BCLP. Client Intelligent

Insights

TIME TO COMPLY: WASHINGTON MY HEALTH MY DATA ACT

Jan 29, 2024

SUMMARY

On April 27, 2023, the Washington State governor signed into law the My Health My Data Act or the MHMDA. In spite of the onerous and at times confusing requirements of the MHMDA, the Washington Attorney General (AG) has only published a short set of Frequently Asked Questions to help address some of this uncertainty. Nevertheless, most of the law's provisions take effect on March 31, 2024, meaning that, at this point, companies have a very short runway to meet their obligations and brace for the private right of action allowed for under the act.

With this in mind, we have prepared this brief recap of the law and the steps companies should consider as they gear up for compliance. Our more detailed summary of the MHMDA is available in our original insight, and we will also be releasing a series of short FAQs over the coming weeks to help companies prepare.

WHEN DOES THE MHMDA COME INTO EFFECT?

The MHMDA requires that companies comply with its obligations and prohibitions starting on March 31, 2024. However, small businesses are granted an extension until the end of June 2024.

WHO DOES THE MHMDA COVER?

Unlike other current or pending State privacy laws, the application of which are often narrowed by a revenue or data subject threshold, the MHMDA applies to **any** legal entity that conducts business in the state of Washington **or** produces or provides products or services targeted to consumers in Washington **and** alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling consumer health data.[1]The FAQs have clarified, however, that the MHMDA will not apply to entities that only store data in Washington.

WHAT DOES THE MHMDA COVER?

Although the MHMDA purports to protect only "consumer health data," rather than all consumer data, the MHMDA's broad definitions in this regard will sweep in significantly more data than the term would suggest. "Consumer health data" is defined as "personal information that is linked or reasonably linkable to a consumer and identifies the consumer's past, present, or future physical or mental health status."[2] Generally, the following information may trigger the obligations of the MHMDA:

- Individual health conditions, treatment, diseases or diagnoses,
- Social, psychological, behavioral, and medical interventions,
- Health-related surgeries or procedures,
- Use or purchase of prescribed medication,
- Gender-affirming care,
- Reproductive or sexual health information,
- Bodily functions, vital signs, symptoms, or measurements of information described as health status,
- Biometric data, including gait,
- Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies, and
- Any information that is used to associate a consumer with information about health status and that is derived or extrapolated from non-health data.

The AG clarified that simply collecting information on the purchase of toiletries does not fall within the MHMDA's definition of consumer health data. *However*, an inference drawn from those purchases could be considered "consumer health data." Therefore, companies will need to understand how consumer purchase information is used, particularly when such information could fall under the broad definition of consumer health data.

WHAT DOES THE LAW REQUIRE?

Privacy Notices: The MHMDA obligates regulated entities to maintain a "consumer health data privacy policy" that meets the related detailed content requirements.[3] Under the most recent FAQs, the Washington AG clarified that the link to the MHMDA Consumer Health Privacy Policy must be a separate and distinct link on the regulated entity's homepage and may not contain additional information not required under the MHMDA. This new guidance is still unclear as to whether the MHMDA requires a separate privacy policy for the collection and use of consumer health data or

whether the notice itself can be embedded in an organization's broader privacy policy. Until further clarification is provided, preparing a separate policy or a separate MHMDA section in the existing policy that contains all mandatory content (as opposed to cross-referencing relevant provisions in the general privacy policy) would likely be the safest approach.

The MHMDA also requires:

- **Consent for sharing, disclosing, and processing consumer health data.** One critical feature of the MHMDA is the explicit obligation that entities obtain express opt-in consent from consumers for the collection and use of their health data for everything but the processing necessary to provide the requested product or service.[4]
- **Authorization for sale of consumer health data.** In addition to obtaining the general consent described above, companies must also obtain an express and signed (separate) authorization from consumers prior to selling their consumer health data to another organization.[5] This authorization is similar in content to a HIPAA authorization.
- Under the MHMDA, it is unlawful for any person to implement a geofence around an entity that provides in-person health care services where such geofence is used to: (1) identify or track consumers seeking health care services; (2) collect consumer health data from consumers; or (3) send notifications, messages, or advertisements to consumers related to their consumer health data or health care services.[6]
- **Data subject access requests.** The MHMDA provides consumers with several rights concerning their consumer health data, including the right to confirm whether a company is selling or sharing consumer health data as well as to know the identity of the third parties or affiliates to which the company is sharing or selling data, the right to withdraw consent, and/or the right to request deletion of their consumer health data.[7]Typical exceptions, such as the compliance with law exception, are notably absent under the MHMDA.

WHAT ARE THE POTENTIAL PENALTIES?

The MHMDA allows the Washington Attorney General to enforce violations through the State's Consumer Protection Act. The AG's office can impose a civil penalty of up to $7,500 per violation. In addition, and more importantly from a practical impact, the MHMDA provides consumers a private right of action to seek damages for violations of the law, creating the real and immediate risk of a costly class action lawsuit.[8]

WHAT SHOULD YOUR ORGANIZATION DO TO PREPARE?

Given the private right of action and the complex obligations of the MHMDA, it is critical for companies to begin compliance efforts as soon as possible. As a starting point, companies should

work to:

- Understand the scope of impacted data, as well as the underlying purposes of use, sources and potential recipients,
- Analyze and document whether any exceptions apply,
- Evaluate where current disclosures, consent mechanisms (e.g., cookies consent management platforms) or other compliance efforts may already address certain requirements of the law and/or can be updated for these purposes, and
- Begin building required notices, consents and authorizations, likely in a more conservative fashion until additional guidance or clarification is available.

We will be digging into the MHMDA's obligations in the weeks to come to help companies work through these next steps in more detail.

FOOTNOTES

[1] Section 3(23).

[2] Section 3(8)(a).

[3] Section 4.

[4] Section 5.

[5] Section 9.

[6] Section 10.

[7] Section 6.

[8] Section 11.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Goli Mahdavi

San Francisco

goli.mahdavi@bclplaw.com
+1 415 675 3448

Andrea Rastelli

Boulder

andrea.rastelli@bclplaw.com
+1 303 417 8564
