Proskauer

Going Beyond HIPAA – Washington Health Privacy Law Enacted: Broad Reach, Amorphous Scope, Big Litigation Risk

Proskauer on Privacy on **May 1, 2023**

The Health Information Portability and Accountability Act ("HIPAA") has long been described as the floor for health care privacy laws and that states and regulators are free to enact more restrictive health care privacy laws. Last week, Washington state became the first state in the nation to codify into law broad protections for consumer health data that go well beyond HIPAA.

Washington Governor Jay Inslee signed multiple healthcare privacy-related bills, including the enactment of Washington's "My Health My Data Act" (House Bill 1155) (or the "Act" or MHMDA"), which bolsters privacy protections around the collecting, sharing and selling of "consumer health data." In brief, the MHMDA: (1) establishes consumer rights with regard to consumer health data and defines obligations of regulated entities and businesses that collect, process, share, and sell consumer health data, subject to certain exceptions; (2) prohibits selling consumer health data without the requisite consent; (3) prohibits implementing a geofence around entities that provide in-person health care services if the geofence is used for certain purposes, including to identify or track consumers seeking healthcare services; (4) gives not only the state attorney general enforcement power, but grants consumers a private right of action to bring suit under the state's Consumer Protection Act for violations of the MHMDA. While the ban on geofencing comes into force in July 2023, the other provisions of the Act will not become effective until March 31, 2024 (or June 30, 2024 for "small businesses").

The MHMDA is a big deal.

The MHMDA is more than a health care privacy law. The Act will have a fundamental impact on the processing of personal information and will potentially have a more outsized impact than the California Consumer Privacy Act of 2018 ("CCPA"). Importantly, while styled as a health data law, the potential scope of "consumer health data" is expansive and extends to personal information much more into the realm of a traditional privacy law. In addition, the Act has wide scope and applies to non-Washington persons whose is data processed in Washington and out-of-state entities that "conduct business in Washington," and, the Act's consumer consent requirements are stringent and most important, the Act allows a private right of action for violations of the Act that is more extensive than the CCPA's provision (which is limited to data breaches involving certain information). The legal requirements under the Act also apply to regulated entities' processors, whether it be prohibitions against selling or sharing or the exercise of consumer rights under the Act (which apply to third party providers as well), perhaps prompting parties to reexamine vendor contracts that perhaps were previously revised in light of the CCPA.

While a full analysis of the law is beyond the scope of the post, below is a look at some of the more salient aspects of the MHMDA:

- **Main thrust:** Under the Act, a regulated entity or a "small business" may not collect or share any consumer health data except "with consent from the consumer for such collection for a specified purpose" or "to the extent necessary to provide a product or service that the consumer to whom such consumer health data relates has requested from such regulated entity or small business." It is unlawful under the Act for any person to sell consumer health data concerning a consumer without first obtaining a valid authorization from the consumer.
- **Consumer health data**: The definition of "consumer health data" is capacious and could be interpreted to include many more types of consumer data that is regularly shared across the digital ecosystem and bring many more types of entities under the umbrella of the Act than first thought. "Consumer health data" means "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." The Act includes a non-exhaustive list of examples, which begin with traditional healthcare and reproductive health data but also includes biometric and genetic data, precise geolocation information or other data that can pinpoint a consumer's attempt to receive health services, or any "data that identifies a consumer seeking health care services." The statute also brings in "individual health conditions,

status, diseases, or diagnoses" and "bodily functions, vital signs, symptoms, or measurements of the information described in this subsection" under the definition of "consumer health data," the types of information that are often collected and used by health-related apps of all sorts. The definition of "consumer health data" also includes catchalls that covers "data that identifies a consumer seeking health care services" and "any information that a [regulated entity or their respective processor], processes to associate or identify a consumer with [any of the other types of deemed to be consumer health data under the statute] derived or extrapolated from non-health information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning)." This catchall likely implicates data beyond traditional medical services or health app information and would seem to reach data profiling activities that use multiple points of "non-health information" or mobile location data for targeted advertising purposes and data profiling. The scope of the MHMDA gets even murkier when one considers the broad definitions of other terminology, including "consumer," "health care services," "personal information" and "reproductive or sexual health services."

