise process[ing]***" consumer health data. Similar to the CCPA, GDPR, and other privacy laws, MHMD defines "processing" to include "any operation or set of operations performed on consumer health data." This provision makes the definitions of "consumer" and "consumer health data" circular, and it raises the question of whether MHMD applies to health data about individuals who reside outside of Washington. The final Senate report summarizes member comments suggesting that the intent of this definition is to cover non-residents who travel to Washington to obtain health care. The MHMD text, however, is not clearly limited to this circumstance.

Irrespective of whether "consumers" are limited to a Washington resident, MHMD's definition of

"consumer health data" is expansive. It includes any information, ***including inferences***, that is reasonably linkable to a consumer or household and that "identifies the consumer's past, present, or future physical or mental health status." Examples of health status include data types that are widely regarded as sensitive, such as genetic data and reproductive or sexual health information.

Other examples, however, sweep in a much broader array of data. MDMH opponents asserted that "overly broad definitions" of "consumer health data" would cover "the purchase of everyday consumer products like toilet paper, deodorant, and even shoes." It remains to be seen whether MDMH is interpreted this broadly, but the law expands on terms defined in existing laws and includes broad categories of data without regard to data sensitivity. Examples include:

- Biometric data. MDMH's definition of "biometric data" does not expressly exclude photographs, nor does it require information to be used to identify an individual. This is in contrast to definitions under the Illinois Biometric Information Privacy Act and Washington's own biometric privacy law.
- "Use or purchase of prescribed medication." MDMH does not distinguish between medications based on their sensitivity. Common antibiotics that could be used to treat a wide range of infections are subject to the same requirements as drugs that are prescribed for a specific condition.
- ,"Bodily functions, vital signs, symptoms, or measurements" of health status. These terms could capture fitness tracker and health app data.
- "Seeking health care services." Again, MDMH does not draw distinctions based on the sensitivity of services. For instance, an advertising platform would have to treat a consumer's interest in visiting a dental office with the same level of sensitivity as seeking treatment from a fertility clinic."
- **Regulated Entities.** A "regulated entity" is defined as a legal entity that (1) does business in Washington and (2) determines the "purpose and means of collecting, processing, sharing, or selling consumer health data." Certain regulated entities are "small businesses" if they (1) process consumer health data of fewer than 100,000 consumers during a calendar year, or (2) derive less than 50 percent of their revenue from processing consumer health data and process consumer health data of fewer than 25,000 consumers. Small businesses must comply with MHMD by June 30, 2024, but their compliance obligations are otherwise the same as those of regulated entities.
- **Processors.** A "processor" under MHMD processes consumer health data "on behalf of" a regulated entity. A processor and regulated entity must have a written contract in place that, among other things, provides "binding instructions" for processing consumer health data. A processor becomes a regulated entity to the extent that it violates any of the regulated entity's instructions.

Regulated Entities' Obligations

MHMD provides a set of comprehensive individual rights over consumer health data. The bill also distinguishes between "sharing" and "selling" data but does not track the CCPA's definition of "sharing."

- **Notice and Consent for "Collection" and "Sharing."** MHMD requires regulated entities to obtain opt-in consent before (1) "collecting" or (2) "sharing" consumer health data. "Sharing"

includes most disclosures of consumer health data, except disclosures to a processor or to a third party that has a direct relationship with the consumer. The final Senate report indicates that separate consents are required for collection and sharing.

MHMD consents must disclose the categories of consumer health data to be collected or shared, the specific purpose of collection of sharing, the categories of entities with which consumer health data will be shared, and how consumers can withdraw consent from future collection or sharing. Similar information must appear in the notices that regulated entities must post to describe their consumer health data practices. (MHMD does not specify whether a regulated entity may provide this information as part of its general privacy notice.)

- **Authorization to "Sell" Consumer Health Data.** To "sell" consumer health data – defined as exchanging such data for "monetary or other valuable consideration" – a regulated entity must obtain an ***authorization*** from the consumer. Similar to HIPAA authorizations, MHMD authorizations must specify the consumer health data to be sold, identify the buyer, and describe the purpose of the sale, in addition to providing other information. Authorizations are valid for one year at most and are revocable by consumers at any time.

