GUNDERSON DETTMER

Data Privacy Insight: Broad-sweeping Privacy Law Takes Effect in Washington

Insights
April 3, 2024

On March 31, 2024, the Washington My Health My Data Act ("MHMDA") took effect, ushering in one of the most significant and far-reaching privacy laws in the United States to date. While primarily designed to protect health data not covered by HIPAA, the law's broad scope captures a surprising range of companies and types of data—and not just those related to health care services. And, significantly, MHMDA exposes regulated entities to potential class actions, since unlike most U.S. state privacy laws, it is enforceable by consumers through a private right of action. From supplement manufacturers to health-tech companies to athletic gear providers to grocery stores and more, the impact of this law on a variety of industries and the way they process consumer health data, including for marketing, is significant. Below is a summary of the scope of the law, key requirements, how the law can be enforced, and what regulated entities can do now to mitigate risks.

Key Takeaways:

- **MHMDA is now in effect for most regulated entities.** The MHMDA took effect on **March 31, 2024** for "regulated entities" doing business in Washington or producing products or services targeted to Washington residents. If you are a "small business,"[1] you will need to comply with MHMDA by **June 30, 2024**.
- **MHMDA protects more data than most expect.** MHMDA applies to "consumer health data," which is personal information that is linked or reasonably linkable to a Washington consumer and that identifies such consumer's past, present, or future physical or mental health status. This broad language captures data related to health, wellness, nutrition, fitness, social and behavioral interventions, and other

indicators. Categories of data explicitly included are: *precise geolocation,* if it shows a consumer getting health services or supplies; *bodily functions*, which includes information related to a consumer's digestion or perspiration (included as an example in the Washington Office of Attorney General ("OAG") FAQs); data that identifies a consumer *seeking health care services*, which may be interpreted to include information about a consumer joining a gym or subscribing to meal replacement deliveries; and possibly even a photograph of a person's face.

- **MHMDA restricts how regulated entities use and share consumer health data.** The MHMDA imposes strict consent requirements on a variety of data collection and processing activities, including requiring explicit (opt-in) consent for any processing of consumer health data beyond what is necessary to provide a consumer-requested product or service. Critically, MHMDA also requires an extremely detailed and lengthy authorization that must be *signed and dated by a consumer* when a regulated entity "sells" consumer health data. "Sale" is defined similar to the CCPA, which is the exchange of consumer health data for monetary or *other valuable consideration*. These provisions, taken together, impose stringent obligations that may require regulated entities to adjust how they use and share consumer health data, including for marketing purposes.

- **Consumer rights under MHMDA are broad and include granular requirements.** For instance, the "right to access" requires regulated entities to provide consumers with a list of, and contact information for, all third parties and affiliates with or to whom the regulated entity has shared or sold consumer health data. This level of specificity is not required under other state privacy laws. The "right to delete" similarly deviates from most other state privacy laws in that it has only a limited exemption for security and fraud related purposes. In other words, a consumer's right to deletion is nearly unqualified. Regulated entities implementing processes to comply with these rights may find doing so difficult to square with their current consumer request program.

- **The MHMDA requires a separate and distinct homepage link to a Consumer Health Privacy Policy.** The OAG's FAQs make clear that a separate link is required on the regulated entities' homepage and the policy may not contain additional information not required under the MHMDA.

- **There is a private right of action.** The OAG is charged in enforcing the MHMDA. However, unlike other state privacy laws, aggrieved consumers can sue regulated entities directly for noncompliance. Although plaintiffs are required to show injury (i.e., the MHMDA does not have statutory damages), it's likely that noncompliance will be pursued aggressively by class action plaintiffs' lawyers.

If You Are a Regulated Entity, What Should You Do Now?

- Prominently post a **standalone** consumer health data privacy policy that addresses only the requirements of MHMDA on your website and in your mobile app, if any.
- **Obtain consent** consistent with the MHMDA requirements for any collection, use, disclosure, or other processing of health data beyond what is necessary to provide a consumer-requested product or service. If you are "selling" consumer health data, consider whether you can obtain prior **authorization** from the consumer.
- Modify and adjust how you **comply with consumer requests** to account for nuances under the MHMDA, including the consumer right to receive a list of all third parties and affiliates.
- Review and revise your **vendor contracts**, including any data protection agreements, with your processors and service providers. Ensure that your contracts include clauses restricting vendors from using consumer health data beyond the specific scope outlined in your contracts. Unlike other U.S. state privacy laws, the MHMDA does not permit processors and service providers to process consumer health data for their own "operational purpose(s)."

How can GD help?

If you have any questions regarding this client alert, or your company needs assistance with this topic, please reach out to your Gunderson Dettmer attorney or contact any of the following members of our data privacy group:

Anna Westfelt (650) 463-5367 awestfelt@gunder.com

Cecilia Jeong (646) 490-9094 cjeong@gunder.com

Frida Alim (415) 801-4921 falim@gunder.com

James Gately (617) 648-9313 jgately@gunder.com

Jerel Pacis Agatep (424) 214 1747 jagatep@gunder.com

---

[1] A "Small Business" is a regulated entity that either: (a) collects, processes, sells, or shares consumer health data of fewer than 100,000 consumers during a calendar year; or (b) derives less than 50% 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.

Related People

Anna C. Westfelt
PARTNER
P +1 650 463 5367

Frida Alim
ASSOCIATE
P +1 415 801 4921

Cecilia Jeong
ASSOCIATE
P +1 646 490 9094

James W. Gately
ASSOCIATE
P +1 617 648 9313

Jerel Pacis Agatep
PRACTICE INNOVATION ATTORNEY
P +1 424 214 1747

Related Services

Data Privacy

Featured Insights

FIRM NEWS

Gunderson Dettmer Commemorates 2025 Asian American and Pacific Islander Heritage (AAPI) Month

CLIENT NEWS

Brazilian Carbon Capture Company Mombak Announces $30M Financing

CLIENT NEWS

Africa B2B OmniRetail Announces $20M Financing

Africa B2B OmniRetail Announces $20M Financing

CLIENT NEWS

Glacier Announces Series A Financing to Expand Robot Recycling Fleet

CLIENT NEWS

Dataminr Announces $100M Investment Led by Fortress Investment Group

CLIENT NEWS

Omnidian Announces $87M Series C for Renewable Energy Performance

INSIGHTS

Splitting the Pie: How Savvy Founders Divide Ownership and Navigate Other Founder Equity Decisions

CLIENT NEWS

Chainguard Announces $356 Million Series D Led by Kleiner Perkins and IVP

INSIGHTS

Client Insight: California AI Transparency Act

INSIGHTS

Client Insight: Prepare for BE-10 Benchmark Survey of US Direct Investment Abroad

INSIGHTS

Tech Brew Interviews Aaron Rubin in “Where the legal battle stands around copyright and AI training”

CLIENT NEWS

Latin America Fintech Belvo Announces $15M Funding