Published on *The National Law Review* https://natlawreview.com

Nevada and Washington State Pass Far-Reaching Consumer Health Data Privacy Laws

Article By:

Eva J. Pulliam

Gayland O. Hethcoat II

Mariam Creedon

As more states adopt consumer data privacy laws, Nevada and Washington stand out for their recent passage of legislation aimed specifically at protecting "consumer health data." Both states' laws are notably broad in their potential application to businesses in various industries throughout the United States and even in other countries. In this Q&A, we break down key requirements in Nevada's SB 370 and Washington's HB 1155, the Washington My Health My Data Act (MHMDA).

What Is "Consumer Health Data"?

Both SB 370 and MHMDA define "consumer health data" as personally identifiable information that is linked or reasonably capable of being linked to a consumer. Each law lists various categories of information that fall within this broad definition. Examples include information relating to a consumer's medical diagnoses and clinical treatment, as well as bodily functions, vital signs, symptoms, or measurements, such as those recorded by a wearable fitness tracker.

Both laws specify reproductive or sexual health care and gender-affirming care information in their respective definitions of "consumer health data," acknowledging the heightened sensitivities about this information as some states have adopted restrictions on abortion and gender-affirming procedures since the US Supreme Court overturned the federal constitutional right to abortion in *Dobbs v. Jackson Women's Health Organization*. Both laws also apply to geolocation information that may indicate a consumer's attempt to acquire or receive health care services, such as Global Positioning System (GPS) information showing a consumer at the address of an abortion clinic.

While some states have adopted consumer privacy laws that specifically protect genetic or biometric data, SB 370 and MHMDA define "consumer health data" to include both of those categories. SB 370 is narrower than MHMDA in this respect, however, applying only to biometric or genetic data relating to another specified category of consumer health data.

Who Must Comply with SB 370 and MHMDA?

Both SB 370 and MHMDA apply to "regulated entities," which is a legal entity that: (1) conducts business in the state or produces or provides products or services that are targeted to consumers in the state; or (2) determines the purpose and means of collecting, processing, sharing, or selling of consumer health data. Relatedly, a "consumer" is a natural person who resides in the applicable state or whose consumer health data is collected in that state. Given these broad definitions, both laws, which are industry agnostic, may apply extraterritorially to myriad types of businesses in other states and countries, even if data collection occurs while a consumer receives a product or service in another state or country.

What Must a Regulated Entity Do to Comply with SB 370 and MHMDA?

Like comprehensive state consumer privacy laws that have taken or will take effect in 2023, SB 370 and MHMDA impose standards on regulated entities' practices regarding the collection and sharing of consumers' data. In general, a regulated entity must obtain a consumer's consent to collect or share consumer health data, unless the collection or sharing is necessary to provide a product or service that the consumer requests. Moreover, the parameters for the regulated entity's data collection and sharing practices must be documented in a consumer health data privacy policy on the regulated entity's website. Among other information, the privacy policy must describe the categories of consumer health data that the regulated entity may collect and share, the purposes of the collection and sharing, and the categories of other entities with which the regulated entity may share consumer health data. To the extent the regulated entity seeks to engage in data collection or sharing activities outside these parameters, additional consent from the affected consumer is required.

Once a regulated entity acquires consumer health data, it must limit access to the data on a need-to-know basis, in furtherance of the purposes for which the consumer consented or to provide a product or service that the consumer requested. To this end, the regulated entity must maintain administrative, technical, and physical data security policies and safeguards.

SB 370 and MHMDA are further similar to other state consumer privacy laws in enumerating various rights to which a consumer is entitled with respect to his or her health data. These include rights to:

- Know whether a regulated entity is collecting, sharing, or selling the consumer's health data
- Access the consumer's health data
- Withdraw consent to the collection and sharing of the consumer's health data
- Have the consumer's health data deleted upon request
- Submit a request to exercise the consumer's rights
- Appeal a regulated entity's refusal to act on a request

Do SB 370 and MHMDA Apply to HIPAA Covered Entities?

Both SB 370 and MHMDA contain exceptions related to the federal Health Insurance Portability and Accountability Act (HIPAA), but SB 370's HIPAA exception is broader than MHMDA's. SB 370 categorically excepts "any person or entity" that is subject to HIPAA, including health care providers

and other covered entities and their business associates, from compliance with SB 370's requirements. By contrast, MHMDA's exception is limited only to "protected health information" (PHI) regulated under HIPAA. While both SB 370 and MHMDA include additional exceptions for PHI deidentified in accordance with HIPAA, MHMDA leaves open the possibility that a HIPAA covered entity, or its business associate, may be subject to MHMDA requirements in its processing of consumer health data that is not PHI or de-identified PHI.

When Do SB 370 and MHMDA Take Effect?

SB 370 and most of MHDMA's provisions take effect on March 31, 2024. For regulated entities that qualify as a "small business," most MHDMA requirements will not take effect until June 30, 2024.

Beginning July 23, 2023, MHDMA makes it unlawful for *any person* — whether a regulated entity or otherwise — to implement a geofence around a provider of in-person health care services for the purpose of: (1) identifying or tracking consumers seeking health care services; (2) collecting health data from consumers; or (3) sending notifications, messages, or advertisements to consumers related to their health data or health care services.

What Are the Penalties for Non-Compliance with SB 370 and MHMDA?

A violation of SB 370 is a "deceptive trade practice" under Nevada's deceptive trade practices law. Similarly, a violation of MHDMA is an "unfair or deceptive act in trade or commerce and an unfair method of competition" under Washington's consumer protection law. As such, non-compliance could subject a regulated entity to civil and criminal penalties under those other state laws.

Key Takeaways

Although SB 370 and MHMDA appear to be a reaction to some states' restrictions on abortion and gender-affirming care services, both laws have broader reach extending to both businesses within the burgeoning digital health and wellness sector that are not regulated under HIPAA, as well as businesses that have only a tangential connection to the health care and wellness industries. Before these laws take effect in 2024, businesses across the country should assess whether they collect any data that falls within each law's broad definition of "consumer health data." Businesses that do collect such data should take appropriate measures to be ready to comply with each applicable law. While some businesses may have to develop new privacy compliance processes, others may find that the programs they have established to comply with other state privacy laws can support compliance with SB 370 and MHMDA.

National Law Review, Volume XIII, Number 186