COLLECTIVE INTELLIGENCE

Meet the New Global Regulator of Consumer Health Data: Washington State

Armin Tadayon
June 2023

Companies across the US and around the world may soon find themselves governed by regulators in Olympia, Washington, if their products or services are involved with consumer health data in the state.

A new Washington state law, which takes effect in less than a year, will likely extend beyond its borders and traditional healthcare organizations, potentially applying to the makers of fitness trackers, health apps and automobiles along with retailers and data-storage services.

Any company in the world that is engaged in the use and collection of consumer health data should take note of the following key aspects of Washington's My Health My Data Act (MHMDA):

- A regulated entity means any organization – including nonprofits – that has commercial ties to Washington and collects, processes, shares or sells consumer health data.
- Consumers aren't defined as state residents, rather as anyone whose data is processed in Washington.
- Health data 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."

Implications and trends

Unlike privacy laws in other states, MHMDA does not include revenue, data processing or consumer thresholds for regulated entities within its scope.

That's why Washington's rules may end up governing companies that aren't in health-focused industries and extend to companies that make, distribute or sell (wholesale or retail) products like smart watches or GPS devices if they collect location information that could indicate a consumer's attempt to access health services or supplies. For example, the maker of any car that stores the route to a pharmacy or doctor's office in Washington could be subject to the law.

Washington is going beyond federal data protections by addressing the proliferation of apps, services and websites that collect health information. The US federal Health Information Portability and Accountability Act (HIPAA) only protects health information collected by specific healthcare entities. While MHMDA is the first act of its kind in the US, other states such as California, New York and Illinois have introduced similar bills, indicating further state action in the absence of a comprehensive federal privacy law.

Is your organization ready?

The act may be enforced by the Washington attorney general and entitles aggrieved consumers to bring legal action against regulated entities themselves. This significantly raises the compliance risk. Washington's law goes into effect on March 31, 2024, for most regulated entities and on June 30, 2024, for small businesses.

If your firm is governed by the law, it must comply with obligations and restrictions for handling consumer health data that include:

1. disclosing to consumers the organization's health data collection and sharing practices and the consumer's rights;
2. obtaining affirmative consent for the particular purpose of collecting consumer health data and obtaining separate consent for sharing consumer health data (other than as necessary to provide a product or service a consumer has requested);
3. obtaining time-limited, opt-in consent and authorization to sell consumer health data;
4. implementing certain compliance agreements with service providers to ensure their compliance with the act;
5. granting consumers certain data subject rights (e.g., deletion, correction, etc.); and
6. prohibiting geofencing around in-person healthcare services.

Armin Tadayon
Associate, Washington, D.C.
atadayon@brunswickgroup.com
+1 (202) 908-8408

Armin is an attorney specializing in data security and privacy. Since joining Brunswick, he has advised clients on a variety of crisis and reputational issues – with a specific focus on data security and privacy. He also teaches a variety of law and technology courses at George Mason University.