ROTHWELL FIGG

Wash. Health Privacy Bill May Affect Cos. Across Industries

Authored by Jenny Colgate for Law360
Article
7.6.23

In late April, Washington's governor signed the My Health My Data Act, or MHMD, into law.

The law, which goes into effect next year, aims to regulate the vast amount of health-related data processing that takes place outside of the Health Insurance Portability and Accountability Act, and provides a broad private right of action to enforce any violation.

If you are not a health-related company, are not located in Washington, are a small entity, are a nonprofit or do not process much data, you may be thinking, "My Health My Data is not my problem." If so, it is time to think again.

There are many reasons why you should think twice before disregarding this law.

First, unlike the general state privacy laws passed thus far, MHMD applies to all companies regardless of their revenues, how much data they process, and what percentage of their annual revenue is generated from processing or selling personal data. Also, there is no nonprofit carveout.

So, even if you process a tiny bit of health data — and keep reading to see how expansive the definition is of what constitutes consumer health data — MHMD may apply.

Second, it may be beyond a business's control whether they need to comply with MHMD. The law applies to:

- Washington residents;
- Any regulated entity that "conducts business in Washington or that produces or provides products or services that are targeted to customers in Washington"; and
- All "natural person[s] whose consumer health data is collected in Washington."

Key Contact

Jenny L. Colgate

Related Areas of Practice

Privacy and Data Protection

That does not sound so broad, right? Wrong.

The definition of "collect" is a game-changer. "Collect" is expansively defined to mean much more than gathering data in Washington.

"Collect" is defined as "to buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any manner." The possible breadth of this definition becomes clear when you fully explore the scope of each term.

- All natural persons whose consumer health data is purchased or rented in Washington.
  - Does this require direct purchase, or indirect purchases as well?
- All natural persons whose consumer health data is accessed in Washington.
  - If someone, a customer or employee, travels to Washington and accesses a person's consumer health data while there, does the company have to comply with MHMD?
- All natural persons whose consumer health data is retained in Washington.
  - If a company's data is even backed up on a server in Washington, does that subject them to MHMD? If so, the data center market in Seattle may shrink as a result of this law.
- All natural persons whose consumer health data is received or acquired in Washington.
  - Again, if a customer or employee is traveling in Washington and receives data while there, does this subject the company to MHMD?
- All natural persons whose consumer health data is inferred or derived in Washington.
  - If a company uses artificial intelligence to derive or generate consumer health data in Washington, it would be subject to MHMD compliance. While presumably the company would also be subject to compliance for storing the training data in Washington, the focus on derived consumer health data in MHMD appears to target situations where training data does not meet the definition of consumer health data, but the derived data does meet the definition of consumer health data.
- All natural persons whose consumer health data is processed in any way in the Washington.
  - Under this catch-all provision, one could potentially argue that a company is subject to MHMD compliance anytime a person's consumer health data touches the state of Washington in any way, regardless of whether the company has any say at all in — or knowledge of — the activities that take place in Washington.

Only time will tell whether such broad readings of MHMD's applicability will be permitted to stand, or whether courts will hold that the law does not apply in situations where the company's contacts with the state of Washington are de minimis.

Third, "consumer health data" is defined very broadly as "personal information that is linked or reasonably linkable to a consumer that identifies the consumer's past, present, or future physical or mental health status."

MHMD does not define "mental health" or "physical health," but the scope of data that could be encompassed by these terms is extensive. The act provides a nonexhaustive list of 13 categories of information that would be covered by the definition:

- Individual health conditions, treatment, diseases or diagnoses;
- Social, psychological, behavior and medical interventions;
- Health-related surgeries or procedures;
- Use or purchase of prescribed medication;
- Bodily functions, vital signs, symptoms or measurements of the information described in this subsection;
- Diagnoses or diagnostic testing, treatment or medication;
- Gender-affirming care information;
- Reproductive or sexual health information;
- Biometric data;
- Genetic data;
- Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies;
- Data that identifies a consumer seeking health care services; and
- Any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the data described in the above categories that is derived or extrapolated from nonhealth information — such as proxy, derivative, inferred or emergent data by any means, including algorithms or machine learning.