- **Regulated entities:** "Regulated entity," among other things, means any legal entity that conducts business in Washington or "produces or provides products or services that are targeted to consumers in Washington" (except governmental agencies and vendors working on their behalf). This broad definition does not include any thresholds that appear in the CCPA (except the Act defines "small businesses," which would receive some additional time to comply with the law)[1]. It should be noted that regulated entities would not necessarily be limited to in-state businesses and seem to include, for example, out-of-state businesses or app operators that reach Washington users and collect covered data. Moreover, the Act could also potentially be applicable to non-Washington residents who happen to be in the state, as the Act's definition of "consumer" includes "a natural person whose consumer health data is collected in Washington," thereby widening the scope of the Act and making compliance even more burdensome and potentially national (or at least regional) in scope.
- **Notice and consent:** Besides requiring regulated entities to post details of their health data practices within their privacy policies, the Act requires regulated entities to obtain prior, express, opt-in consent from consumers before collecting or sharing consumer health data (with a prohibition against discriminating against consumers who exercise any rights under the Act). The Act also gives consumers the right to withdraw consent or request the deletion of consumer health data. The extent of the right of deletion requires regulated entities to notify all "affiliates, processors, contractors, and other third parties with whom the regulated entity or the small business has shared consumer health data of the deletion request."

- **Exceptions**: Generally speaking, the law's requirements do not include personal information that is used to engage in public or peer-reviewed scientific, historical, or statistical research that adheres to all other applicable federal and state privacy laws, nor does it apply to personal information governed by the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, and certain Washington state health statutes. The Act's requirements placed on regulated entities, small businesses, and processors will not apply where such regulated entities are collecting, using or disclosing consumer health data for the purposes of preventing or detecting cyberattacks or to respond to incidents of fraud or illegal behavior. It should be noted that "personal information" under the Act does not include deidentified data.
- **Applicability to HIPAA-regulated entities:** HIPAA regulates health data collected by specific covered entities (e.g., healthcare providers, health plans) and business associates and requires such entities to obtain an individual's authorization before using or disclosing protected health information (PHI). However, unbeknownst to many consumers, HIPAA does not regulate the collection and sharing of health-related data provided by consumer to certain apps, wearables and websites and it appears that the MHMDA seeks to close this loophole. The Act provides an exception for "protected health information for purposes of [HIPAA and related regulations]." Thus, HIPAA entities would have to comply with the Act for any covered activities regarding "consumer health data" that is not PHI regulated by HIPAA.
- **Private right of action:** The Act is enforceable by the state attorney general. However, one of the most far-reaching aspects of the MHMDA is its provision of a private right of action, allowing claims to brought for "a violation of this chapter" under state consumer protection laws. Thus, unlike many of the state data privacy laws that are the progeny of the CCPA, the MHMDA's private right of action may make Washington courts one of the new hotspots for privacy class actions (along with Illinois as the locus of biometric privacy suits under its state law).

Final Thoughts

The broad scope of the MHMDA, which brings in many types of consumer health data than traditional PHI, probably contains a few surprises for healthcare and other providers that already navigate HIPAA compliance with other state privacy requirements. As stated above, the reach of the Act will bring in not only traditional healthcare providers and services, but also perhaps online retailers that share data on consumer purchases of healthcare products and services, online providers collecting consumer data from health-related websites, and ad tech, mobile advertising providers, app operators and data brokers that might collect and package "consumer health data" or data that identifies a consumer with other healthcare data derived or profiled from non-health information. Taking advantage of the 2024 effective date of the Act, entities should consider reexamining consumer data flows to ensure an understanding of what is collected and shared and might fall under the Act's reach and what data is sufficiently deidentified or aggregated that would place it beyond the scope of the Act. The availability of a private right of action alone should cause many entities in the healthcare industry and related digital advertising space – including operators of health and lifestyle-related apps that formerly were beyond the reach of HIPAA – to look at the law closely and manage compliance risks. Without passage of a federal comprehensive data privacy law that would perhaps preempt Washington's law, providers will have to add the MHMDA to their list of compliance and litigation concerns.

---

[1] The Act contains a definition of "small business" (e.g., collects, sells, shares consumer health data of fewer than 100,000 consumers in a calendar year…"), but merely delays enforcement for such small businesses until June 30, 2024, a few months later than other regulated entities.

View original.