PAUL HASTINGS

Stay Current

March 2024

Follow @Paul_Hastings

Biometrics Litigation Update: Washington Is Poised to Become a New Frontier for Private Litigants

By Adam M. Reich & Jeremy Berkowitz

In just a few short weeks, a new front may emerge for biometrics litigation in the United States. On March 31, 2024, the My Health My Data Act ("MHMDA") will go into effect in Washington for most entities that conduct business or sell products in that state (MHMDA goes into effect on June 30, 2024, for small businesses). MHMDA is a comprehensive privacy bill that focuses exclusively on protecting the processing of "consumer health data," but it uniquely includes "biometric data" among its regulatory focus. While Washington has a separate Biometric Privacy Law, Wash. Rev. Code § 19.371.010 et seq., MHMDA will be the only law in Washington that provides a private right of action relating to biometric privacy.

How is MHMDA Different than HIPAA?

Although MHMDA focuses on consumer health data, as we detailed previously, many of MHMDA's provisions go beyond the regulation of protected health information ("PHI") by the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). This is intentional, as Washington's legislators expressly intend MHMDA to supplement HIPAA, writing in the Act itself:

> Washingtonians expect that their health data is protected under laws like . . . HIPAA. However, HIPAA only covers health data collected by specific health care entities, including most health care providers. Health data collected by non-covered entities, including certain apps and websites, are not afforded the same protections. [MHMDA] works to close the gap between consumer knowledge and industry practice by providing stronger privacy protections for all Washington consumers' health data.[1]

Who Needs to Pay Attention to MHMDA Right Now?

Any legal entity that conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington, is subject to the MHMDA if the entity also "determines the purpose and means of collecting, processing, sharing, or selling consumer health data."[2] There are no minimum requirements for consumer base, revenue, or quantity or quality of processed data to meet the broad requirements of a regulated entity under MHMDA.

As used in MHMDA, the terms collecting, processing, sharing, and selling have the following meanings:

- "Collecting" means buying, renting, accessing, retaining, receiving, acquiring, inferring, deriving, or otherwise processing consumer health data in any manner.[3]
- "Processing" broadly means carrying out any operation on consumer health data.
- "Sharing" generally means releasing, disclosing, disseminating, divulging, making available, providing access to, licensing, or otherwise communicating consumer health data to a third party or affiliate.[4] Exceptions include disclosures to (i) processors, with the consumer's knowledge, in order to provide goods or services in a manner consistent with the purpose for which the consumer health data was collected; (ii) third parties, as part of a merger, acquisition, bankruptcy, or other asset transaction, which comply with MHMDA; and (iii) third parties with whom the consumer has a direct relationship and where the consumer has consented to the third party receiving the data, provided some additional identified requirements are satisfied.[5]
- "Selling" generally means exchanging consumer health data for money or any other valuable consideration, unless the exchange is: (i) to a third party, as part of a merger, acquisition, bankruptcy, or other asset transaction; or (ii) to a processor, as disclosed to the consumer, consistent with the purpose for which the consumer health data was collected.[6]

Government agencies, tribal nations, and contracted service providers that process consumer health data on behalf of a government agency are exempt from MHMDA's regulations.[7] Covered Entities and Business Associates under HIPAA are also exempt with respect to the collection and processing of PHI.

What Consumer Health Data Does MHMDA Regulate?

MHMDA regulates "***personal information that is linked or reasonably linkable to a consumer that identifies the consumer's past, present, or future physical or mental health status[,]" including biometric data***.[8] As used in MHMDA, biometric data means "data that is generated from the measurement or technological processing of an individual's physiological, biological, or behavioral characteristics and that identifies a consumer, whether individually or in combination with other data."[9] Beyond fingerprints, face prints, handprints, and eye imagery, the biometric data regulated by MHMDA includes vein patterns, voice recordings, as well as keystroke or gait patterns and rhythms that contain identifying information.[10]

The Washington State Attorney General's Office recently updated guidance regarding MHDMA, advising that regulated consumer health data also includes any data that can infer a consumer's "past, present, or future physical or mental health status." Thus, if an entity could draw inferences about an individual's health from the purchase of certain products, such as a retailer calculating pregnancy probability based on shopper purchase behavior, then that entity would come within the ambit of MHMDA.

What Does MHMDA Require Effective March 31, 2024

MHMDA includes many provisions around the processing of consumer health data that are now standard in state and global privacy laws. Organizations must provide ***notice of the types of data they are collecting and how they are processing it***. They must also ***offer individuals the right to access and delete consumer health data***. Further still, MHMDA ***prohibits the sale of consumer health data without written authorization from consumers***.

