SQUIRE PATTON BOGGS

Privacy World

Keeping you informed on the evolving law on data privacy, security and innovation.

Are you Ready for Washington and Nevada's Consumer Health Data Laws?

By Alan Friel, Kyle Fath, Niloufar Massachi & Gicel Tomimbang on April 17, 2024

Washington's My Health My Data Act ("MHMDA") and **Nevada's SB 370** ("NV CHD Law") (collectively, "CHD Laws") went into effect at the end of last month, on March 31, 2024 (as many

know, MHMDA's geofencing prohibition went into effect last summer). Unlike the Health Insurance Portability and Accountability Act ("HIPAA"), a federal law which governs privacy and security in traditional healthcare settings, CHD Laws regulate "consumer health data" or "CHD"– a very broadly defined term as we discuss below and in a **prior post** – collected by companies in a broad swath of health and non-health related industries alike. Even ancillary purposes like providing accessibility accommodations and defending personal injury claims are enough to trigger the laws. CHD Laws impose restrictions and obligations on regulated entities far more burdensome than state consumer privacy laws, many of which already regulate some of the same health data, and unlike those general consumer privacy laws are not proposed to be preempted by the potential federal **America Privacy Rights Act**.

As such, compliance programs that businesses may have developed to comply with state consumer privacy laws, such as the California Privacy Protection Act ("CCPA"), will not be sufficient to address the requirements of the CHD Laws, though they can be leveraged such as for consumer rights request and processor management. There are some material differences beyond the scope of the data regulated. For example, businesses must add another website footer link (and potentially elsewhere, such as in mobile apps) and post a separate privacy policy applicable to the processing of CHD. The facilitation of consumer rights must be CHD-specific, for example providing the right to delete just CHD, rather than all personal information. Moreover, businesses that have CHD use cases not within narrow exceptions (e.g., as necessary to provide a requested product or service), which differ somewhat as between the two laws, will have to grapple with the foreboding consent and authorization requirements which, in some cases, could result in subjecting visitors or customers to a litany of notices and pop-ups in an environment already plagued by what some dub as "consent fatigue."

In view of the private right of action under Washington's law in particular, regulated entities should evaluate their data practices to determine if they collect and process CHD and address applicable compliance obligations as soon as possible:

- Do you collect CHD subject to the Washington or Nevada laws as a controller of that data, (a "regulated entity")? If so,
- Do you have a compliant privacy policy and consumer rights process?
- If you collect CHD outside of narrow exceptions, do you sufficiently obtain the appropriate level of consent or authorization?
- Are your CHD processor agreements sufficient?

1. ***Jurisdictional Scope***

Key Takeaway: The jurisdictional scope of the CHD Laws is broad, resulting in extraterritorial applicability. They apply to entities conducting business in Washington and Nevada in some capacity (notably, though, governmental entities and companies acting on behalf of governmental entities are not "regulated entities"). Washington provides qualifying "small businesses"[1] an additional three months (until June 30, 2024) to comply with MHMDA requirements, but Nevada does not provide such a delay in effectiveness as to small businesses. Further, the CHD Laws apply to the CHD of both residents and non-residents whose CHD is collected in-state (subject to additional criteria in Nevada), as discussed in the next takeaway.

The definitions for "regulated entity" and "consumers" under the CHD Laws result in the CHD Laws having a very broad scope. The CHD Laws apply to legal entities (excluding government entities and their contractors) that conduct business activities in Washington and/or Nevada, OR produce or provide products or services targeted to consumers in those states, AND that alone or jointly with others determine the purpose and means of collecting, processing, sharing or selling of CHD. Of note, the Washington CHD Law delays the compliance date for "small businesses" from March 31, 2024 to June 30, 2024. The Washington CHD Law defines "small business" as "a regulated entity that satisfies one or both of the following thresholds: (a) [c]ollects, processes, sells, or shares consumer health data of fewer than 100,000 consumers during a calendar year; or (b) [d]erives less than 50 percent of gross revenue from the collection, processing, selling, or sharing of consumer health data, and controls, processes, sells, or shares consumer health data of fewer than 25,000 consumers." The Nevada CHD Law does not have carve outs for small businesses.

Additionally, the CHD Laws apply to the data of "consumers", which are residents and non-residents whose CHD is collected in the applicable state, but excluding in an employment context and governmental contexts. Specifically, Washington defines a "consumer" as "(a) a natural person who is a Washington resident; or (b) a natural person whose consumer health data is collected in Washington" who is "act[ing] in an individual or household context" and not in an employment context. In Nevada, a "consumer" is "a natural person who has requested a product or service from a regulated entity and who resides in [Nevada] or whose consumer health data is collected in [Nevada]" excluding persons "acting in an employment context or as an agent of a governmental entity." As such, the definition of consumer under the NV CHD Law is narrower in that it additionally requires the individual to have requested a product or service from the regulated entity, though not necessarily a product or service for which the CHD is collected.

