Buchalter
CLIENT ALERT

August 14, 2024

Washington State Privacy Update: My Health My Data Act is Now Effective

By: Wendy Lee

A little more than a year ago, on July 23, 2023, the Washington My Health My Data Act (WMHMDA) was passed into law. The law originally went into effect on March 31, 2024, however the compliance deadline for small businesses was June 30, 2024. This law was passed as a reaction to the *Dobbs v. Jackson* Supreme Court ruling and was designed to protect consumer health data. The focus of the Washington State Legislature was to plug perceived gaps in the Health Information Portability and Accountability Act (HIPAA) for data that is collected by noncovered entities (the law itself references apps and websites). The law applies to covered entities that conduct business in the state of Washington, all entities that process Washington residents' health data, and any entity or natural person that transfers consumer health data. For those familiar with other state privacy laws, you will immediately notice that this law is different in that it has a private right of action, exemptions are based on data categories (not entities) and the new valid authorization required to sell covered data is very unique compared to the consents required under GDPR and state privacy laws.

The WMHMDA protects consumer health privacy data by affording consumers the right to control the collection and use of their health data, while also implementing privacy protection requirements for businesses collecting, storing, processing, and transferring consumer health data. The WMHMDA is unique due to its broad language that both covers consumer health data, and even consumer nonhealth data.

Collecting and Storing Consumer Health Data

The WMHMDA requires covered businesses operating in Washington to "clearly and conspicuously" alert consumers of the desired categories of health data collected and shared. Businesses may only collect or share consumer health data if they obtain consent from the consumer, or are able to show the use or transfer of the consumer's data is necessary to provide the services for which the consumer provided their data.

Once a business obtains the consumer's health data, the businesses must establish, implement, and maintain a reasonable standard of technical and physical security practices to protect the consumer's data.

Consumer Control over their Data

Under the WMHMDA, consumers retain the right to inquire and confirm what third-parties have access to their health data even after consenting to the use of their data. Further, consumers may withdraw their consent from the business collecting data or sharing their data, and even demand their data be deleted. A

business will normally have forty-five days to comply with the consumer's request, unless the complexity and amount of consumer requests introduce excess difficulty.

In addition to the typical consent required under the GDPR and state privacy laws related to collection, sharing, and use of covered data, the Washington law requires a separate "valid authorization" for any sale or offer to sell consumer health data. This authorization requires specific disclosure of the data that is intended to be sold, the entity to which the data would be sold, a signature and date, and a one year expiration date. There is a record retention policy requiring that entities retain this authorization for six years from the later of the date of the signature or the date when it was last in effect.

Failure to comply is deemed by the law to be an unfair or deceptive act in trade or commerce and can put your business in risk of a private right of action under the Consumer Protection Act, which entitles the plaintiff to seek treble damages, civil penalties and attorney's fees and costs.

The Importance of this Act

Under the WMHMDA, "consumer health data" is not specifically limited to health data recorded or monitored by physicians or another healthcare provider. Rather, consumer health data includes biometric data, location data that could "reasonably indicate" that a consumer is acquiring health services, and any extrapolated nonhealth data that could indicate any physical or mental health status.

Due to the breadth of this newly effective privacy law, it is important for all entities conducting business in Washington to review all data they collect from consumers, and evaluate whether this data is either: (a) directly related to consumer physical or mental health, or (b) whether nonhealth data is used to identify a consumer's physical or emotional health status. If either of these criteria are met, entities with business in Washington must follow the appropriate disclosure, consent, authorization gathering, storage, security, and transfer requirements in the statute. Additionally, any legal entity who targets products or services to Washington consumers should get this legal compliance checkup as well. Unlike other state privacy laws, there is no exemption for number of data subjects or revenue thresholds that can protect the business.

Enforcement

Because this law has both a private right of action and can be enforced by the Washington State Attorney General, it is anticipated that enforcement will require a strong compliance program. The Attorney's General Office has provided some FAQs that might be helpful as you get started on your compliance efforts: https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy.

About Buchalter: Buchalter is a full service business law firm offering both a Privacy and Data Security Practice group together with a Health Care / Life Sciences Practice Group to help guide entities who may need to comply with this law.

Wendy Lee
Shareholder
(206) 319-7037
wlee@buchalter.com