Consumer Health Data Privacy Policy

MHMDA requires each regulated entity to "prominently publish a link to its consumer health data privacy policy on its homepage."[11] That privacy policy must "clearly and conspicuously disclose[]" what types of consumer health data are collected, the purposes for the collection, how the data will be used, sources of the collected data, categories of data that may be shared and with whom, and how consumers can exercise specified rights regarding their health data, such as the right to withdraw consent.[12]

MHMDA prohibits, without notice and obtaining consumer consent: (i) the collection, use, or sharing of categories of consumer health data not identified in an entity's privacy policy; (ii) the collection, use, or sharing of identified categories of consumer health data for purposes not identified in the privacy policy; and (iii) the contracting with a processor to process consumer health data in a manner inconsistent with the privacy policy.[13]

Consumer Consent

MHMDA requires entities to obtain consumer consent before collecting or sharing consumer health data, unless doing so is necessary to provide a product or service that the affected consumer has requested from the regulated entity.[14] To obtain consumer consent, regulated entities must provide a request for consent, which "clearly and conspicuously disclose[s]:" the subject categories of consumer health data; the purpose for the collecting or sharing, including the specific ways that the consumer health data will be used; the categories of entities with whom the consumer health data is shared; and how the consumer can withdraw consent for future collection or sharing of the consumer's health data.[15]

Consumer Rights

MHMDA provides for six (6) consumer rights relating to their health data:

1. Right to confirm whether a regulated entity is collecting, sharing, or selling consumer health data concerning the consumer;

2. Right to access any consumer health data collected, shared, or sold by a regulated entity;

3. Right to receive a list of all third parties and affiliates with whom the regulated entity has shared or sold the consumer health data, and an email address or other online mechanism for the consumer to contact these third parties;

4. Right to withdraw consent for the collection and sharing of consumer health data;

5. Right to deletion of consumer health data upon request; and

6. Right to appeal any refusal by the regulated entity to take action on a request.[16]

The regulated entity must provide a secure and reliable means for consumers to exercise their rights, and explain the method in the privacy policy.[17] The prescribed method must take into account the ways in which consumers normally interact with the entity and have a manner to authenticate the identity of the requestor, other than requiring the consumer to create a new account.[18] If a regulated entity is unable to authenticate the request using commercially reasonable efforts, it is not required to comply with a consumer request and may seek additional information reasonably necessary to authenticate the consumer and the consumer's request.[19]

The timeline for a regulated entity to comply with authenticated consumer requests is within 45 days of receipt of the request, though the response period may be extended once by an additional 45 days when reasonably necessary.[20] The regulated entity may not charge the requesting consumer for requested information, unless the consumer makes requests that are manifestly unfounded, excessive (*i.e.*, more than twice per year), or repetitive.[21]

If a regulated entity receives a consumer request to delete consumer health data, it must: (i) delete the health data from its records, including its network and archive or backup systems; and (ii) notify all affiliates, processors, contractors, and other third party recipients of the consumer's health data of the deletion request.[22]

MHMDA also requires regulated entities to establish a "conspicuously available" ***appeals process*** for consumers to appeal any refusal by the entity to take action on consumer requests.[23] In the event that an entity denies an appeal, it must provide the consumer a method to contact the state attorney general to submit a complaint.[24]

Data Security

In addition to the foregoing, ***MHMDA requires reasonable security practices*** relating to consumer health data, including restricted access, and establishing, implementing, and maintaining administrative, technical, and physical data security practices that, at minimum, satisfy the reasonable standard of care within the entity's industry for protecting confidentiality, integrity, and accessibility of consumer health data.[25]

Restrictions on Consumer Health Data Sale Rights

MHMDA requires regulated entities to obtain signed consumer authorizations to sell consumer health data, separately and distinctly from the consent obtained to collect or share consumer health data.[26] To be effective, the authorization must meet various enumerated requirements, including that it be written in "plain language"; specifically identify what consumer health data will be sold, who will be involved in the transaction(s), and the purpose of the transaction(s); and have the affected consumer's signature and date of signing.[27]

Entities are required to retain copies of all valid authorizations for sale of consumer health data for six (6) years from the latter of the date of its signature or the date when it was last in effect.[28]

What are the Pathways to Enforcement of MHMDA?

Both ***the government and private litigants*** are empowered to bring suit to remedy MHMDA violations. All matters covered by MHMDA are statutorily deemed "matters vitally affecting the public interest" and all statutory violations are expressly considered unfair or deceptive acts in trade or commerce and an unfair method of competition, subject to Washington's Consumer Protection Act, chapter 19.86 RCW ("CPA"). The CPA permits authorized injured persons to bring a civil action to enjoin further violations and recover actual damages sustained, costs of the suit, including a reasonable attorney's fee, and 3x treble damages up to a maximum of $25,000.[29]

Unique from other privacy laws, MHMDA defines "consumers" to include non-state residents, acting in an individual or household context (rather than an employment context), whose consumer health data is collected in Washington.[30] This may, in turn, lead to MHMDA litigation in multiple jurisdictions outside of Washington.

Organizational Planning for MHMDA

Entities that conduct business in Washington, or produce or provide products or services targeted to consumers in Washington, should take a proactive approach to MHMDA in the weeks ahead. This may include:

- Assessing collected, processed, and stored personal data, including through a mapping exercise assisted or overseen by experienced privacy professionals;
- Evaluating existing policies, websites, disclosures, consent mechanisms, storage procedures, and any existing compliance programs against MHMDA's requirements;
- Analyzing contracts with third parties relating to data sharing, processing, and selling to ensure consistency with MHMDA;
- Working with experienced counsel to revise or prepare MHMDA-compliant notices, disclosures, policies, consents, and, as appropriate, training materials for personnel;
- Appraising existing insurance policies to determine whether there are gaps in coverage for potential litigation claims under MHMDA; and
- Consulting with experienced legal professionals regarding existing health privacy laws and biometric privacy laws, and related court opinions that may be persuasive to Washington Courts evaluating legal claims under this new statute.

While it is unknown whether litigation will immediately follow on or after March 31, 2024—indeed, it took several years after the enactment of Illinois' Biometric Information Privacy Act ("BIPA") for the plaintiffs' bar to take advantage of a similarly broad private right of action and file proliferative lawsuits, and then still more time for the Illinois Supreme Court to first weigh in on a threshold question pertaining to the statute—entities subject to MHMDA that take steps now to ensure compliance will be much better positioned if litigation does occur.

Paul Hastings is uniquely positioned to aid in the review and revision of data collection and retention practices and policies, assess and design effective compliance programs, and defend companies in privacy litigation matters by employing an industry-leading, cross-disciplinary team of legal and regulatory experts, and deft litigators experienced with biometric and health privacy laws.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact either of the following Paul Hastings lawyers:

Chicago

Adam M. Reich
1.312.499.6041
adamreich@paulhastings.com

Washington, D.C.

Jeremy Berkowitz
1.202.551.1230
jeremyberkowitz@paulhastings.com

Paul Hastings LLP

Stay Current is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership.

[1] Wash Rev. Code § 19.373.005(2)

[2] Wash Rev. Code § 19.373.010(23)

[3] Wash Rev. Code § 19.373.010(5)

[4] Wash Rev. Code § 19.373.010(27)

[5] Wash Rev. Code § 19.373.010(20)

[6] Wash Rev. Code § 19.373.010(26)

[7] Wash Rev. Code § 19.373.010(23)

[8] Wash Rev. Code § 19.373.010(8)

[9] Wash Rev. Code § 19.373.010(8)

[10] *Id*.

[11] Wash Rev. Code § 19.373.020(1)(b)

[12] Wash Rev. Code § 19.373.020(1)(a)

[13] Wash Rev. Code § 19.373.020(1)(c)-(e)

[14] Wash Rev. Code § 19.373.030

[15] *Id*.

[16] Wash Rev. Code § 19.373.040(1)(a)-(c), (h)

[17] Wash Rev. Code § 19.373.040(1)(d)

[18] *Id*.

[19] Wash Rev. Code § 19.373.040(1)(e)

[20] Wash Rev. Code § 19.373.040(1)(g)

[21] Wash Rev. Code § 19.373.040(1)(f)

[22] Wash Rev. Code § 19.373.040(1)(c)

[23] Wash Rev. Code § 19.373.040(1)(h)

[24] *Id*.

[25] Wash Rev. Code § 19.373.050

[26] Wash Rev. Code § 19.373.070

[27] *Id*.

[28] *Id*.

[29] Wash Rev. Code § 19.86.090

[30] Wash Rev. Code § 19.373.010(8)