- **Consumer Rights.** MHMD provides consumers with the rights to confirm processing, delete, and withdraw consent for the collection and sharing of consumer health data. Regulated entities are required to send deletion requests to affiliates, processors, and third parties that received the consumer's health data. The narrow exceptions to these rights include a six-month delay to delete consumer health data in backup or archive systems and declining requests that are "manifestly unfounded, excessive, or repetitive." On the other hand, MHMD does not contain a provision akin to CCPA section 1798.192, which prohibits contract terms that "purport[] to waive or limit in any way rights under this title, including, but not limited to, any right to a remedy or means of enforcement, . . ." Contractually limiting the exercise of consumer rights or remedies, such as through the private right of action, may be a possibility.

- **Ban on Geofencing.** Finally, MHMD broadly prohibits regulated entities from using a geofence to identify consumers, collect consumer health data, or send ads or notifications based a consumer's proximity to in-person health care services facilities for certain purposes. Specifically, regulated entities would be prohibited from using consumer location of less than 2000 feet – a little more than one-third of a mile – for any of these purposes.

Exemptions

- MHMD exempts several ***types*** of personal data. Notably, MHMD does not apply to protected health information (PHI) that is subject to the HIPAA Privacy Rule or "health care information" that is handled "in accordance with" Washington's existing health privacy law (chapter 70.02 RCW). Other carve-outs include data that is processed "pursuant to" the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, and FERPA, among other federal and state statutes.

Preparing for MHMD – and Beyond

If MHMD becomes law, it will leave regulated entities with less than one year to prepare for compliance. At the same time, MHMD is part of a broader, accelerating trend toward treating health data as a particularly sensitive category of personal data. These trends suggest short-term and long-term priorities.

In the short term, regulated entities should ask:

- **Have you identified all instances in which you collect, share, or sell consumer health data?** Because MHMD's definitions of these terms differ from those in other state privacy laws, companies may want to review whether their assessments of "sensitive" health-related information require revision under MHMD's more expansive definitions. The same holds true for "sale" and "shares" of consumer health data. For example, this might include reexamining if there is a material distinction between certain wellness products versus health products under the bill. It is also worth taking a close look at your digital advertising practices and whether there is risk that consumer health data is collected, shared, or sold without required consent (or authorization) – a step that recent FTC enforcement actions also suggest, as we discussed in connection with the *BetterHelp* case.

- **How can you build on existing processes for honoring consumer requests?** Companies that have taken a state-by-state approach to state privacy compliance may need to expand rights to Washington residents. In addition, companies may want to assess whether exceptions they use to manage deletion and other consumer requests align with MHMD's narrow exceptions.

- **Do our current notice and consent practices meet MHMD's detailed, prescriptive disclosure requirements?** MDMH's disclosure and consent are extensive and specific. Notices must describe the categories of consumer health data that regulated entities collect, the categories of their sources, the categories they share, a list of the categories of third parties and specific affiliates with which they share consumer health data, and instructions on exercising consumer rights under MHMD. Consents must disclose the categories of consumer health data to be collected or shared, the specific purpose of collection or sharing, the categories of entities with which consumer health data will be shared, and how consumers can withdraw consent from future collection or sharing.

MHMD also shines a bright light on the long-term trend toward stricter health data privacy regulation. The relatively short compliance deadline in MHMD illustrates that companies may have little time to adjust to how they collect and disclose personal information for advertising and other purposes. Building on MHMD compliance steps toward longer-term management of health data identification and management processes could be a step in this direction.

* The deadline to comply with most MHMD obligations, including the notice, consent, and authorization requirements, is March 31, 2024. The primary exception is the prohibition on geofencing in section 10 of the law. Because MHMD does not specify an effective date for this provision, the July 23, 2023 effective date applies. The placement of the effective date in other MHMD obligations could give rise to arguments that the deadline to comply with parts of those obligations is not delayed, which may factor into some companies' risk mitigation strategy. Notably, the AG enforcement and private right of action are also effective on July 23, 2023.