BCLP. Client Intelligent

Insights

WASHINGTON MY HEALTH MY DATA ACT FAQS: DATA SUBJECT RIGHTS

Feb 14, 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.

Like so many other features of the MHMDA, data subject rights are deceptively complicated and have the potential to create significant administrative hurdles to getting it right. As promised in our recent summary of the MHMDA (MHMDA: Time to Comply), we are examining in more detail these tricky issues in our MHMDA FAQs and have done a deep dive into data subject rights in this FAQ.

WHAT DATA SUBJECT RIGHTS ARE AVAILABLE UNDER THE MHMDA?

The MHMDA provides consumers with the right to know/access consumer health data, the right to have such information deleted and the right to withdraw consent that had previously been granted. Organizations are also required to provide consumers with the right to appeal any denial of a request.

RIGHT TO KNOW/ACCESS

A consumer has the right to confirm whether an organization is collecting, sharing (disclosing) or selling their consumer health data and to access such data. The information provided must include a list of all third parties and affiliates to which consumer health data has been shared or sold **and** an active email address or other online mechanism that the consumer may use to contact these parties. Note that this obligation does not cover service providers/processors.

RIGHT TO WITHDRAW CONSENT

A consumer has the right to withdraw consent to the relevant processing, sharing or sale of consumer health data.

RIGHT TO DELETE CONSUMER HEALTH DATA

A consumer has the right to have consumer health data deleted from an organization's records, including archived or back-up systems. The organization must also push this request to all affiliates, processors, contractors and other third parties with whom the organization has shared the data.

RIGHT TO AN APPEAL

In addition to the primary rights described above, an organization must establish an appeals process by which a consumer can appeal the organization's decision not to grant a request (e.g., denial of an access or deletion request). If an organization subsequently denies the appeal, the response must provide a written explanation of the reasons for denying the appeal. Notably, the response also must provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Washington Attorney General to submit a complaint. The Washington AG has not yet published a dedicated mechanism for complaints, but may do so prior to the March 31, 2024 effective date. If not, an email address or phone number should be sufficient.

WHAT ARE THE TIMING REQUIREMENTS?

Organizations are required to comply with the request within **45** days of receipt of the request. One 45-day extension can be applied depending on the complexity or number of the requests so long as a consumer is notified of the extension within the initial 45 day period.

Appeals must also be addressed within **45** days of receipt of the appeal from the consumer. No extensions are available for resolving the appeal.

ARE THERE EXCEPTIONS?

No, there are no express exceptions to the data subject rights provided to consumers under the law. This is a significant issue that will hopefully be addressed via amendments or the regulations.

There is a limited catch-all exception indicating that the obligations imposed by the law do not restrict an organization's ability to collect, use or disclose consumer health data 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 law or federal law;

- preserve the integrity or security of systems; or
- investigate, report, or prosecute those responsible for any such action that is illegal under Washington state law or federal law.

Organizations could point to these exceptions for requests for access or deletion to the extent necessary for one of the purposes listed above, but organizations that rely on this exception have the burden of demonstrating that the decision qualifies. In addition, this exception does not appear to extend to compliance with applicable law (e.g., retention requirements), a common exception in other data privacy laws. Therefore, if and until there is additional guidance provided by Washington regulators, organizations should generally work to honor data subject rights requests wherever possible or tailor any denial as narrowly as possible.

HOW CAN YOU PREPARE?

It is important to be prepared to address data subject rights as soon as the law is in effect. With this in mind, organizations can start this process by considering the following:

EVALUATE CURRENT DATA SUBJECT RIGHTS PROCESSES

developed for other states and laws to understand where these existing efforts can be leveraged for addressing the obligations of the MHMDA. The good news is that most organizations will have some steps in place for addressing rights of access and deletion as well as honoring withdrawal of consent. Nevertheless, adjustments will be needed to address the unique aspects of this law.

ESTABLISH A PROCEDURE FOR IDENTIFYING WASHINGTON RESIDENTS

Because these rights are unique and more onerous in a number of ways, organizations should carefully determine whether and how they will limit compliance to Washington residents. Typical methods could involve requesting a confirmation from the consumer of the state of residence or potentially applying geofencing, noting that a more conservative approach to honoring requests will likely make sense for this law considering the private of action.

IDENTIFY WHAT CONSUMER HEALTH DATA WOULD BE IN-SCOPE FOR THE REQUESTS

Although the definition of consumer health data is quite broad under the MDMHA, it is more limited than the expansive definitions of personal information (any information that could reasonably identify an individual) under other state privacy laws. Therefore, to both provide an appropriately scoped response under the law and also to limit the scope of the data subject rights under the MHMDA, companies will need to specifically identify what information about a consumer would qualify as consumer health data so they can then provide relevant information or take action (deletion).

IDENTIFY RECIPIENTS OF CONSUMER HEALTH DATA

As noted above, organizations are required to identify all affiliates and other organizations that to which they have disclosed consumer health data **and** provide a manner to contact those entities. This will practically be a heavy lift for organizations that have multiple affiliates and/or that routinely disclose information to unaffiliated third parties. For affiliated companies, companies could consider providing a central email or source of contact for all such companies, but it will be critical to confirm that any request or inquiry from a consumer is addressed with enough specificity on the affiliate level to be defensible. Companies should push down contractual obligations on unaffiliated parties regarding their compliance with these requests.

DETERMINE WHERE THE BROAD EXCEPTION DISCUSSED ABOVE MIGHT BE APPLICABLE

Companies should carefully consider whether the broad exception will apply in certain circumstances and then begin the process of documenting these decisions so they are able to meet the corresponding burden of proof.

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

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.