

## Washington Passes Expansive Consumer Health Data Privacy Law

*Becky Burr, Adrienne E. Fowler, Daeyeong Kim, and Alex Tate*

On April 27, 2023, Washington State Governor Jay Inslee signed a new law that strictly regulates certain entities' collection and use of consumer health data that falls outside the reach of HIPAA and other federal health privacy laws. The [My Health My Data Act](#) ("MHMDA" or "Act") defines "consumer health data" broadly to include personal information that reveals a past, present, or future physical or mental health status of a consumer. Under the Act, businesses handling this kind of information as a controller will need to acquire affirmative consent prior to processing, sharing, or selling it. Importantly, the Act contains a private right of action. The Act's provisions go into effect on March 31, 2024, or June 30, 2024, depending on the size of the covered entity.

Below is our high-level overview of the Act's key definitions, consumer rights, duties of regulated entities (which may vary based on the size of the business), enforcement provisions, and next steps for businesses.

### **Definitions.**

The Act includes a number of broad definitions, which will impose regulatory obligations on many companies that are not currently subject to health-privacy-specific laws. For example:

- The Act is designed to protect any "**consumer**," which is broadly defined as any natural person who is a Washington resident or whose consumer health data is collected in Washington state. There is an employee exclusion, however: "Consumer" excludes a natural person acting in an employment context.
- "**Consumer health data**" is broadly defined to include information that is reasonably linkable to a consumer and identifies (either directly or by inference) a past, present, or future physical or mental health status. **Physical or mental health status**, in turn, is broadly defined to include individual health conditions, treatment, diseases, or diagnoses; social, psychological, behavioral, and medical interventions; gender-affirming care information; reproductive or sexual health information; use or purchase of prescribed medication; and data (including precise location information) that identifies a consumer seeking health care services or supplies. And "**health care services**" include any service provided to assess, improve, or learn about a person's physical or mental health.
- The Act applies to "**regulated entities**," entities that are either "businesses" or "controllers" under other privacy laws, i.e., entities that (i) conduct business or provide products or services targeted to consumers in Washington and (ii) determine the purpose and means of processing, sharing, or selling consumer health data. Government agencies, tribal nations, and service providers of government agencies are excluded. The law does not typically apply to entities that are either "service providers" or "data processors" under other privacy laws. But processors can be treated as regulated entities if, for example, they fail to adhere to a regulated entity's instructions for processing consumer health data.

- The Act restricts the “**sale**” of consumer health data, defined as an exchange of consumer health data for monetary or other valuable consideration.

### **Duties of regulated entities.**

Regulated entities:

- **Must establish a consumer health data privacy policy.** The privacy policy must disclose (i) the purposes and categories of consumer health data collected, (ii) the categories of sources from which consumer health data is collected, (iii) the categories of consumer health data that is shared and the categories of third parties and specific affiliates with whom they are shared, and (iv) how consumers can exercise their rights under the MHMDA. Any additional processing beyond what’s covered in the privacy policy requires additional disclosure and affirmative consent.
- **Cannot collect any consumer health data without affirmative consent,** unless such collection is necessary to provide a product or service requested by the consumer.
- **Cannot share or sell any consumer health data without affirmative consent.** Consent for **sharing** must be separate from the consent obtained to collect consumer health data. The **sale** of consumer health data requires valid authorization, i.e., separate affirmative consent meeting additional requirements.
- **Must establish reasonable data security practices,** including restricting consumer health data access to only necessary personnel, processors, and contractors.

### **Consumer rights.**

Consumers have the right to (i) request confirmation as to whether a covered entity is processing, sharing, or selling consumer health data, (ii) withdraw their consent for processing, and (iii) request to delete their covered health data. On the face of the statute, there are no exceptions to the deletion requirements.

### **Prohibition against geofencing.**

The Act bans geofencing, i.e., using location data to create a geographic boundary or to identify a consumer as within a geographic boundary, around an entity providing in-person health care services for the purposes of (i) identifying or tracking consumers seeking health care services, (ii) collecting consumer health data from consumers, or (iii) sending notifications, messages, or advertisements to consumers related to their consumer health data or health care services.

### **Enforcement.**

Both the Attorney General of Washington and consumers may enforce violations of the MHMDA under Washington’s Consumer Protection Act. The Attorney General can seek a civil penalty of up to \$7,500 per violation. In a private suit, a consumer can recover up to the lesser of \$25,000 or 3 times actual damages.

### **Next steps for businesses.**

**Determine whether your business falls within scope.** Given the broad scope of consumer health data covered by the law and the increased risk of litigation due to the Act’s private right of action,

businesses (particularly those that are not currently regulated by HIPAA) should carefully determine whether their data processing practices will be regulated by Washington's MHMDA.

**If a business falls within the Act's scope, the next step is to determine how to acquire affirmative consent consistent with the Act's requirements.** As outlined above, under MHMDA a regulated entity must acquire affirmative consent prior to collecting, sharing, and selling consumer health data. Consent must be stand-alone, i.e., not included in general terms and conditions, and the consent for sharing and selling such data must be separate from the consent for collection of that data. This will require covered entities to either modify their practices (to avoid collecting covered data) or update their consent forms and authorization flows for obtaining consumer consent.

Regulated entities typically have until March 31, 2024, to comply. Small businesses have until June 30, 2024. A "**small business**" is a regulated entity that (i) processes, sells, or shares consumer health data of fewer than 100,000 consumers annually or (ii) derives less than 50% of gross revenue from consumer health data and processes, sells, or shares consumer health data of fewer than 25,000 consumers.

\* \* \* \*

For more information on Washington's My Health My Data Act or HWG's data privacy, security, and governance practice, please contact [Becky Burr](#), [Adrienne E. Fowler](#), [Walter E. Anderson](#), [Alex Tate](#), [Daeyeong Kim](#), or the HWG lawyer with whom you regularly work.

*This advisory is not intended to convey legal advice. It is circulated to our clients and others as a convenience and is not intended to reflect or create an attorney-client relationship as to its subject matter.*