FENWICK

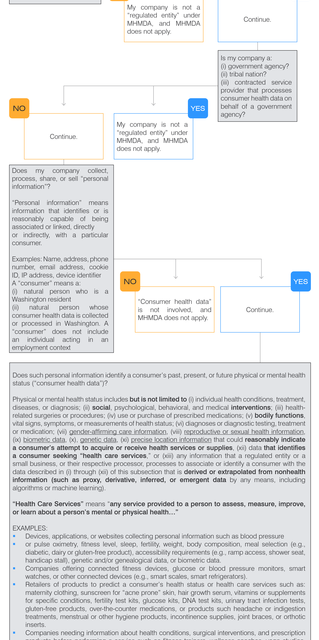
Washington's My Health My Data Act – A Roadmap for Compliance

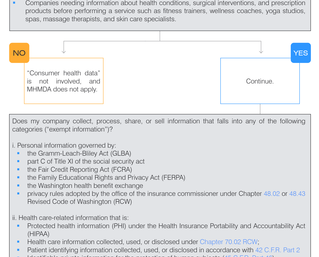
What is the new Washington My Health My Data Act (MHMDA)?

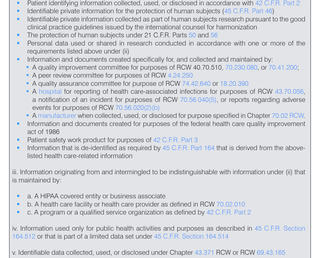
MHMDA aims to provide stronger privacy protections for "consumer health data" by:

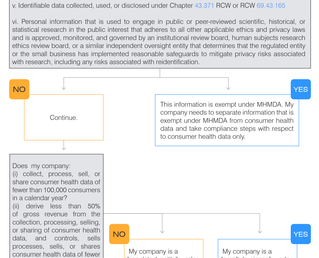
- Requiring additional disclosures for the collection, use, and sharing of consumer health data
- Restricting the use of consumer health data to what is necessary to provide a consumer-requested service unless the consumer provides their consent or a written authorization for additional processing
- Giving consumers the right to access and delete their consumer health data and withdraw their consent for collection and sharing
- Prohibiting the sale of consumer health data without a valid authorization signed by the consumer
- Prohibiting certain uses of a geofence around a facility that provides health care services

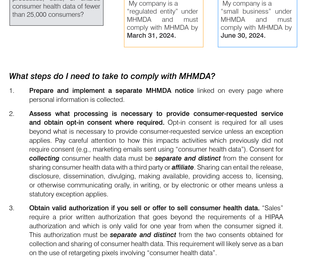
Does MHMDA apply to my company?











What steps do I need to take to comply with MHMDA?

1. **Prepare and implement a separate MHMDA notice** linked on every page where personal information is collected.
2. **Assess what processing is necessary to provide consumer-requested service and obtain opt-in consent where required.** Opt-in consent is required for all uses beyond what is necessary to provide consumer-requested service unless an exception applies. Pay careful attention to how this impacts activities which previously did not require consent (e.g., marketing emails sent using "consumer health data"). Consent for *collecting* consumer health data must be *separate and distinct* from the consent for sharing consumer health data with a third party or **affiliate**. Sharing can entail the release, disclosure, dissemination, divulging, making available, providing access to, licensing, or otherwise communicating orally, in writing, or by electronic or other means unless a statutory exception applies.
3. **Obtain valid authorization if you sell or offer to sell consumer health data.** "Sales" require a prior written authorization that goes beyond the requirements of a HIPAA authorization and which is only valid for one year from when the consumer signed it. This authorization must be *separate and distinct* from the two consents obtained for collection and sharing of consumer health data. This requirement will likely serve as a ban on the use of retargeting pixels involving "consumer health data".
4. **Implement or update mechanisms to respond to broadened individual rights requests.** Under MHDMA, consumers have unique access and deletion rights that go further than other U.S. consumer privacy laws. For example, individuals have the right to receive a list of all third parties and affiliates with whom the regulated entity has "shared" or "sold" consumer health data. Consumers have the right to receive an email address or online mechanism to contact such third parties. In addition, there are no common statutory exceptions to consumers' deletion rights, such as compliance with applicable law.
5. **Understand and/or develop approach around prohibitions on geofencing.** MHMDA prohibits geofencing around locations that provide in-person health care services where the 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. **Implement and maintain reasonable security practices** to protect consumer health data.
7. **Review and update your processor contracts.** If you are a regulated entity or a small business subject to the MHMDA ("Regulated Company"), you must have a binding contract in place with all vendors that process consumer health data on your behalf. Such contracts must include provisions setting forth the processing instructions and limiting actions the processor may take when processing consumer health data. If you are a process consumer health data for a Regulated Company, and you fail to adhere to its instructions, or if you process consumer health data in a manner that is outside the scope of your contract with the Regulated Company, you are considered a Regulated Company and become subject to all the requirements of the MHMDA!

What are the risks for not complying with MHMDA?

The biggest risk is that, unlike most U.S. state privacy laws, violations of MHMDA can be enforced through a private right of action, but plaintiffs must prove damages. Because of the extraterritorial application of MHMDA, the broad spectrum of data that can qualify as

"consumer health data," the burdensome compliance requirements, and the greater range of companies that used to be excluded from the HIPAA compliance but now fall under the ambit of this law, we anticipate that the plaintiffs' bar will be very active, if not aggressive, in suing companies for violating any provision of MHMDA (especially those which are obvious from visiting a company's website).

The law allows plaintiffs to recover actual damages for the injury they suffered because of a company's violation of MHMDA, as well as the costs of the suit, including reasonable attorney's fees. Courts also have the discretion to award treble damages up to the $25,000 limit.

In many cases, it may be challenging for plaintiffs to prove actual damages in connection with a company's violation of the MHMDA. However, plaintiffs' attorneys may still use the MHMDA to try and extract low-value settlements from companies that have obvious compliance issues as the cost of these low-value settlements may be cheaper than any resulting defense from the plaintiffs' claims.

In addition to the private right of action, this law also empowers the Washington attorney general to bring enforcement actions against the noncompliant companies. Noncompliance with MHMDA is a per se violation of the Washington Consumer Protection Act, RCW 19.86 carrying a civil penalty of not more than $7,500 for each violation. There is no cure period to remedy noncompliance that we see in most U.S. state privacy laws. As a result, "Regulated Entities" and "Small Businesses" under the MHMDA risk becoming the subject of an enforcement action for violating MHMDA from the first day it becomes effective.