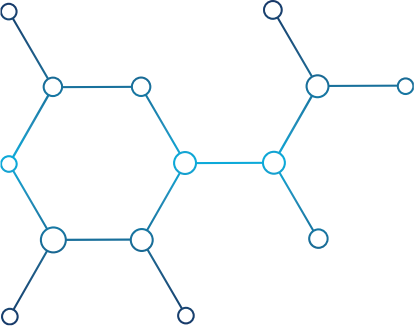
My Health
My Data
My Opt-In

Morgan Reed, President
Anna Bosch, Privacy Policy Association
Caleb Williamson, State Public Policy Counsel

ConnectedHealthInitiative



Washington state has just added a new wrinkle to the increasingly complex patchwork of state privacy laws. The My Health My Data Act (MHMD) aims to increase consumers' control of and information about their sensitive health data. MHMD is a groundbreaking and far-reaching data protection bill that will change how businesses collect, use, and disclose consumer health data. Here are some important things to know about MHMD.

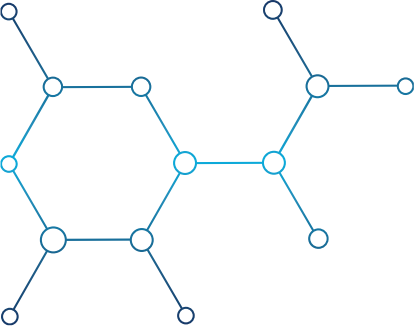
1. It is sweeping in scope

MHMD contains a far-reaching definition of "consumer health data" and applies to a broad scope of consumers and entities. MHMD broadly defines "health data" as any form of personal data gathered in Washington to "identify a consumer's past, present, or future physical or mental health status," or other attributes like their "bodily functions."

MHMD's definition of health data goes beyond specific medical conditions and diagnoses. It includes a non-exhaustive list of 13 categories of information including biometric and location data, which can be used to infer an individual's health status when associated with health or wellness products or services. Consumer products like wearable devices, websites, and apps that collect and share data on step counts, body temperature, heart rate, menstrual cycles, online health searches, and geolocation data for health-related visits would fall under the purview of the bill. Additionally, the definition of "personal information" includes cookie IDs, IP addresses, device identifiers, or any other form of "persistent unique identifiers."

When considering the expansive scope and definition of "consumer health data" within MHMD, it's crucial to acknowledge that the broad definition encompasses more than just physiological aspects related to health. It also includes non-medical factors known as **social determinants of health (SDOH)**, which significantly impact health outcomes and contribute to health equity. Some of these SDOH factors include education, food accessibility, affordable healthcare services, working conditions, and even access to broadband.

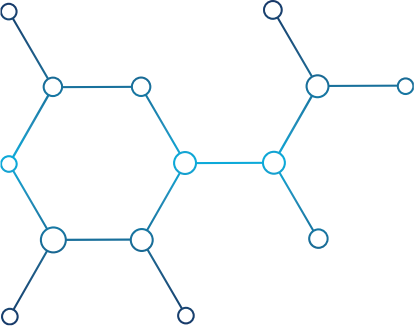
In essence, all aspects of our lives are intertwined with SDOH, and the data collected during our daily activities—whether healthcare-related or seemingly unrelated activities like grocery shopping, playing sports, working out, or visiting museums—falls under the broad definition of "consumer health data" as defined by MHMD. MHMD establishes an applicability presumption that mirrors a comprehensive privacy bill by encompassing all entities involved.



To illustrate the potential impact of this broad definition, think of a local grocery store in a rural or urban food desert—an area with only one or two grocery stores—that offers a loyalty keychain card with a barcode on the back for shoppers to gain rewards points or apply discounts. The store collects data on customers' purchase history and analyzes those purchases to award points and to alert customers about coupons or weekly deals that align with their purchase history. Under MHMD nearly every purchase you make at that store— health related or not—would be covered and regarded as "consumer health information." While the primary purpose of the grocery rewards is to enhance convenience and personalize shopping experiences, the expansive definition of health data in MHMD may require the store to comply with additional privacy obligations typically associated with more sensitive health-related data and entities. On top of that, these additional requirements could be enforced by trial attorneys through the private right of action (read on for more details on that) which adds to the potential liability and serves as even more of a disincentive to create programs consumers may want or that could benefit them.

In essence, MHMD's broad definition of health data extends its reach to various sectors and entities that are not usually subject to health privacy regulations. MHMD essentially operates as a comprehensive privacy bill and should be regarded as joining the patchwork of state privacy bills on the books (expected to hit double digits by the end of this year). This raises concerns about the practicality and potential burdens for large and small business that are outside the traditional healthcare realm but collect data that could be tangentially related to health. Striking a balance between protecting consumer privacy and avoiding undue compliance burdens on non-healthcare entities is crucial to ensure the effectiveness and fairness of MHMD.

