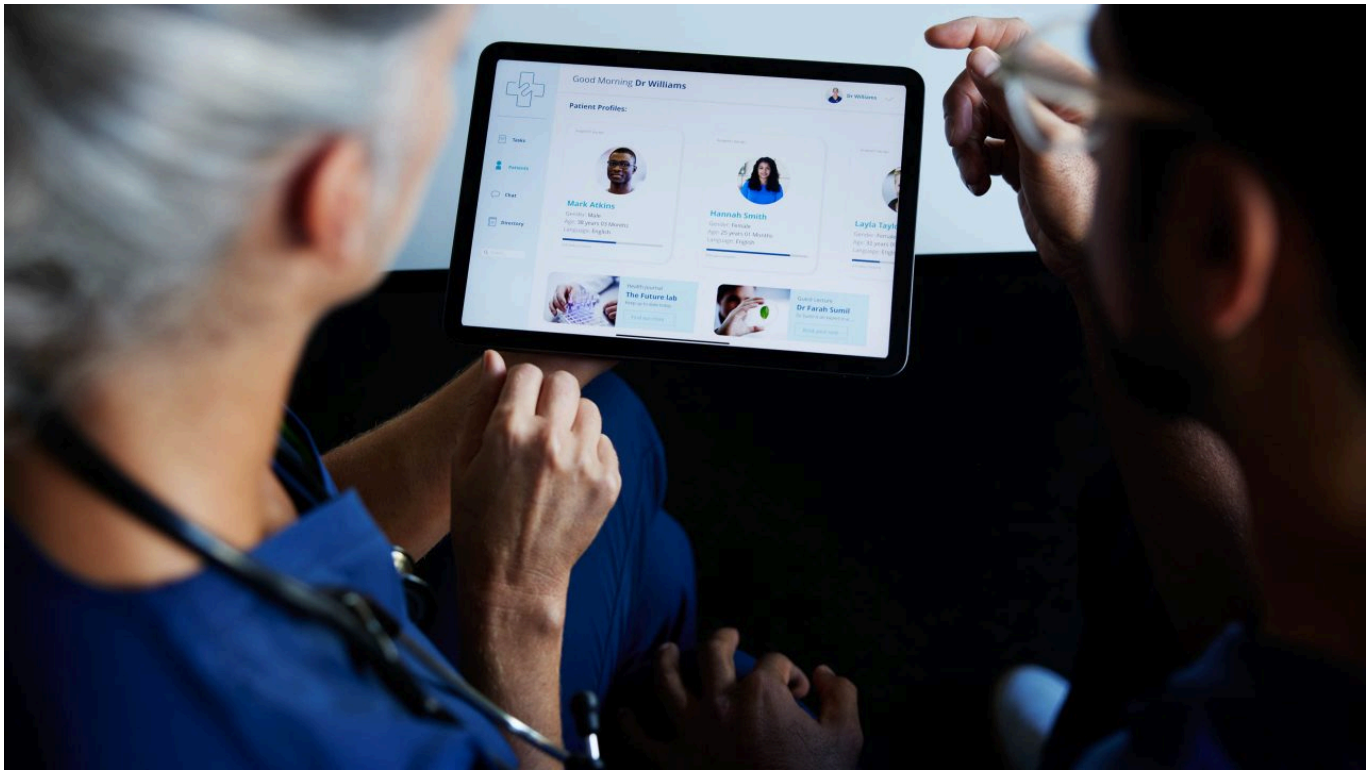
ARTICLE

Compliance Steps for Washington's My Health My Data Act

Ali Jessani

Apr 03, 2024 6 min read

Healthcare | Data Privacy Laws & Regulations | Data Privacy



Solskin via Getty Images

Compliance Insights for Washington's My Health My Data Act

One of the most notable privacy law developments from 2023, in what was a landmark year for the field, was the passage of Washington state's My Health My Data Act ("MHMDA" or the "Act"). The My Health My Data Act represents a new category of US privacy law – one that focuses on protecting "consumer health data" that falls outside the scope of the Health Insurance Portability and Accountability Act ("HIPAA") "Non-HIPAA" health data has been a focus for legislators and regulators in recent years (particularly the Federal Trade Commission), but the MHMDA is the first US privacy law that broadly and comprehensively develops rules for this area.

For companies building multistate privacy compliance programs, there are three elements of the MHMDA that are particularly notable: 1) it is a consent-driven law; 2) it is especially broad in its scope, despite theoretically only applying to a subset of personal information; and 3) it includes a private right of action for privacy violations. These factors distinguish the MHMDA from many other recent US state privacy laws.

Two other factors that make Washington's MHMDA especially notable are how quickly it passed the state legislature and how quickly it has inspired copycat bills. Unlike the California Consumer Privacy Act (CCPA), which needed the threat of a ballot initiative before it became the first state comprehensive privacy law in the United States, the MHMDA went through the normal legislative process in the state of Washington and passed relatively quickly through both chambers before being signed into law by the governor. This is noteworthy because Washington state has been unable to pass a general comprehensive privacy law, despite years of trying (see e.g., the Washington Privacy Act), but that did not stop the MHMDA from passing. Soon after the MHMDA passed, Nevada and Connecticut passed substantially similar bills, albeit without a private right of action in either. This also differs from the trajectory of the CCPA, which needed a few years after its passage in 2018 to inspire comprehensive privacy laws in other states.

