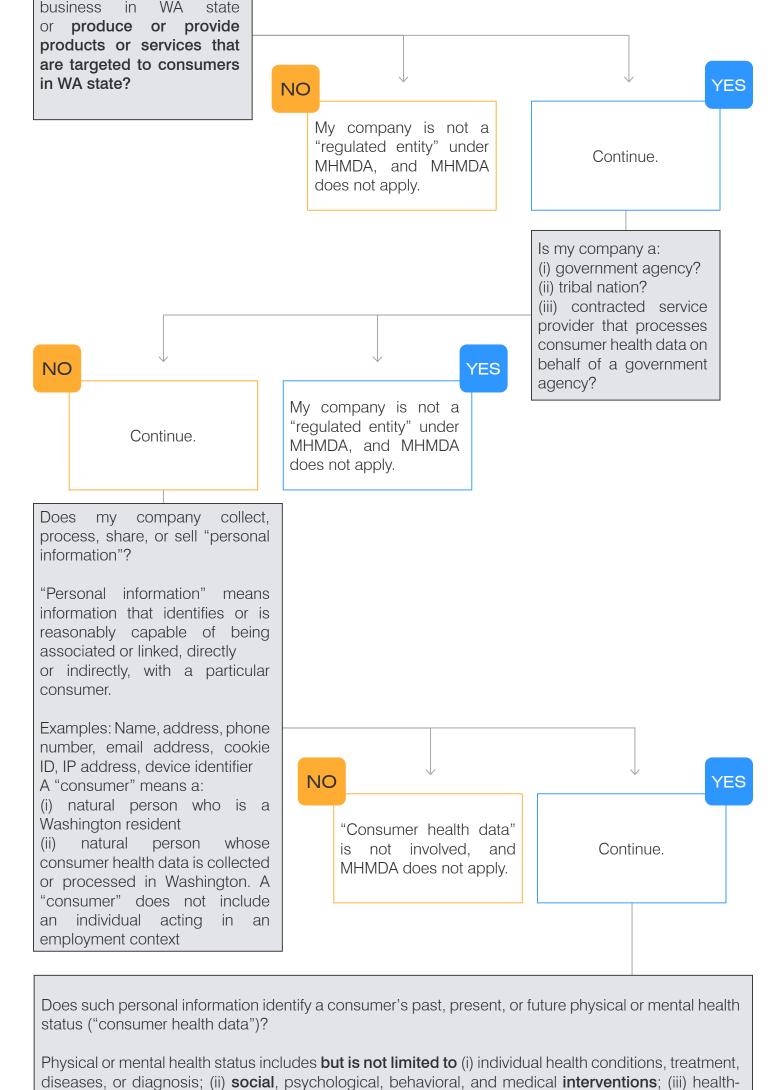
Washington's My Health My Data Act - A Roadmap for Compliance What is the new Washington My Health My Data Act (MHMDA)?

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?

Does my company conduct



data described in (i) through (xii) of this subsection that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).

"Health Care Services" means "any service provided to a person to assess, measure, improve,

related surgeries or procedures; (iv) use or purchase of prescribed medications; (v) bodily functions, vital signs, symptoms, or measurements of health status; (vi) diagnoses or diagnostic testing, treatment or medication; (vii) gender-affirming care information, (viii) reproductive or sexual health information, (ix) biometric data, (x), genetic data, (xi) precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies, (xii) data that identifies a consumer seeking "health care services," or (xiii) any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the

or learn about a person's mental or physical health..." **EXAMPLES**: Devices, applications, or websites collecting personal information such as blood pressure or pulse oximetry, fitness level, sleep, fertility, weight, body composition, meal selection (e.g., diabetic, dairy or gluten-free product), accessibility requirements (e.g., ramp access, shower seat, handicap stall), genetic and/or genealogical data, or biometric data. Companies offering connected fitness devices, glucose or blood pressure monitors, smart watches, or other connected devices (e.g., smart scales, smart refrigerators). Retailers of products to predict a consumer's health status or health care services such as: maternity clothing, sunscreen for "acne prone" skin, hair growth serum, vitamins or supplements for specific conditions, fertility test kits, glucose kits, DNA test kits, urinary tract infection tests,

Companies needing information about health conditions, surgical interventions, and prescription products before performing a service such as fitness trainers, wellness coaches, yoga studios,

spas, massage therapists, and skin care specialists.