2. ***Broad Definitions of Consumer Health Data (though, Washington's is broader)***

Key Takeaway: The definition of "consumer health data" under the CHD Laws is immensely broad and applies to data that, under existing privacy laws, may not even be considered health data or otherwise sensitive data. .

The CHD Laws are expansive, impacting businesses with CHD, which is data that "is linked or reasonably linkable to a consumer and identifies past, present or future physical or mental health status" (Washington) or "personally identifiable information that is linked or reasonably capable of being linked to a consumer and that a regulated entity uses to identify the past, present or future health status of the consumer" (Nevada). This includes not only health conditions (conditions or status in Nevada), treatment (Washington only), diseases or diagnosis, but also bodily functions, vital signs, symptoms and health measurements (Washington only), and information regarding seeking health-related services, including precise location that could indicate an attempt to receive health services or supplies, and inferences about physical or mental health status extrapolated from non-health data, including inferences.

Data that meets certain deidentification standards under the CHD Laws, will no longer be CHD. However, the collection of CHD to create deidentified data will still be subject to the CHD Laws.

3. ***HIPAA Exemptions***

Key Takeaway: The HIPAA exemptions under the CHD Laws are different, and under MHMDA, regulated entities may still have MHMDA obligations as to non-PHI CHD that they maintain.

Although the NV CHD Law provides a blanket exemption for businesses that must comply with HIPAA, MHMDA HIPAA exemptions are narrower, applying only to PHI and PHI-derived data (i.e., sourced from PHI or intermingled to be indistinguishable from PHI). Thus, in Washington, HIPAA covered entities may have obligations with respect to non-PHI in their systems that qualifies as CHD.

4. ***Consumer Health Data Privacy Policy and Rights Requests***

Key Takeaway: The CHD Laws require publication of a CHD privacy policy detailing a regulated entity's practices with respect to CHD. The CHD privacy policy must include certain enumerated provisions and be accessible via a footer link on the regulated entity's website and potentially other places like mobile app menus. The MHMDA-required disclosures in the CHD privacy policy may not be intermingled with privacy disclosures required by non-MHMDA laws, at least according ***to non-binding guidance by the Office of the Attorney General of Washington****, seemingly necessitating at least a separate MHMDA privacy policy.*

In Washington, the CHD privacy notice must include the following information: (i) the categories of CHD collected and the purpose for which the data is collected, including how the data will be used; (ii) the categories of sources from which the CHD is collected; (iii) the categories of CHD that is shared; (iv) a list of the categories of third parties and a list of specific affiliates with which the regulated entity shares the CHD; and (v) how a consumer can exercise the rights provided in MHMDA. Under MHMDA, the CHD privacy policy must not contain additional information not required by MHMDA, meaning that the substance of the Washington CHD privacy policy may not be intermingled with privacy disclosures required by non-MHMDA laws and regulations, such as disclosures required under the Nevada CHD Law, HIPAA, and various state consumer privacy laws.[2] However, it would seem that a CHD notice could be a section of a broader policy if directly linked to and it could have Washington and Nevada subsections.

In Nevada, the CHD privacy policy must, in addition to the above, include: (i) the manner in which CHD will be processed; (ii) the process by which the regulated entity notifies consumers of material changes to the policy; (iii) whether a third party may collect CHD over time and across different Internet websites or online services when the consumer uses any Internet website or online service of the regulated entity; and (iv) the effective date of the CHD privacy policy. In Nevada, regulated entities may also (but do not have to) disclose the process, if any such process exists, for a consumer to review and request changes to any of his or her CHD that is collected by the regulated entity.

Regulated entities must receive and process consumer rights requests, including requests to exercise the right to:

- confirm whether a regulated entity is collecting, sharing, or selling CHD;
- access to CHD, including a list of all third parties and affiliates with whom the regulated entity has shared or sold the CHD;
- withdraw consent for the regulated entity's collection and sharing of CHD; and

- have consumer health data deleted (with CCPA-like notification and clawback requirements with respect to sharing recipients).

Importantly, rights are CHD-specific and companies that "over" comply with the consumer rights provisions may risk violating the prohibition against unlawful discrimination in the CHD Laws (e.g. by deleting all personal information rather than just CHD).

See our **prior blog post** for further requirements regarding treatment of consumer rights under MHMDA.

5. ***Data Processing Agreements Applicable to CHD Processing***

Key Takeaway: The CHD Laws require regulated entities and their processors to enter into data processing agreements ("DPA"). Those with DPAs that meet state consumer privacy law requirements will meet the DPA requirement of CHD Laws.

The CHD Laws obligate regulated entities and their processors to enter into DPAs that set forth the parties' obligations as to the CHD that is being processed pursuant to the business relationship between the parties. This applies even if collection of CHD is necessary to respond to a request (e.g., provide a disability accommodation) and not otherwise used. Notably, the CHD requirements for DPAs are less stringent than what is required currently under state consumer privacy laws. Therefore, businesses with DPAs that comply with such laws should not need to make changes to their DPAs to address requirements of the CHD Laws.

6. ***Consents for Collection and Sharing; Authorizations for Sales***

*Key Takeaway: As described in our **prior post**, the CHD Laws require regulated entities to obtain the data subject's separate and distinct consents prior to collecting and/or sharing of CHD, as well as the data subject's separate and distinct valid signed authorization prior to selling or offering to sell CHD. The content and procedural requirements for consents are exacting, and even more burdensome for sale authorizations.*

There are exceptions to the consent requirement for collection and sharing, but the exceptions are quite limited. Other exceptions can be found in carve outs in the definitions of sharing and selling. These exceptions and carve outs differ as between the laws and are not well crafted. Both laws permit collection and sharing without consent to the extent necessary to provide a product or

service that the consumer to whom such consumer health data relates has requested. Washington also exempts from its collection and sharing consent requirements uses where the collection and sharing is carried out 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. The Nevada law lacks such an exception, but exempts from consent to sharing requirements disclosures required or authorized by law, and clarifies that various types of disclosure are not sales. For instance, Nevada, unlike Washington, carves out from the definition of sales transfers necessary to provide requested products or services and the facilitation of consumer requests, transfers to affiliates and transfers of data a consumer made publicly available by unrestricted mass media. Washington carves out of the definition of sharing (and thus presumably of sale, which is a more narrow form of transfer) disclosures to a third party with which the consumer has a direct relationship when the disclosure is for purposes of providing a product or service, the transferor maintains ownership and control of the CHD and the third party limits its use to the collection purpose. A transfer as part of a qualifying merger, asset sale or change of control is carved out of the definition of sharing in Washington, and from the definition of sale in Nevada, but Nevada specifies that the transferor's obligations are assumed by the transferee. Disclosure to a qualifying processor for permitted purposes is carved out of the definition of sharing under the Washington law from the definition of sale under the Nevada law.

The CHD Laws define "sale" as the exchange of CHD for monetary or other valuable consideration, but do not clarify the bounds of what qualifies as "other valuable consideration." As detailed further in **this post**, regulators in other jurisdictions (i.e., California) have interpreted "other valuable consideration" under state consumer privacy laws (i.e., the California Consumer Privacy Act) to mean non-monetary consideration that includes other benefits such as free or discounted advertising services,[3] or opportunities to advertise directly to customers of other companies participating in a marketing co-operative.[4]

As we discuss in a **prior blog post**, separate and detailed signed sale authorizations are required *for each purchaser*. Thinking through use cases it appears challenging or impossible to obtain authorizations in certain contexts. For example, given the number of players involved in the digital advertising ecosystem and otherwise in the context of cookies and digital advertising, it would appear to be virtually impossible to obtain the necessary authorizations if required to do so, and query if the signed writing requirement could be met. Accordingly, geo-blocking digital advertising and other activities that may constitute a CHD sale, if technically feasible, would be prudent.

7. ***Geofencing Restrictions***

Key Takeaway: The CHD Laws each prohibit geofencing within a certain radius (Washington = 2,000 feet or less, Nevada = 1,750 feet or less) of any person or entity that provides in-person health care services or products for purposes of: (1) identifying or tracking data subjects seeking in-person health care services or products; (2) collecting CHD; and/or (3) sending notifications, messages, or advertisements to data subjects related to their CHD or health care services or products. While the CHD Laws were not in effect until March 31, 2024, the geofencing restrictions of MHMDA have been in effect since July 23, 2023.[5]

The term "health care services" is not defined under the NV CHD Law, but is broadly defined under MHMDA ("any service provided to a person to assess, measure, improve, or learn about a person's mental or physical health"). When considered together with MHMDA's broad definition of CHD, businesses and activities not historically in scope of health-related laws may be in scope for the CHD Laws. Brick-and-mortar retailers and other businesses with in-person customers and visitors should carefully examine these use cases to understand the scope of their application.

