

# The Washington State 'My Health, My Data' Act

---

## U.S. Legislation Policy Brief

April 27, 2023

*By Felicity Slater, Keir Lamont, and Tatiana Rice*



## Executive Summary

This Policy Brief summarizes and analyzes key elements of the Washington [‘My Health, My Data’ Act](#) (MHMD), which was signed into law by Governor Inslee on April 27, 2023.


The drafters of MHMD explicitly set out to protect consumer health data that is not covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. Regulators across the country have been focused on the sensitivity of, and lack of formal legal protections for, such data in the aftermath of the Supreme Court’s 2022 decision in [Dobbs v. Jackson Women’s Health Organization](#) (*Dobbs*). Furthermore, the Act aims to protect individuals seeking care at both reproductive health and gender-affirming care clinics in the state from facing harassment through messages and advertisements sent to their mobile devices using geofencing technology. MHMD is arguably the furthest reaching consumer privacy law to be enacted in a U.S. state.

While there is some uncertainty about [the Act’s effective dates](#), it appears that its data privacy provisions will take effect on March 31, 2024 (or June 30, 2024 for small businesses) and its geofencing and enforcement provisions will likely take effect on July 22, 2023.

Key elements of MHMD include:

- **Broad Definition of “Consumer Health Data:”** MHMD defines “consumer health data” broadly to encompass “physical and mental health status,” and sets out a non-exclusive list of examples of covered data that includes information categories not typically treated as health information under other legal regimes.
- **Prescriptive Consent Requirements:** Unless “necessary” to provide a consumer-requested product or service, MHMD requires independently obtained consumer consent for the “collection” and “sharing” of consumer health data and independent “valid authorization” for the “sale” of consumer health data. These forms of consent each require discrete disclosures made “prior to the collection or sharing, as applicable.”
- **Expansive Consumer Rights:** MHMD grants consumers rights to confirm whether a regulated entity is processing their health data; to access their health data; and to delete their health data across all records managed by a regulated entity. Notably, MHMD gives consumers the right to access a list of the names and contact information of third-parties and affiliates with whom their health data was “shared” or “sold.”
- **Limitations on Geofencing:** MHMD places use-based restrictions on the geofencing of “health care facilities” (defined broadly). These restrictions could impact a wide range of geofencing uses and entities.
- **Private Right of Action:** MHMD provides for enforcement through a private right of action, which sets it apart from many other state privacy laws.

## U.S. Legislation Policy Brief

This brief addresses the following elements of MHMD (the most significant observations about the bill are marked with a 

<b>1. Covered Entities</b>	<b>1</b>
<b>2. Covered Data</b>	<b>2</b>
<b>3. Consumer Choice</b>	<b>5</b>
<b>4. Consumer Rights</b>	<b>7</b>
<b>5. General Business Obligations</b>	<b>8</b>
<b>6. Regulated Entity and Processor Duties</b>	<b>9</b>
<b>7. Restrictions on Geofencing</b>	<b>10</b>
<b>8. Exemptions</b>	<b>10</b>
<b>9. Enforcement</b>	<b>12</b>

### **1. Covered Entities**

MHMD imposes obligations on “**regulated entities**” that “conduct[] business in Washington” and “produce products or services that are targeted to consumers in Washington” (Sec. 3(23)). MHMD creates blanket exemptions for three categories of organizations: government agencies, tribal nations, and “contracted service providers when processing consumer health data on behalf of a government agency” (Sec. 3(23)). MHMD’s data privacy provisions are largely intended to take effect on **March 31, 2024**.

MHMD creates a sub-category of regulated entities called “**small businesses**” that either: (a) “collect[], process[], sell[] or share[] the consumer health data of fewer than 100,000 consumers during a calendar year” or (b) derive less than 50% of their gross revenue from “the collection, processing, selling or sharing,” of consumer health data and control the consumer health data of fewer than 25,000 consumers (Sec. 3(28)). Small businesses are fully subject to MHMD; however, they typically have a delayed effective date of **June 30, 2024**.

Finally, MHMD creates rights for “**consumers**,” defined as natural persons who are “resident[s] of” Washington or whose health data is “**collected** in Washington,” and are acting only in an individual or *household* context (Sec. 3(7)). The Act excludes data arising from an employment context for its scope of coverage (Sec. 3(7)). Notably, MHMD defines “collect” to include the processing of consumer health data in “*any manner*” (emphasis added) (Sec. 3(5)).

#### **Observations:**

- **Extraterritorial Effect:** MHMD’s broad definition of “collect” covers processing data in “any manner,” which could bring many non-Washingtonian individuals within the scope



of MHMD if their covered health data is accessed in or transits through Washington State at any point.

- **Few Entity-Level Carve Outs:** MHMD will apply to numerous categories of organizations that are generally excluded from the scope of U.S. comprehensive privacy laws including small businesses, nonprofit organizations, institutions of higher education, and entities subject to the GLBA and HIPAA (though data-level carve outs exists for these laws, discussed below).
- **Narrow Carve Out for Government “Agencies”:** Unlike most U.S. comprehensive privacy laws that broadly exclude government “entities,” MHMD will only carve out government “agencies.” This may bring unexpected government and political bodies, including lawmakers and their campaign operations, into the scope of the Act.

## 2. Covered Data

MHMD regulates the “collection,” “sharing,” and “sale” of “**consumer health data**,” which is defined as “**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*.” (emphasis added) (Sec. 3(8)(a)). MHMD provides an extensive but non-exhaustive list of 13 categories of information that constitute “physical or mental health status” for purposes of the Act (MHMD defined terms noted in bold):

1. Individual health conditions, treatment, diseases, or diagnosis;
2. Social, psychological, behavioral, and medical interventions;
3. Health-related surgeries or procedures;
4. Use or purchase of prescribed medication;
5. Bodily functions, vital signs, symptoms, or measurements of information described in [this list];
6. Diagnoses or diagnostic testing, treatment, or medication;
7. **Gender-affirming care information;**
8. **Reproductive or sexual health information;**
9. **Biometric data;**<sup>1</sup>
10. **Genetic data;**

---

<sup>1</sup> “Biometric data” is “data that is generated from the measurement or technological processing of an individual’s physiological, biological, or behavioral characteristics and that identifies a consumer, whether individually or in combination with other data. Biometric data includes, but is not limited to: (a) Imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted; or (b) Keystroke patterns or rhythms and gait patterns or rhythms that contain identifying information.” (Sec. 3(22)).

11. **Precise location information**<sup>2</sup> that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies;<sup>3</sup>
12. Data that identifies a consumer seeking **health care services**; or
13. Any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the data described in [this list] that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning) (Sec. 3(8)(b)).

MHMD further defines “**personal information**” as “information that *identifies or is reasonably capable of being associated* or linked, directly or indirectly, with a particular consumer... [including but] not limited to, 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 (emphasis added) (Sec. 3(18)(a)). MHMD excludes “publicly available information” and “deidentified data” from the scope of “personal information” (Sec. 3(18)(b)).

- MHMD defines “**publicly available information**” as 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 (Sec. 3(22)).
- MHMD adopts a fairly typical definition of “**deidentified data**” rooted in the FTC’s 2012 [three part test](#) requiring that an organization (a) take reasonable measures to ensure such data cannot be associated with a consumer; (b) publicly commit to only process the data in a deidentified fashion and not attempt to reidentify it; and (c) contractually obligate any recipients of the data to satisfy these criteria (Sec. 3(10)).

### Observations:

- **Broad Scope of Consumer Health Data:** MHMD’s definition of “consumer health data” encompasses physical and mental health “status,” which is likely broader than most comprehensive state laws that create heightened protections for health “condition” and



<sup>2</sup> “Precise location information” is “information derived from technology including, but not limited to, global positioning system level latitude and longitude coordinates or other mechanisms, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet.” (Sec. 3(19)). MHMD excludes “the content of communications, or any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility” from its definition of “precise location information.” (Sec. 3(19)).

<sup>3</sup> “Health care services” are “any service[s] provided to a person to assess, measure, improve, or learn about a person’s mental or physical health, including but not limited to: (a) Individual health conditions, status, diseases, or diagnoses; (b) Social, psychological, behavioral, and medical interventions; (c) Health-related surgeries or procedures; (d) Use or purchase of medication; (e) Bodily functions, vital signs, symptoms, or measurements of information described in this subsection; (f) Diagnoses or diagnostic testing, treatment, or medication; (g) Reproductive health care services; or (h) Gender-affirming care services.” (Sec. 3(15)).

“diagnosis” information. The list of “health status” examples further expands the types of information that could be encompassed by this definition. For example, it is noteworthy that “precise geolocation data” is covered if it *could* reasonably indicate an attempt to receive health services, whether or not it is actually used for this purpose.

- **Implications for Search and Chatbots:** MHMD establishes “[d]ata that identifies a consumer seeking health care services” as a form of “health status” (Sec. 3(8)(b)(xii)). Additionally, “consumer health data” includes “gender-affirming care information” (Sec. 3(8)(vii)) and “sexual and reproductive health information” (Sec. 3(8)(viii)), terms which are both defined to include “efforts to research or obtain” such information. In an age when seeking services and research are as likely to take place online as at a library or hospital, the classification of such searches as forms of “consumer health information” could be impactful for online search engines as well as artificial intelligence-powered generative Chatbots.
- **Alignment with FTC Approach to Health Data:** MHMD’s definition of personal information includes “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.” This definition aligns with the FTC’s interpretation of what constitutes “personal data” in the health data context in its recent enforcement actions against [GoodRx](#) and [BetterHelp](#). In the complaints made as part of those enforcement actions, the agency alleged that the companies wrongfully disclosed PHI including IP address and unique advertising IDs with third parties.
- **Broad Biometric Data Definition:** MHMD’s definition of “biometric data” appears broader than any other biometric or comprehensive law and is *de facto* considered to be covered consumer health data. Unlike most biometric data privacy regimes, MHMD does not contain a carve-out for photos, videos, and voice recordings not used for identification purposes. MHMD’s definition borrows language from the CCPA that covers data that either by itself or “in combination with other data” identifies a consumer, but does not require use or intended use to “establish individual identity.” MHMD’s “biometric data” definition is also broader than the existing Washington Biometric Identifiers Law (WBIL) ([RCW 19.375.010](#)), which pertains only to “automatic measurements,” creating uncertainty about whether MHMD would have preemptive effect on the WBIL.
- **Ambiguous Definition of ‘Publicly Available Information:’** MHMD defines “publicly available information” as information that is both (a) lawfully made available through government records or “widely distributed media” and (b) that a regulated entity reasonably believes a consumer has made publicly available. While at first glance this definition appears to align with the CCPA, requiring publicly available data to satisfy both of the two prongs may be nearly impossible, as government entities, not consumers, make information in government records publicly available. If interpreted this way, MHMD could implicate significant First Amendment concerns.

### 3. Consumer Choice

#### A. Consent Requirements

MHMD requires organizations to obtain consumer “consent” in three circumstances: (1) for the “collection for a specified purpose” of consumer health data (“collection” is defined broadly to include processing data in “any manner”) (Sec. 5(1)(a)(i)-(ii)); (2) for the “sharing of consumer health data” (excluding transfers to processors and certain entities that hold a direct relationship with a consumer) (Sec. 5(1)(b)(i)-(ii));<sup>4</sup> and (3) for the “collection,” use, or “sharing” of additional categories of consumer health data or of consumer health data for *secondary purposes* (Sec. 4(3)-(4).

- **Necessity exception:** where “collection” or “sharing” of consumer health information is “*necessary to provide a product or service*” that has been “requested” by a consumer, consumer consent is not required. (Sec. 5(1)(b)). However, there is no ‘necessity’ exception for secondary uses of consumer data or the “sale” of such information. (Sec. 4(3)-(4).

MHMD defines “**consent**” as “a clear affirmative act that signifies a consumer’s *freely given, specific, informed, opt-in, voluntary, and unambiguous*” agreement to processing (Sec. 3(6)(a)). The Act specifies that certain actions do not constitute consent, including acceptances of broad terms, “hovering, muting, pausing, or closing particular content, and agreement obtained through the use of **deceptive designs**.”<sup>5</sup> (Sec. 3(6)(b)). In the consumer health data context, MHMD specifies consent “must be obtained prior to the collection or sharing...of any consumer health data” and that any “request for consent” must include various disclosures, including the categories of health data “collected” or “shared,” the “specific ways” it will be used, and how consent may be withdrawn ((Sec. 5(1)(c)(i)-(iv))). Finally, consumers have a right to “withdraw” consent for the “collection” and “sharing” of their health data, which a business must implement within 45 days (Sec. 6(2), (7)), as well as to “revoke” consent for the “sale” of their health data (Sec. 9(2)(f)).

#### B. Valid Authorization

MHMD requires a heightened form of consent called “**valid authorization**” for the “sale” of consumer health data. MHMD defines “**sale**” broadly as, “the exchange of consumer health data for monetary or *other valuable consideration*” (Sec. 3(26)(a)). Furthermore, authorization “must be

---

<sup>4</sup> “Sharing” is “to release, disclose, disseminate, divulge, make available, provide access to, license, or otherwise communicate orally, in writing, or by electronic or other means, consumer health data by a regulated entity or a small business to a third party or affiliate.” (Sec. 3(27)(a)).

<sup>5</sup> “Deceptive design” is “a user interface designed or manipulated with the effect of subverting or impairing user autonomy, decision making, or choice.” (Sec. 3(9)). For more information on restrictions on the use of deceptive design imposed by other privacy laws, see Felicity Slater, *The Future of Manipulative Design Regulation*, Future of Privacy Forum (Jan. 19, 2023), <https://fpf.org/blog/the-future-of-manipulative-design-regulation/>.

separate and distinct from the consent obtained to collect or share consumer health data” (Sec. 9(1)) and there is no ‘necessity’ exception for the “sale” of consumer health data.

MHMD requires that “valid authorization” for the “sale” of consumer health data detail the “specific” consumer health data to be sold, provide the “name and contact information” of both the seller and buyer of that health information, and describe “purpose” of the “sale,” including a description of how the buyer will use the health information, among other explanatory information (Sec. 9(2)(a)-(i)). The Act further provides that valid authorization for “sale” will expire one year from the consumer’s dated signature (Sec. 9(2)(i)). While consumers have the right to “revoke” valid authorization, a time period is not provided for an organization to comply (Sec. 9(2)(f)).

### Observations:

- **Prescriptive Consent Requirements:** MHMD requires separate consumer consent for the “collection” and “sharing” of consumer health data (unless necessary to provide a product or service to meet a consumer request), as well as “valid authorization” for the “sale” of consumer health data. Each of these forms of consent requires distinct disclosures prior to either the “collection,” “sharing,” or “sale.” Furthermore, because MHMD defines “collection” broadly to include any “process[ing] of consumer health data in any manner,” and requires consent for “such collection for a specified purpose,” the bill could be interpreted to require distinct, affirmative consumer consent for every processing activity conducted on consumer health data that is not subject to an exception.
- **“Deceptive Design” Language Differs from Comparable Laws:** Many state-level privacy laws [define](#) “deceptive design” (or “dark patterns”) as “a user interface designed or manipulated with the *substantial effect* of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation.” MHMD leaves out the “substantial effect” requirement from its definition of “deceptive design,” suggesting a lower bar than the one set by other state privacy laws for what constitutes an unlawful deceptive design feature in a consumer consent flow.
- **CCPA-Style Definition of Sale:** MHMD’s definition of “sale” is parallel to the CCPA, which has been [interpreted](#) to include a range of data transfers that may not normally be thought of as a data “sale,” including many forms of third-party online targeted advertising.



## 4. Consumer Rights

Beyond consent requirements, MHMD creates consumer rights to: (a) [confirm](#) whether a regulated entity is processing their health information, (b) [access](#) their consumer health data, and (c) [delete](#) consumer health data (Sec. 6(1)(a)-(c)). Notably, consumers are also entitled to access a list of the [names and email addresses](#) (or other online mechanisms for contact) of third-parties and affiliates with whom the data was “shared” or “sold.”



## U.S. Legislation Policy Brief

- **Deletion Requests** apply to all records managed by a regulated entity, including archived or backup systems and all records stored by affiliates, processors, contractors, and other third parties (Sec. 6(1)(c)). However, if consumer health data is stored on an archived or backup system that requires restoration, the consumer request may be delayed six months from the date of authenticating the request (Sec. 6(1)(c)(iii)).

Consumers must be able to exercise these rights in a manner consistent with the ways in which the consumer normally interacts with the regulated entity that is secure and allows for the authentication of the consumer (Sec. 6(d)). MHMD will further require regulated entities to comply with consumer requests within 45 days of receipt of the request, extendable by another 45 days when reasonably necessary (Sec. 6(g)). Information provided in response to a consumer request shall be provided free of charge, twice annually per consumer (Sec.6(f)). A controller is not required to comply with most consumer rights requests if they are unable to authenticate the request using “commercially reasonable efforts” and may request that the consumer provide additional information (Sec. 6(e)).

### Observations:

- **Broad Right of Access:** MHMD goes beyond access rights provided by most current U.S. comprehensive privacy laws by requiring that regulated entities disclose the names and contact information of third parties or affiliates with which health data is “shared.” Furthermore, the right of access does not contain the typical exception for trade secrets.
- **Broad Right of Deletion:** MHMD’s deletion right gives consumers the right to delete their health data from all records managed by a regulated entity, including from archived or backup systems and from within the records of processors, contractors, and other third parties within six months. The Act contains no exception for data that is retained in order to comply with deletion requests on an ongoing basis. This is significantly broader than the deletion right established by other state-level privacy laws. For example, the recently adopted [Colorado Privacy Act \(CPA\) Implementing Regulations](#) exempt archived and backup systems from the scope of the deletion right while such systems are inactive, and provides that entities may maintain consumer records “as needed to effectuate the deletion request.”
- **No Right to Correct Inaccurate Data:** Of the six U.S. comprehensive privacy laws enacted at the time of this memo, four provide a consumer right to correct inaccurate personal data, but no such right is included in MHMD.
- **No Exclusions for Pseudonymous Data:** Unlike many other comprehensive consumer privacy laws, MHMD does not define or establish consumer rights exceptions for “pseudonymous data.” Some other privacy laws exempt ““pseudonymous data,” which is typically defined as data that cannot be attributed to a specific individual without the use of additional information that a regulated entity or small business cannot access due to technical and organizational controls.

## 5. General Business Obligations

MHMD will impose a series of general business obligations on regulated entities containing both similarities to and differences from comparable state privacy laws. These include:

- **Transparency:** Regulated entities must maintain a “**consumer health data privacy policy**” that clearly and conspicuously discloses (1) the categories of health data “collected;” (2) the purpose of the “collection;” (3) the categories of sources from which data is “collected;” (4) the categories of health data that is “shared;” (5) the categories of third parties and affiliates with whom health data is “shared;” and (6) how a consumer may exercise their rights under the Act (Sec. 4(1)(a)). This policy must be linked on the regulated entity’s homepage (Sec. 4(b)).
- **Organizational Access Controls:** A regulated entity must restrict access to consumer health data to only those employees, processors, and contractors for which access is “necessary” to further the purpose of the “collection” or service the consumer requested (Sec. 7(1)(a)).
- **Data Security:** Regulated entities are also required to establish, implement, and maintain administrative, technical, and physical data security practices that, at a minimum, satisfy reasonable standards of care within the regulated entity’s industry, appropriate to the volume and nature of the consumer health data (Sec. 7(1)(b)).
- **Non-Retaliation:** Regulated entities are prohibited from discriminating against a consumer for exercising consumer rights under the Act (Sec. 5(d)).
- **Appeals Process:** A regulated entity is required to establish a process for consumers to appeal a refusal to take action on a consumer request under MHMD. The process is required to be “conspicuously available and similar to the process for submitting requests to initiate action” on consumer rights. A response to an appeal is required within 45 days and if an appeal is denied, the controller shall provide the consumer with an online mechanism, if available, or other methods through which the consumer may contact the Attorney General to submit a complaint (Sec. 6(h)).

### Observations:

- **Stand-Alone Health Privacy Notice or Not?** It is unclear under MHMD whether the health data privacy policy must be a stand-alone document or can be included with an overarching privacy policy. However, the Act’s provision that a regulated entity must “prominently publish a link to its consumer health data privacy policy on its homepage,” suggests an intent for this to be stand-alone policy that is not included in an overarching privacy notice.
- **No Non-Retaliation Exemption for Bona Fide Loyalty Programs:** Unlike other comprehensive privacy regimes, MHMD does not contain any exemptions for a regulated entity’s ability to offer consumers differential pricing or services based on

participation in bona fide loyalty or rewards programs, premium features, or member discounts. This will likely have significant effects, particularly for insurance wellness programs and device applications with “freemium” models.

- **No Prohibition Against Unlawful Discrimination:** Though a regulated entity may not retaliate against a consumer for exercising their consumer rights provided by the Act, there is no provision that prohibits processing health data in a manner that discriminates against protected classes according to state and federal laws, as provided by most other comprehensive data privacy laws.
- **Industry-Specific Data Security Requirements:** MHMD’s security provisions are unique as they are relative to the regulated entity’s industry standards. This responds to the potential for security norms and practices to develop (and vary) across different industries, but could result in differing standards for different regulated entities even if entities of a similar size are “collecting” the same type of data. Curiously, while organizations are required to limit access to “necessary” employees, the same requirement does not carry through to the individual employees of an organization’s contracted processors.

## 6. Regulated Entity and Processor Duties

MHMD distinguishes and divides responsibilities between regulated entities (including small businesses) and “**processors**” that process consumer health data on their behalf. At certain points, MHMD further refers to “**affiliates**” that share common branding with another legal entity; “**third parties**,” meaning an entity that is not a consumer, processor, small business, or affiliate; and “**contractors**,” which are not defined (See Sec. 6(1)(c)(ii)).

MHMD requires the adoption of a binding contract between a regulated entity and a processor that sets forth the processing instructions and limits the actions the processor may take with respect to the consumer health data (Sec. 8(1)(a)(ii)). Processors are required to assist the regulated entity by appropriate technical and organizations *insofar as is possible* in fulfilling the regulated entities obligations under MHMD (Sec. 8(1)(b)).

### Observations:

- **Common Contractual Requirement Missing:** MHMD is silent on numerous elements that must or must not be included in a contract between regulated entities and processors that are typically addressed by U.S. comprehensive privacy laws. For example, MHMD contains no provisions governing: (a) the retention of subprocessors, (b) either direct or independent assessment of the processor’s policies and compliance; or (c) explicitly limiting access to consumer health data by the processor’s employees or placing duties of confidentiality on the processor’s employees.

## 7. Restrictions on Geofencing

MHMD forbids “**persons**”<sup>6</sup> from “implement[ing] a geofence around an entity that provides in-person health care services where such geofence is used to: (1) *identify or track consumers* seeking health care services; (2) “*collect*” *consumer health* data from consumers; or (3) *send notifications, messages, or advertisements* to consumers related to their consumer health data or health care services.” (emphasis added) (Sec. 10). MHMD does not specify an effective date for these provisions; therefore, per [Washington legislative convention](#), this section will go into effect 90 days from enactment,

MHMD defines “**geofence**” as “technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wifi data, and/or any other form of spatial or location detection to establish a virtual boundary around a specific physical location, or to locate a consumer within a virtual boundary.” It further specifies that geofence “means a virtual boundary that is 2,000 feet or less from the perimeter of the physical location” (Sec. 3(14)).

### Observations:

- **Potential Impact on a Range of Use Cases:** MHMD’s restrictions on geofencing broadly forbid the use of geofencing technology to track or send messages to consumers entering health care facilities. This could impact a wide range of practices that involve the geofencing of health care facilities, including certain building security practices, push notifications that advertise consumer goods, and traffic pattern analysis for urban planning or construction purposes.
- **Broad Scope of Impacted Entities:** MHMD’s broad definition of “health care services” could include gyms, healthcare facilities within broader complexes, and consumer goods stores that house pharmacies.

## 8. Exemptions

MHMD establishes data-level exemptions for information protected under the the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Social Security Act, the Fair Credit Reporting Act (FCRA), and the Family Educational Rights and Privacy Act (FERPA) (Sec. 12(1)(a)(i) & Sec. 12(2)). MHMD further excludes certain information and documents created by hospitals for the purposes of complying with state law reporting requirements and information that is used only for public health activities and purposes as described in 45 C.F.R. Sec. 164.512. (Sec. 12(1)(a)(v)(D), Sec. 12(1)(a)(vi), & Sec. 12(1)(c)).

<sup>6</sup> MHMD defines “persons” more broadly than “regulated entities,” as encompassing “natural persons, corporations, trusts, unincorporated associations, and partnerships.” The definition exempts “government agencies, tribal nations, or contracted service providers when processing consumer health data on behalf of a government agency.” (Sec. 3(17)).

MHMD also establishes comparatively narrow purpose-based exemptions, stating that the obligations of the Act shall not restrict the use of consumer health data to “prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any activity that is illegal under Washington state law or federal law; preserve the integrity or security of systems; or investigate, report, or prosecute those responsible for such action that is illegal under Washington state law or federal law.” In invoking such an exemption, MHMD states that the entity “bears the burden of demonstrating that such processing qualifies for the exemption.” (Sec. 12(4)).

Finally, MHMD excludes “personal information that is used to engage in public or peer-reviewed scientific, historical, or statistical research in the *public interest* that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or a similar independent oversight entity that determines that the regulated entity or the small business has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification” from the scope of “consumer health data” (Sec. 3(8)(c)).

### Observations:

- **Data-Level Rather Than Entity-Level Carve Outs:** In contrast to an often-criticized approach taken by most U.S. comprehensive state laws, MHMD establishes exceptions for information subject to various federal sectoral privacy laws, rather than entities subject to these frameworks.
- **Common Exceptions Absent:** MHMD does not provide a number of common exceptions for product improvement or repair, conducting a product recall, or conducting internal operations reasonably aligned with a consumer’s expectations.
- **Possible Conflict of Law Issues?** Unlike comparable state privacy laws, MHMD does not create exceptions for complying with legal obligations or responding to legal process, raising potential conflict of law issues. MHMD will likely also interact with Washington’s ‘Shield Law’ ([HB 1469](#)), also enacted on April 27, 2023, which is intended to block out-of-state subpoenas related to reproductive health care. Furthermore, consumer requests of access and deletion may conflict with confidentiality and retention obligations required by other laws.
- **Public Interest Research Loophole?** By excluding any data used for public interest research from the definition of “consumer health data,” rather than clearly applying an exception limited to the research context, any data “shared” with researchers could arguably be processed, transferred, and sold to other entities without MHMD’s requirements applying.



