BCLP. Client Intelligent

Insights

WASHINGTON MY HEALTH MY DATA ACT: COMPLIANCE HURDLES AND HOW TO PREPARE

May 18, 2023

SUMMARY

On April 27, 2023, the Washington state governor signed into law the My Health My Data Act, also known as the MHMDA. The majority of the law's provisions will take effect on March 31, 2024, providing companies with one (short) year to prepare to meet their obligations and brace for the private class action litigation allowed under the act. Even with all of the other state laws that have recently passed or are waiting in the wings, the MHMDA stands out in its broad scope, confusing and/or onerous obligations and potential risk for organizations. Companies should not put compliance with its mandates on the back burner. With this in mind, we have prepared a summary of key compliance requirements of the MHMDA. We will continue to examine the law in more depth and track guidance and other developments as they emerge.

What does the MHMDA Cover?

Unlike other current or pending state privacy laws, the application of which is often narrowed by a revenue or data subject quantity 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] "Consumer" includes both a Washington resident or a person whose health data is processed in Washington.[2] These two definitions expand the reach of the law to almost any type of entity operating in Washington and extend the protections of the law to residents and non-residents if their data is processed in Washington.

Although the MHMDA purports to protect "consumer health data," the MHMDA's broad definitions will likely sweep in significantly more data than the name 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."[3] The MHMDA provides a non-exhaustive list of examples of what is considered "health status."[4]

Such examples that would logically be included within the definition of "health status" include information about:

- Individual health conditions, treatment, diseases or diagnosis,
- Social, psychological, behavioral, and medical interventions,
- Health-related surgeries or procedures,
- Use or purchase of prescribed medication,
- Gender-affirming care, and
- Reproductive or sexual health information.

These categories are not, however, limited to information provided in health care settings and/or for the purpose of health care services. Therefore, information entered into websites or apps regarding any of the above could conceivably be covered by this law (e.g., "how do I treat diabetes?" or "side effects of a birth control medicine"). Moreover, the MHMDA includes within the definition of health status other more expansive categories, including information about:

- Bodily functions, vital signs, symptoms, or measurements of information described as health status,
- Biometric data,
- 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.

These broad and relatively undefined categories mean that almost any information that could be associated with a consumer's health, such as purchases at a supermarket or pharmacy, attendance or membership at a fitness center, or the mere act of visiting a website that provides general health information are arguably in scope for all requirements of the law (and potential for class action lawsuits in the event of a potential violation).

It is also important to note that the definition of consumer health status suggests that collection of biometric information in any context is consumer health data because biometric data is listed as consumer health status with no qualifications or exclusions of other uses.

Are There Any Exemptions That Apply to the MHMDA?

While the MHMDA has a broad scope, it does have several exemptions that are important for organizations to consider.[5] For example, de-identified data and publicly available information are excluded from application of the law. Additionally, the definition of "consumer" does not include employees, such that health data gathered in the context of employment or related activities should be squarely outside the scope of the law.[6]

However, the MHMDA does not have many entity-level exemptions, as many other state privacy laws do, and instead provides exemptions for specific types of data. For example, the MHMDA carves out personally identifiable information that falls within the purview of the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, the Social Security Act, Title XI, the Fair Credit Reporting Act, and the Family Educational Rights and Privacy Act, but does not provide a blanket exemption for organizations subject to these laws. The MHMDA also provides a clinical trial carve out similar to that seen in other state privacy laws.

The MHMDA also provides a specific exemption that may be of particular importance for organizations that collect biometric data or other types of information for identity verification or similar security related purposes. More specifically, the MHMDA does not apply if the information is used to prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any activity that is illegal under Washington State or federal law. However, companies must demonstrate that such processing qualifies for one of the listed exemptions and should, therefore, carefully document the underlying reasoning regarding why and to what extent a particular exemption would apply.[7]

What does the MHMDA Require?

Companies subject to the MHMDA will be required to comply with specific requirements that potentially require more compliance measures than other state privacy laws with a particular focus on consent. Key within these obligations are:

Privacy Notices. The MHMDA obligates regulated entities to maintain a “consumer health data privacy policy” that meets the related detailed content requirements.[8] It is still unclear whether the MHMDA requires a separate privacy policy for the collection and use of consumer health data, but based on the language of this provision, preparing a separate policy would likely be the most conservative/safest approach until additional clarification is provided.

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 processing necessary to provide the requested product or service.[9] Companies must fully inform consumers about how their data will be used, and they must obtain consent before collecting or processing any data, even potentially

more than once if the data is used for multiple purposes. Consumers must also have the option to withdraw their consent.