Also sweeping is the bill's potential reach to **any** legal entity that conducts business in Washington state or targets its products or services to Washington residents. This scope means MHMD regulates healthcare providers and health plans as well as any business that provides goods or services that help consumers learn about or improve their health or collects health-related information or information that can lead to an inference about an individual's physical or mental health condition. Unlike many of the current U.S. state privacy laws, MHMD does not contain any applicability thresholds for coverage, such as revenue or volume of data collection. It also does not distinguish between businesses of different sizes or exempt those already covered by the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), or the Federal Educational Rights and Privacy Act (FERPA). Businesses subject to those laws may still need to revisit their privacy programs to ensure compliance with MHMD.



2. It requires recurring notice and opt-in consent

MHMD requires separate opt-in consent for any collection, use, disclosure/transfer, or other processing of consumer health data beyond what is necessary to provide a consumer-requested product or service. Regulated entities must explain to the consumer in clear and easy-to-understand language what they are consenting to, and entities must ensure that a consumer's consent is unambiguous, freely given, specific, and informed. For the sale of health data, MHMD requires "valid authorization" from the consumer, which is a more onerous form of consent. It requires the regulated entity to provide the specific consumer health data it wants to sell, the contact information for the person(s) collecting, selling, or purchasing the consumer health data, a one-year expiration date of the authorization, and to obtain the consumer's signature. This obligation may complicate activities ranging from traditional data sales to data analytics and targeted advertising.

MHMD also restricts geofences around a business providing in-person health services when that geofence is used to collect or track data from consumers or to send advertisements or messages related to consumer health data. This blanket prohibition means that covered businesses cannot obtain consumer consent for such activities. While on its face the bill's strict aim at true geofencing should limit the impact, the implementation is technically challenging. Specifically, the law restricts products from "…locat[ing] a consumer within a virtual boundary." A software distribution platform (like the Google Play store or the App Store) might have to create a database containing all locations in Washington that provide healthcare services, so that products would know of the "boundaries." The platforms would then have to use this database to be able to deny any requests from apps to notify a user about a deal or any other collection request that is triggered by the user's location when the user is near a health provider location. Such a mechanism would require a lot of infrastructure and force platforms to make decisions on what constitutes a "business that provides in-person healthcare services." MHMD's broad definition of "healthcare services" means these restrictions could include geofencing, for example, at gyms, multi-purpose buildings that may include healthcare offices, and general goods stores (e.g., a grocery store with a pharmacy). Another possible way to comply could be for app makers to just stop sending deals or prompting to collect information based on location altogether, including at places that do not provide in-person healthcare services, although consumers often benefit from these services.

3. It establishes a set of rights for consumers over their health data

MHMD creates several consumer rights including: the right to know how personal data is used by an organization, the right to access data, and the right to have health data be deleted. However, MHMD does not contain common exemptions for these rights that other privacy laws include (e.g., not complying with a consumer right to protect trade secrets or to comply with other legal obligations).

4. It welcomes private lawsuits

MHMD can be enforced not only by the Washington Attorney General's office but also by individuals, significantly increasing the compliance risks for companies. Since the definition of "collecting" data in MHMD includes "processing," any data that touches Washington state may be covered. For example, a cloud provider with servers in Seattle that stores health data of consumers from all over the United States potentially brings in consumers that wouldn't be covered otherwise into the private right of action, significantly increasing the size of the class.

The creation of a private right creates a presumption that the courts are the best place to sort out the ambiguities in the bill. However, sole AG enforcement is a better and more responsible way to protect consumers' rights while also eliminating or mitigating a sue-and-settle regime which has historically been used to harass small and medium-sized businesses.

5. Timeline and next steps

MHMD's geofencing provision will come into effect on July 22, 2023, 90 days after the legislature's session ends. All other requirements go into effect on March 31,2024, for regulated entities and on June 30, 2024, for small businesses. Small businesses, defined by the volume of covered data they process and total revenue, are regulated entities and must comply with all obligations of MHMD if they are covered, but they can take advantage of an extra three-month period to become compliant. The earliest any amendments or corrections to MHMD could occur would be when the Washington state legislature goes back into session in 2024. In the meantime, the state attorney general can issue interpretive guidance, but the significant opportunities for private litigation mean that courts will likely resolve the current ambiguities.

Overall, Washington state's MHMD is a significant step forward in the consumer health privacy and data protection space. With its broad scope and comprehensive provisions, MHMD aims to empower individuals with greater control over their health data. However, the act also poses challenges for businesses outside the traditional healthcare realm, highlighting the need for a balanced approach to ensure both privacy and practicality. As MHMD takes effect and court cases inevitably provide clarity, the landscape of privacy regulations continues to evolve, shaping the future of data protection in Washington and across the country.