Further, because the above list is nonexhaustive, one can imagine other possible data that could fall under the definition of "consumer health data."

For example, the Centers for Disease Control and Prevention website says that mental health data includes emotional, psychological and social well-being, and affects how we think, feel and act, as well as how we handle stress, relate to others and make health choices.

Does this mean that MHMD applies to all data concerning one's emotions, psychological well-being, social well-being, how one is thinking, how one is feeling, how one is acting, how one is dealing with stress, how one is relating to others, and health choices one is making?

With respect to physical health, the National Institute of Health website talks about the following: what you put into your body, how much activity you get, your weight, how much you sleep, whether you smoke and your stress levels.

If Washington courts interpret consumer health data broadly, then presumably any companies that touch data concerning food or drinks, activities of any kind, anything relating to one's size or weight, such as clothing, and sleep may also be subject to MHMD.

It is difficult to imagine any company that does not collect data that falls into any of the above categories. Indeed, just as the term "personally identifiable information" was called into question in recent years because to a certain extent all data may be personally identifiable, the same may be true for Washington's expansively defined consumer health data.

In view of its broad scope, one can imagine the law applying not only to entities in the health care space, but also to retailers, clothing companies, grocery stores, any service with geolocation tracking, social media companies, gyms and other recreational facilities, movie theaters, restaurants, the entertainment industry, artificial intelligence companies, security companies that use biometric information, and the list goes on.

The reason why it matters that MHMD is so expansive and likely applies to so many companies, across so many industries, is because it has teeth.

MHMD contains a private right of action, enabling consumers to sue companies for violating any provision of the act under Washington's Consumer Protection Act and recover actual damages, costs and reasonable attorney fees, plus possible enhanced damages, capped at $25,000.

And notably, there are numerous ways in which a company can violate MHMD, triggering the private right of action, including:

- Failing to maintain and publish the required consumer health data privacy policy;
- Failing to obtain affirmative consent to collect consumer health data unless the collection is necessary to provide a product or service that the customer requested — again, note the broad definition of "collect" discussed above;
- Failing to obtain affirmative consent to share consumer health data unless the sharing is necessary to provide the product/service that the consumer requested;
- Failing to obtain a signed authorization to sell or offer for sale consumer health data;
- Failing to implement a geofence around facilities that provide in-person health care services; and
- Failing to provide the required consumer rights to, inter alia, confirm if data is being collected, shared or sold, access the data, and request deletion of data.

The broad scope of MHMD, combined with the numerous obligations required by the act and the fact that violation of any of them can trigger a private right of action, is likely going to result in more privacy litigation than we have seen under any other state privacy statute to date.

Thus far, it has been more the exception than the norm for state privacy statutes to contain a private right of action, and where they do, they have been limited.

For example, the California Consumer Privacy Act, as modified by the California Consumer Privacy Act, has only a limited private right of action tied to a statute that sets forth security rules, providing that consumers whose information is breached due to a business's failure to comply with the security rules can bring a private right of action.

Illinois' Biometric Information Privacy Act is probably the most litigated state privacy statute, and even its scope pales in comparison to MHMD.

In view of the above, it is important that companies — even companies that think at first glance that MHMD does not apply to them — to look very closely at the statute.

Companies should consider all of the data the company touches in any way through the lens of: Can this be considered "personal information that is linked or reasonably linkable to a consumer that identifies the consumer's past, present, or future physical or mental health status."

Further, while the least risky approach is always to just comply, companies should realize that compliance with MHMD is not easy. This is particularly true given the broadly defined terms — which will be further stretched by plaintiffs lawyers — and the demanding affirmative consent obligations, which can be off-putting for business.

This article was originally published in Law360's Expert Analysis section on July 6, 2023. Read more at: https://www.law360.com/articles/1695726/wash-health-privacy-bill-may-affect-cos-across-industries.