NO

"Consumer health data" is not involved,

MHMDA does not apply.

gluten-free products, over-the-counter medications, or products such headache or indigestion treatments, menstrual or other hygiene products, incontinence supplies, joint braces, or orthotic

YES

YES

YES

must

This information is exempt under MHMDA. My company needs to separate information that is

exempt under MHMDA from consumer health data and take compliance steps with respect

My company is a

June 30, 2024.

MHMDA

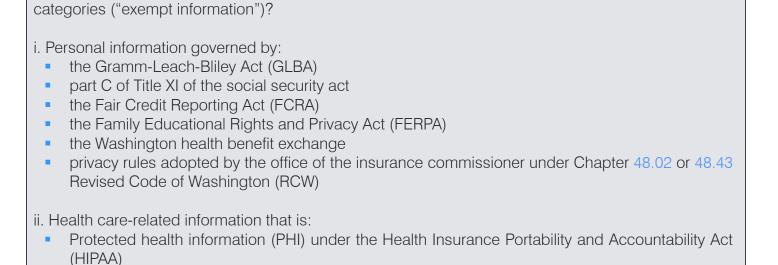
"small business" under

comply with MHMDA by

and

to consumer health data only.

Continue.



Does my company collect, process, share, or sell information that falls into any of the following

Personal data used or shared in research conducted in accordance with one or more of the requirements listed above under (ii) Information and documents created specifically for, and collected and maintained by: A quality improvement committee for purposes of RCW 40.70.510, 70.230.080, or 70.41.200;

 A hospital for reporting of health care-associated infections for purposes of RCW 43.70.056, a notification of an incident for purposes of RCW 70.56.040(5), or reports regarding adverse

• A manufacturer when collected, used, or disclosed for purpose specified in Chapter 70.02 RCW. Information and documents created for purposes of the federal health care quality improvement

Information that is de-identified as required by 45 C.F.R. Part 164 that is derived from the above-

Patient identifying information collected, used, or disclosed in accordance with 42 C.F.R. Part 2

Identifiable private information collected as part of human subjects research pursuant to the good

Health care information collected, used, or disclosed under Chapter 70.02 RCW;

clinical practice guidelines issued by the international counsel for harmonization

A quality assurance committee for purpose of RCW 74.42.640 or 18.20.390

The protection of human subjects under 21 C.F.R. Parts 50 and 56

A peer review committee for purposes of RCW 4.24.250

Patient safety work product for purposes of 42 C.F.R. Part 3

events for purposes of RCW 70.56.020(2)(b)

a. A HIPAA covered entity or business associate

act of 1986

NO

data,

1.

2.

Continue.

or sharing of consumer health

processes, sells, or shares

consumer health data of fewer

than 25,000 consumers?

and controls, sells

personal information is collected.

Identifiable private information for the protection of human subjects (45 C.F.R. Part 46)

listed health care-related information iii. Information originating from and intermingled to be indistinguishable with information under (ii) that is maintained by:

b. A health care facility or health care provider as defined in RCW 70.02.010 c. A program or a qualified service organization as defined by 42 C.F.R. Part 2

164.512 or that is part of a limited data set under 45 C.F.R. Section 164.514

and is approved, monitored, and governed by an institutional review board, human subjects research ethics review board, or a similar independent oversight entity that determines that the regulated entity or the small business has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

iv. Information used only for public health activities and purposes as described in 45 C.F.R. Section

vi. Personal information that is used to engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws

v. Identifiable data collected, used, or disclosed under Chapter 43.371 RCW or RCW 69.43.165

Does my company: (i) collect, process, sell, or share consumer health data of fewer than 100,000 consumers in a calendar year? (ii) derive less than 50% of gross revenue from the collection, processing, selling,

My company is a

March 31, 2024.

Prepare and implement a separate MHMDA notice linked on every page where

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

MHMDA

"regulated entity" under

comply with MHMDA by

and

must

NO

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

- 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
- 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!

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

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

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

- 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. Implement and maintain reasonable security practices to protect consumer 6. 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
- "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

What are the risks for not complying with MHMDA?

application of MHMDA, the broad spectrum of data that can qualify as

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

violating MHMDA from the first day it becomes effective. © 2024 Fenwick & West, LLP