## 9. Enforcement

MHMD provides for Attorney General enforcement as well as a private right of action by establishing that a violation of the Act is an unfair or deceptive trade practice under the Washington Consumer Protection Act ([chapter 19.86 RCW](#)) (“WCPA”) (Sec. 11).<sup>7</sup>

- **Attorney General Enforcement:** The Washington Attorney General’s office may seek injunctive relief as well as monetary damages for consumer restitution and legal costs, including reasonable attorney’s fees when suing to enforce the WCPA ([Chapter 19.86.80 RCW](#)).
- **Private Right of Action:** The WCPA permits a private right of action (PRA) by holding that, “[a]ny person *who is injured* in his or her business or property by a violation of RCW 19.86.020, 19.86.030, 19.86.040, 19.86.050, or 19.86.060... may bring a civil action...” ([Chapter 19.86.090 RCW](#)).<sup>8</sup> Consumers alleging violations of the WCPA may seek injunctions, to recover actual damages (including the cost of bringing suit and reasonable attorney’s fees), and the court has the discretion to award treble damages up to \$25,000 ([RCW 19.86.090](#)).

Finally, MHMD would require Washington’s [Joint Legislative and Audit Committee](#) to submit a report about enforcement actions taken pursuant to the Act to the Governor and relevant Legislative Committees by September 30, 2030 (Sec. 13(1) & (4)). The report will include information about the number of enforcement actions brought by both the Attorney General and consumers, any civil actions deemed by a judge to be “frivolous,” and “recommendations for potential changes to enforcement” of MHMD.

### Observations:

- **Lack of Clarity About PRA Requirements:** Between the engrossed text of MHMD and the [Senate Bill Report](#), it is unclear whether a violation of MHMD is intended to be a *per se* violation of the WCPA or if consumers must prove additional elements required for a civil action.
  - The Senate’s [‘legislative effects’](#) analysis states that the MHMD is intended to remove the requirement that a consumer injured by a violation must establish all required elements of an action under the WCPA.
  - However, to bring an action under the WCPA, a consumer typically must prove [five elements](#) to establish an individual claim: “[1] an unfair or deceptive act or practice, [2] occur[ing] in trade or commerce, [3] public interest impact, [4] injury to plaintiff’s business or property, and [5] causation.”



<sup>7</sup> “A violation of this chapter is not reasonable in relation to the development and preservation of business, and is an unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the consumer protection act.” (Sec. 11).

<sup>8</sup> “Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce” are unlawful under the CPA. ([Chapter 19.86.20 RCW](#)).

- MHMD establishes that “the practices covered by this chapter are *matters vitally affecting the public interest...*[and] [a] violation of this chapter...*is an unfair or deceptive act in trade or commerce* and an unfair method of competition for the purpose of applying the consumer protection act.” (emphasis added) (Sec. 11).
- This language [may indicate](#) that elements [1]-[3] of a private claim under the WCPA are established *per se* by a violation of MHMD, but that consumers still must prove elements [4] and [5] (injury to “business or property” and causation). Washington courts will have to resolve whether a violation of MHMD without the demonstration of further harm (such as financial or physical harm) constitutes adequate injury for the purpose of a private claim under the WCPA.
- **Private Right of Action:** MHMD’s inclusion of a private right of action, which sets it apart from many other state privacy laws, has drawn comparisons to the [Illinois Biometric Information Privacy Act \(BIPA\)](#). However, while BIPA provides for statutory damages (\$1,000 for a negligent violation and \$5,000 for an intentional or reckless violation), MHMD does not. Rather, MHMD allows plaintiffs to sue to recover actual damages for harms they suffer because of violations of the Act and gives courts the discretion to award treble damages up to the \$25,000 limit.

---

We welcome hearing from leaders at organizations that are thinking through how to comply with this new law. Contact us at [info@fpf.org](mailto:info@fpf.org), to continue the conversation and learn more about FPF’s U.S. Federal & State Legislation Group, as well as FPF’s Health Working Group.

*Disclaimer: This brief is for informational purposes only and should not be used as legal advice.*