The MHMDA does not provide meaningful guidance on what is considered necessary and what would require consent. Therefore, companies must clearly delineate and analyze what use of consumer health data is essential to provide the requested services and build a consent mechanism for other uses (e.g., internal analytics, development of profiles, advertising). Additionally, any sharing of health data with affiliates also requires express consent before such information can be shared. This again is a deviation from the requirements imposed by other state privacy laws and could pose a significant compliance burden, particularly for large organizations that are comprised of multiple related affiliates even if they operate under the same brand. For example, it appears that organizations comprised of multiple legal entities for tax or other purposes would be required to obtain consumer consent before storing on a central CRM and/or using this information across the broader organization.

Furthermore, if consent is required, companies must obtain express consent that clearly and conspicuously discloses: (i) the categories of consumer health data disclosed, (ii) the purpose for the collection and sharing of the consumer health data, including how it will be used, (iii) the categories of entities that the information will be shared with, and (iv) how consumers can withdraw consent. Providing this information as part of a streamlined consent mechanism will almost certainly prove difficult for organizations and potentially could lead to consumer frustration with lengthy and multiple consent prompts.

Authorization for Sale of Consumer Health Data. Under the MHMDA, companies cannot sell consumer health data without first obtaining a signed (separate) authorization from consumers.[10] The definition of "sale" is broad under the MHMDA and includes any exchange of consumer health data for monetary or other valuable consideration.[11] Notably, this authorization must be obtained separately from any previous consent collected. Among other explicit requirements, this authorization must identify the specific consumer health data the company intends to sell, the name and contact information of the organization purchasing the data, and a description of the purpose of the sale. It also remains to be seen whether the use of cookies or similar technologies for advertising or similar marketing purposes would qualify as a sale. If that were the case, and because there is no carve out provided for disclosures done at the direction of the consumer like that provided by the California Privacy Rights Act, organizations would likely have a very difficult time meeting these authorization requirements in this context.

Geofencing. 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.[12] Under the MHMDA, geofence means a virtual boundary that is 2,000

feet or less from the perimeter of the physical location of the company.[13] Due to the broad definition of health care services as "any service provided to a person to assess, measure, improve, or learn about a person's mental or physical health"[14] as well as "consumer health data" (discussed above), this provision could implicate substantially more than just a health care facility, but also potentially fitness facilities, spas, beauty salons, and pharmacies such that organizations utilizing geofencing will need to carefully consider how to best to avoid triggering this provision even in these other non-traditional health care settings.

Data Subject Access Requests. The MHMDA provides consumers with several rights concerning their consumer health data.[15] Consumers have the right to confirm whether a company is collecting, sharing, or selling consumer health data and to access such data. Additionally, consumers have the right to withdraw their consent and request deletion of their consumer health data. Unlike other state privacy laws, the MHMDA does not provide for exemptions to these rights (i.e., companies do not have a right to reject a deletion request if another conflicting law requires that the company maintain the data). This could cause direct conflicts with existing laws and/or generally create confusion as to when data may be retained for valid reasons.

The deletion and access requests have substantial technical implications as well. Deletion will need to include all archives, backup systems and information held by third party processors. Additionally, if a company receives an access request, the company will have to provide the consumer a copy of the names and email addresses of all organizations that consumer health data was shared or sold to.

When does the MHMDA Come into Effect?

The MHMDA goes into force on March 31, 2024. However, small businesses are granted an extension until the end of June 2024. The only exception to these dates is the provision prohibiting geofencing, which does not have an effective date, making it enforceable within 90 days of the passage of the bill.

What are the Penalties under the MHMDA?

The MHMDA allows the Washington attorney general to enforce violations through the state's Consumer Protection Act.[16] The attorney general's office can impose civil penalties that rise 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. However, it is important to note that consumers must allege actual damages under the MHMDA to bring suit. The threat of private enforcement will leave organizations scrambling to decipher the broad and at times confusing obligations of the law in anticipation of an almost certain flurry of class action lawsuits and/or meaningful guidance via enforcement or regulations.

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 kick off their compliance efforts for this new law as soon as possible. Companies should work to:

- Understand the potential in-scope 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 or other compliance efforts may already address certain requirements of the law and/or can be updated for these purposes,
- Begin building required notices, consents and authorizations, likely in a more conservative fashion until additional guidance or clarification is available, and
- Stay tuned for additional guidance from the BCLP Global Privacy and Security team.

[1] Section 3(23).

[2] Section 3(7).

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

[4] Section 3(8)(b).

[5] Section 12.

[6] Section 3(7).

[7] Section 12(d)(3)-(4).

[8] Section 4.

[9] Section 5.

[10] Section 9.

[11] Section 3(26).

[12] Section 10.

[13] Section 3(14).

[14] Section 3(15).

[15] Section 6.

[16] Section 11.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Christian M. Auty

Chicago

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

Amy de La Lama

Boulder

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

Goli Mahdavi

San Francisco

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

Andrea Rastelli

Boulder

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

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.

© 2025 Bryan Cave Leighton Paisner LLP.