Other states have also passed measures to protect CHD. Last year, Connecticut amended the Connecticut Data Privacy Act ("CTDPA") to designate CHD as a type of sensitive data. Like the Washington and Nevada CHD Laws, the CHD amendments to CTDPA, which went into effect on July 1, 2023, impose geofencing restrictions (1,750 feet or less) prohibiting geofencing around any mental health, reproductive, or sexual health facility for the purpose of identifying, tracking, collecting data from or sending any notification to a consumer regarding the consumer's health data. This is much narrower than the Washington and Nevada approaches. New York, which does not have a state consumer privacy law, likewise passed amendments to its general business law (N.Y. Gen. Bus. Law § 394-6), which became effective on July 2, 2023, to prohibit geofencing (1,850 feet or less) around any health care facility, other than a business's own health care facility, for the purpose of delivering advertising to consumers for the purpose of building consumer profiles, or to infer a consumer's health status, medical condition, or medical treatment.

8. ***DPIAs/Assessments***

Key Takeaway: The CHD-related CTDPA amendments require regulated businesses to conduct data protection assessments for processing of such data, as discussed more fully in ***here****. The CHD amendments to CTDPA went into effect on July 1, 2023, the same date as the rest of CTDPA. The CHD*

Laws do not explicitly require data protection assessments but given the breadth of the treatment of CHD and the robustness of the corresponding privacy and security obligations under MHMD and the NV CHD Law, as well as the growing sensitivity to health data generally, we recommend conducting a specific health data protection assessment as to use cases involving health data.

9. ***Enforcement***

Key Takeaway: Regulated entities that fail to comply with the requirements of the CHD Laws may face enforcement by the applicable state's attorney general. Additionally, MHMDA, but not the NV CHD Law, grants a private right of action. Notably, as of the date of this blog post, no actions have been filed under MHMDA's private right of action.

Violations of MHMDA are deemed a violation of Washington's Consumer Protection Act ("WCPA"), its UDAP/unfair competition law, and subject to its private right of action that allows consumers to recover actual damages (with the court's discretion to award treble damages), limited to $25,000, reasonable attorney's fees, and costs. Private litigants are also able to seek injunctive relief for violations of the WCPA. Courts also have discretion to award treble damages (based on actual damages), up to $25,000. Accordingly, it can be expected that the plaintiffs' bar will bring actions based on a broad interpretation of MHMDA, notwithstanding the difficulty they may have in trying to quantify actual damages. Though the lack of statutory damages may deter the plaintiffs' bar from filing cases, the availability of attorneys' fees and costs, as well as injunctive relief, may eventually embolden consumer advocates and plaintiffs' firms to bring suits and arbitration claims under MHMDA.

The CHD Laws are enforceable by the applicable state's attorney general, under each state's consumer protection law (e.g., WCPA as discussed above). The state attorneys general may investigate and prosecute claims under their respective laws, and seek injunctive relief as well as civil penalties.

10. **Conclusion**

The CHD Laws are broadly drafted to affect businesses' data practices pertaining to the health- and health-adjacent data of consumers within and beyond Washington's and Nevada's state borders. The CHD Laws are intended to reach businesses not regulated by HIPAA, not only in the digital health and wellness sector, but also in other industries including, for example, transportation, property management, hospitality, retail, and others that rely on in-person

interactions or visits (e.g., collection of CHD for disability accommodations, incidents and accidents on-premises, and in preparation for or in defense of legal claims and for related purposes), beauty (collection of CHD for personalized skincare recommendations) and health-related consumer products, and also businesses holding a mix of HIPAA and non-HIPAA-regulated data. Therefore, businesses should assess whether they have data qualifying as CHD in their custody and if so, conduct a gap analysis to identify where current compliance initiatives meet and fall short of the requirements of the CHD Laws, and promptly address any gaps to mitigate the risk of legal and regulatory scrutiny and private action.

We will continue to cover developments related to CHD Laws. For more information, contact the authors or your Squire Patton Boggs relationship attorney.

---

[1] Note under MHMDA, a "small business" is a type of regulated entity. RCW 19.373.010(28). Considering this, our references to "regulated entity" throughout this blog includes small businesses, except where noted otherwise.

[2] Washington Attorney General MHMDA FAQs, #4, **https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy**.

[3] **https://oag.ca.gov/system/files/attachments/press-docs/Complaint%20%288-23-22%20FINAL%29.pdf**.

[4] *People of the State of California v. DoorDash Inc.* (21 February 2024), **https://oag.ca.gov/system/files/attachments/press-docs/DoorDash%20Complaint.pdf**.

[5] FAQ #1, **https://www.atg.wa.gov/protecting-washingtonians-personal-health-data-and-privacy**.

Disclaimer: While every effort has been made to ensure that the information contained in this article is accurate, neither its authors nor Squire Patton Boggs accepts responsibility for any errors or omissions. The content of this article is for general information only and is not intended to constitute or be relied upon as legal advice.

Copyright © 2024, Squire Patton Boggs All Rights Reserved.