Generally, entities that do business in Washington have only until March 31, 2024 before most of the law's substantive provisions go into effect, with small businesses having until June 30, 2024 to comply. Businesses that fall squarely within the law's purview because they clearly process what would be considered "consumer health data" under the law – such as companies that offer fitness trackers, wellness apps, personal health records, and health-related advertising – should carefully evaluate their compliance obligations. Other companies that process non-health data that may potentially be associated with consumer health data should also evaluate whether they fall subject to the law (or else potentially face class action litigation risk). This article details some of the notable elements of the MHMDA that companies should pay attention to as they evaluate how the law may impact their business.

Broad Scope

The MHMDA is broader than other U.S. state privacy laws, both in terms of whom it applies to, and what categories of health information it protects. The Act applies to "regulated entities," which, in relevant part, are entities that conduct business in Washington or produce or provide products or services that are targeted to consumers in Washington. This targeting language is unique for US state privacy laws and is similar to the extraterritoriality language used in the General Data Protection Regulation in the EU. The Act also applies to small businesses: While most state comprehensive privacy laws exclude certain entities that do not meet a minimum data processing or revenue

threshold, the MHMDA only pushes back the law's compliance timeline for these types of entities (small businesses are required to comply by June 30, 2024 compared to March 31, 2024 for "regulated entities" more generally).

The MHMDA covers a wide range of "consumer health data" and uses an expansive definition for this term. "Consumer health data" includes traditional categories of health information, such as information about health conditions and treatments, but it also incorporates other categories of personal information that are linked or "reasonably linkable" to a consumer and that identify the consumer's past, present or future physical or mental health status, such as precise location information, biometric data, and genetic data. Most notably, the term also incorporates "any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with [other categories of consumer health data] that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning). Because of this, the law has the potential to apply many companies that would not usually consider themselves as subject to a health privacy law.

Consent-Based Law

Unlike the state comprehensive privacy laws, which generally do not create a baseline consent requirement for the processing of personal information in the first instance (though they do require consent for certain specific processing activities), the MHMDA is a consent-driven law. And, like the GDPR, the law has a strict definition of consent. It defines consent as "a clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and unambiguous agreement." The law prohibits entities from obtaining consent through: 1) acceptance of a general or broad terms of use that includes descriptions of information collected along with other unrelated information; 2) a consumer hovering over, muting, pausing, or closing a given piece of content; or 3) deceptive designs (i.e., dark patterns).

In terms of where consent is relevant– regulated entities are required to obtain consent prior to collecting or sharing consumer health data, unless the collection or sharing is necessary to provide a product or service requested by the consumer. This restriction will create challenges for entities that do not have a direct relationship with consumers in relation to processing their consumer health data or who wish to process consumer health data for a secondary purpose.

The challenges will be even greater for entities that wish to "sell" consumer health data. The Act defines "selling" health data broadly as the exchange of consumer health data for monetary or other valuable consideration. Selling consumer health data requires entities

to obtain a specific authorization that includes nine distinct elements, including an expiration date that indicates that the authorization expires one year after it was obtained. This means that entities subject to the Act will need to renew their authorization annually to continue to sell such data. Based on how broadly sale is defined and how other regulators have interpreted similar definitions of this term, it seems likely that this requirement will be relevant for entities in the health advertising ecosystem.

Other Notable Provisions

In addition to being a consent-driven law, the MHMDA also has other unique provisions. For example, the law prohibits a person from placing a "geofence" around an entity that provides in-person healthcare 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. The Act defines a geofence as a 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. The law also requires regulated entities to implement access control requirements in relation to the consumer health data they process.

Even the Act's more "standard" provisions have their own twist. For example, the Act requires entities to provide consumers with a privacy notice that includes certain disclosures about how the entity processes consumer health data. Recent guidance from the Washington attorney general's office clarified that this policy "may not contain additional information not required under the My Health My Data Act." This adds another compliance obligation for entities subject to the law.

Enforcement

One of the most notable elements of the Act is that it is also enforceable as a violation of Washington's consumer protection law, which includes a private right of action and creates potential class action risk for companies. (This is in addition to being enforceable by the state attorney general, as many other state privacy laws are). The private right of action for aggrieved consumers can lead to civil penalties of up to $7,500 per violation. This raises the risk of non-compliance for businesses as they cannot solely rely on regulator discretion to avoid potential liability because plaintiffs' lawyers will be keeping an eye out as well. Given this risk, regulated entities should carefully evaluate their compliance practices ahead of the law's March 31 effective date (and small businesses should do the same before June 30).

Authors

Ali Jessani

...

View Bio →

Committees

This content was produced by:

Privacy and Information Security Committee →

Related Content

Consumer Protection | Data Privacy

Connecticut Attorney General Releases First Report on the CTDPA

Apr 02, 2024

Consumer Protection | Data Privacy

Updates in Privacy and Information Security, July 2023

Jul 31, 2023

Antitrust | Consumer Protection | Data Privacy

Office of Civil Rights Issues Guidance on HIPAA Compliant Use of Meta Pixels

Apr 24, 2023

Antitrust | Consumer Protection | Data Privacy

Can I Avoid Targeted Ads? The EU Rules on Pay or OK

Mar 18, 2024

Antitrust | Consumer Protection | Data Privacy

Auto Repair in the Age of Telematics Recap

Mar 15, 2024

Antitrust | Data Privacy

Designing Effective AI Compliance Programs

Feb 28, 2024