Articles + Publications | May 2, 2023

Washington Legislature Goes Big With “My Health My Data Act

WRITTEN BY

James Koenig | Ronald Raether, Jr. | Angelo A. Stio, III | Brent T. Hoard | Molly S. DiRago | Tricia M. Brauer | Laura Hamady | Robyn W. Lin

On April 27, the state of Washington enacted the My Health My Data Act (MHMDA), a comprehensive health privacy law that imposes broad restrictions on how “consumer health data” can be used by companies doing business in the state of Washington or engaging with Washington residents. Notably, the MHMDA requires opt-in consent for any collection, use, or disclosure of consumer health data not strictly necessary to provide a service or good requested by the consumer and includes a consumer private right of action for alleged noncompliance.

After drafting but repeatedly failing to pass a comprehensive privacy law in 2019, the MHMDA — adopted partially in response to the Supreme Court’s decision in *Dobbs v. Jackson Women’s Health Organization* to address concerns about the safety and privacy of individuals who seek access to reproductive health care or gender affirming services — now establishes a novel and expansive privacy legislation, imposing a suite of new and uncertain compliance obligations on many organizations.

Some of the MHMDA’s key definitions and requirements include:

Key Definitions

- ***Regulated Entities*:** Many types of organizations, including small businesses and nonprofits may be covered by the MHMDA.

- ***Consumers*:** The MHMDA explicitly protects Washington residents and extends to protect any consumer health data “collected” in the state of Washington. Given that the MHMDA explicitly states that it includes persons identified through “unique identifiers,” it is unclear how organizations could be confident in excluding data other than their employee and business-to-business data (*i.e.*, the MHMDA excludes data from an “individual acting in an employment context”). Additionally, the defined term “collect” contains an expansive catchall to include “otherwise process[ing] consumer health data in any manner” within the definition. Thus, the MHMDA could be read to apply to a consumer anywhere in the world if a company collects (*i.e.,* processes) that consumer’s consumer health data in Washington. (Note: Washington is home to two of the world’s largest cloud hosting platforms, Microsoft and Amazon.).

- ***Data*:** While purportedly designed to protect health data not covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the MHMDA’s definition of consumer health data applies broadly to “*personal information that is linked or could reasonably be linked to a consumer’s past, present, or future physical or mental health status*.” Notably, the MHMDA’s definition of personal information explicitly includes

Cookie-IDs, appearing to leverage recent Federal Trade Commission (FTC) enforcement actions and the Office for Civil Rights' (OCR) bulletin that we analyzed in our recent alert "Cookies and Online Tracking of Health Signals – An OCR Prescription for Potential Peril."

Key Requirements

- ***Private Right of Action*:** In addition to attorney general enforcement power, the MHMDA provides for a private right of action under the Washington Consumer Protection Act, which, among other things, enables consumers to pursue litigation for declaratory relief, injunctive relief, and damages of the lesser of $25,000 or three times the actual damages sustained, along with attorneys' fees and costs.

- ***Disclosures*:** The MHMDA seems to require regulated entities to develop bespoke privacy disclosures in a "consumer health data privacy policy" that may be redundant or inconsistent with existing notice regimes. If these disclosures must be separately displayed, consumers must then navigate through an increasingly confusing and disconnected series of online notices and website links.

- ***Opt-In Consent*:** The MHMDA prohibits organizations from collecting consumer health data beyond what is minimally necessary to provide requested services unless it first obtains specific consent.

- ***Authorization to Sell*:** Separately, the MHMDA outlaws selling or offering to sell consumer health data without a signed form of authorization containing a series of diligence-heavy disclosures proscribed by the MHMDA.[1] Such authorization would only be valid for one (1) year and could be revokable at any time. A company must also retain authorizations for six (6) years.

- ***Expanded Data Subject Rights*:** The MHMDA provides new variations of individual privacy rights — including a right of access that mandates companies to share a list of all third parties and affiliates with whom the consumers data has been shared, together with contact information for such organizations, as well as a right of deletion with no exceptions. The right of deletion extends to all downstream third parties and even backups/archived data (within six (6) months of the request). In both cases, the deletion process will, at best, be challenging and costly to execute. Interestingly, given the detailed information included in an authorization (*i.e.*, consumer's signature, specific health data, etc.), the authorization itself would seem to fall within the scope of a record that must be deleted — and yet authorization must be maintained for six (6) years — creating a potentially unavoidable violation (and claim).

- ***Limitation on Geofencing*:** The MHMDA also prohibits using a geofence to locate a consumer around any facility that provides in-person health care services if the geofence collects consumer health data; identifies or tracks consumers seeking health care services; or sends notifications, messages, or advertisements to consumers related to either their consumer health data or health care services. Given the breadth of the definitions in the MHMDA, it is not clear that either consumers or regulated entities may anticipate when geofences may or may not be applied, or how to practically address this prohibition since obtaining consumer consent in this case is not permitted.

Common Compliance Elements and Exclusions: The MHMDA seems to leverage some requirements that are common with existing privacy laws — such as baseline data security requirements. It also appears that the MHMDA's contractual requirements between regulated entities and processors could be consistent with the terms of many organizations' existing data protection clauses drafted to comply with the CCPA and other privacy laws, perhaps with minor adjustments. The MHMDA also excludes data regulated by various federal laws (FCRA, FERPA, GLBA, and HIPAA), some publicly available data (although the definition of "publicly available" is open to interpretation[2]), certain data used for research in the public interest, and de-identified data (but with additional nonstandard requirements).

Effective Date: Regulated entities must comply by March 31, 2024, and small businesses must comply by June 30, 2024. However, due to imprecise drafting, certain MHMDA requirements (such as geofencing) could arguably to go into effect within months.

Four Practical Steps You Can Take to Prepare: Given the broad applicability of the MHMDA, organizations may consider taking the following four steps to prepare for compliance:

1. **Evaluate data and data flows.** Evaluate or prepare data inventories and flows to determine if any of your organization's personal information is "consumer health data" covered by the MHMDA.

2. **Assess operational and compliance needs.** If an organization is processing "consumer health data" as defined by the MHMDA, assess what operational and compliance changes may be required (and when).

3. **Make a plan.** Based on the above steps, prepare a list of action items and a roadmap (with budget/resource needs) for required compliance activities.

4. **Analyze marketing practices.** Think about your organization's use of mobile and online advertising. Given the broad definitions of consumer health data, sharing, and "sales" under the MHMDA (which, like CCPA, could include most types online third-party advertising), regulated entities may be required to obtain consent and/or consumer authorizations to maintain current marketing practices.

---

[1] For example, the authorizations need to include, among other things, the specific consumer health data concerning the consumer that the person intends to sell, contact information about the purchaser, their contact information, how they will use the consumer health data, and the consumer's signature.

[2] As defined in the statute, "publicly available" means information that "(a) is lawfully made available through federal, state, or municipal government records or widely distributed media, **and** (b) a regulated entity or a small business has a reasonable basis to believe a consumer has lawfully made available to the general public."

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber