New Twist or Approaching Tornado: The Remarkably Broad Washington State My Health My Data Act is Almost Here

February 20, 2024

By: Alfred Brunetti

While the past several years have seen a bevy of proposed and enacted comprehensive state privacy laws, the recently introduced health data-focused law from Washington State, known as the My Health My Data Act (MHMDA), reaches expansive new heights both in scope and reach. Arguably, MHMDA's terms will make it the broadest and most precarious state privacy law to date. Set to come into effect on March 31, 2024, the MHMDA may redefine the concept of health data privacy nationwide.

What Will MHMDA Regulate?

The MHMDA will regulate "consumer health data," expansively defined to be any personal information that is linked or reasonably linkable to a consumer and identifies his or her "past, present, or future physical or mental health status." Not surprisingly, this term specifically includes health diagnoses, treatments, and procedures. But, it also includes "bodily functions," "symptoms," data that identifies a person "seeking health care services," and any other information processed to associate a person with data that is "derived or extrapolated from non-health information." As a result, if an entity draws inferences about a person's health status from his or her purchase of certain products, those inferences themselves will be considered protected consumer health data. For example, if a regulated entity tracks the purchase of certain products in order to predict whether an identifiable consumer is pregnant, suffers from acid reflux, battles migraines, or even endures flat feet, that data will be viewed as protected "consumer health data."

Who Will MHMDA Regulate?

Any legal entity that conducts business in Washington State, or produces or provides products or services targeted at Washington State consumers, and (either alone or with others) determines the purpose and means of collecting, processing, sharing, or selling consumer health data, will be subject to the MHMDA's requirements. Unlike some other comprehensive state privacy laws, the MHMDA does not contain any gross revenue or consumer-count type thresholds for application. Therefore, "small businesses"[1] will also be within the MHMDA's scope.

Given its intentionally broad language, the MHMDA may cover the data of consumers who have no physical or purposeful connection to Washington State at all. The MHMDA will apply if a consumer's data is processed in Washington State, the home of many well-known cloud service providers. While simply storing data (rather than processing it) in the state's behemoth cloud computing infrastructures might not, alone, bring that stored data into the MHMDA's scope, any processing of that data in Washington State – a function that expressly includes accessing the data – can trigger the MHMDA.

Consumer Rights and Litigation Traps

Regulated entities will need to afford consumers various rights, including, but not limited to, withdrawable opt-in consent for the collection of his or her health data, the right to delete his or her health data, and the right to know all third parties with whom his or her health data has been shared. Additionally, all regulated entities will need to have a detailed and entirely separate Consumer Health Data Privacy Policy linked to their homepage. Like most other state privacy laws, the state Attorney General will enforce violations of the law.

The MHMDA additionally provides consumers with a private right of action that can be brought under Washington's Consumer Protection Act. Given the massive proliferation of litigation that has arisen from the Illinois Biometric Information Privacy Act (BIPA) – the only other state privacy law with a fulsome private right of action – it is a near certainty that the plaintiff's bar will probe and explore the applications of every one of MHMDA's expansive terms.

Geofencing

An uncommon aspect of the MHMDA is its absolute prohibition of the use of geofences. Generally, geofencing works by utilizing trackers and other data to create virtual boundaries that can interact with devices to locate and target individuals. The MHMDA bans the use of geofences on entities that provide "health care services," broadly defined to include any services provided to a person to "access, measure, improve or learn about" his or her mental or physical health. It further prohibits the use of geofencing to identify or track consumers who are seeking such health care services to collect consumer health data, or to send notifications, messages, or ads to a consumer related to their consumer health data or any health care services they have received. With this provision, Washington State will join Nevada, Connecticut, and New York as the only other states prohibiting geofencing of facilities where in-person health care services are provided.

Next Steps

Regulated entities under the MHMDA must fully comply beginning March 31, 2024. "Small businesses" generally have until June 30, 2024, but some requirements, like certain restrictions on the collection and sharing of health data, will take effect beginning March 31 for all entities regardless of size.

As you work toward updating policies and reviewing privacy practices in preparation for complying with upcoming state privacy laws, this is an opportune time to consider whether your business may fall within the scope of the MHMDA, and, if so, to address any requirements in advance of the law becoming fully operative. We anticipate enforcement of the MHMDA and other state privacy laws will increase with time, and we encourage all businesses to prepare accordingly.

---

[1] A regulated small business is defined as an entity that either: (a) collects, processes, sells, or shares consumer health data of fewer than 100,000 consumers during a calendar year; or (b) derives less than 50% of gross revenue from the collection, processing, selling, or sharing of consumer health data, and controls, processes, sells, or shares consumer health data of fewer than 25,000 consumers.