



Privacy & Cybersecurity Update

May 2023

Washington State Enacts My Health, My Data Act

In a time of increased telehealth and a sharper focus on healthcare-related privacy, the scrutiny and regulation of health and wellness data and practices continue to deepen, and the U.S. states are key players in this development. In a noteworthy example, on April 27, 2023, Washington state Governor Inslee signed the My Health, My Data (MHMD) Act into law. The MHMD Act will go into effect on March 31, 2024, for some larger organizations conducting business in Washington, and on June 30, 2024, for organizations that qualify as a “small business” under the law. The MHMD Act applies to a *far wider range* of entities than what are traditionally considered healthcare providers under federal law, like the Health Insurance Portability and Accountability Act (HIPAA).

Certain types of violations of the MHMD Act are considered “unfair trade practices” and are subject to enforcement by the Washington attorney general pursuant to the state’s Consumer Protection Act (CPA). Importantly, individuals can also bring a *direct action* against a covered business for actual damages they incur for violations of the CPA.

Consumer Health Data. The MHMD Act defines “consumer health data” broadly, and in a more expansive manner than under other traditional health care privacy laws. Specifically, it covers all “personal information that is linked or reasonably linkable to a consumer and that identifies the consumer’s past, present, or future physical or mental health status including data about physical or mental health status,” and enumerates several categories of such data, including the following related to an individual:

- health conditions, treatment, diseases, or diagnoses;
- health-related surgeries or procedures;
- social, psychological, behavioral, and medical interventions;
- use or purchase of prescribed medication;
- certain bodily functions, vital signs, symptoms, or measurements;
- diagnoses or diagnostic testing, treatment, or medication;
- gender-affirming care information;
- reproductive or sexual health information;
- biometric and genetic data;
- precise location information (within a radius of 1,750 feet) that could reasonably indicate a consumer’s attempt to acquire or receive health services or supplies;
- data that identifies a consumer seeking health care services; and
- any information that can associate or identify a consumer with these data sets that are derived or extrapolated from non-health information.

Under the law, the term “health care services” is broadly defined to mean “any service provided to a person to assess, measure, improve, or learn about a person’s mental or physical health.”

Scope of Applicability. As noted above, the MHMD Act applies to a broad range of organizations. In particular, the law applies to any “regulated entity” which is defined as any legal entity that (i) conducts business in the state or produces or provides products or services that are targeted to consumers in Washington; and (ii) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data. The law creates less onerous provisions for a “small business,”

which is defined as a regulated entity that satisfies one or both of the following thresholds: (i) collects, processes, sells, or shares consumer health data of fewer than 100,000 consumers during a calendar year; or (ii) derives less than 50 percent of gross revenue from collecting, processing, selling, or sharing of consumer health data, and controls, processes, sells, or shares consumer health data of fewer than 25,000 consumers.

The term “consumer” relates to Washington residents and other individuals in Washington state who have their health information collected by covered businesses.

Key Requirements. The MHMD Act states that it is unlawful for any person (not just a regulated entity or small business) to sell or offer to sell consumer health data concerning a consumer without first obtaining valid authorization from the consumer. The term “sell” means the exchange of consumer health data for monetary or other valuable consideration, and this phrase could arguably be interpreted as applying the disclosure of data derived from an organization’s website (e.g., web forms, cookies, pixels, and tags) to third-party service providers.

In addition, a regulated entity or small business may *not* collect any consumer health data except with “consent from the consumer for such collection for a specified purpose” or “[t]o the extent necessary to provide a product or service that the consumer to whom such consumer health data relates has requested.”

Similarly, neither a regulated entity nor a small business may release, disseminate, or otherwise disclose any consumer health data except (i) with consent from the consumer for such “sharing” that is separate and distinct from the consent obtained to collect consumer health data, or (ii) to the extent necessary to provide a product or service that the applicable consumer has requested. The MHMD Act sets forth several requirements for how such consent must be presented to a consumer and obtained.

Consumer Data Privacy Rights and Obligations.

Washington state consumers are given certain data privacy rights concerning their health data, including the following: (i) the right to confirm whether a regulated entity or a small

business is collecting, sharing, or selling their health data, (ii) the right to access their health data, including a list of third parties with whom their data was shared or sold, (iii) the right to withdraw consent from a business's collection and sharing their health data, and (iv) the right to have a business delete their health data.

As typical under other legal privacy frameworks, the MHMD Act requires businesses to implement processes to intake and respond to consumers' data privacy rights and provide a consumer with the right to appeal a business's privacy request response or decision. It also requires them to implement and maintain technical, physical, and administrative security controls to protect the confidentiality, integrity, and accessibility of consumer health data and execute written contracts with their service providers who process such data on their behalf.

Geofencing Restrictions. The MHMD Act also includes a restriction on geofencing. Specifically, it makes it unlawful for any person to implement a “geofence” around an entity that provides in-person health care services if the geofence is used to (i) identify or track consumers seeking health care services, (ii) collect consumer health data from consumers, or (iii) send notifications, messages, or advertisements to consumers related to their consumer health data or health care services. The term “geofence” is defined as “technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency, identification, wifi data, and/or any other form of spatial or location detection to establish a virtual boundary around a specific physical location, or to locate a consumer within a virtual boundary . . . that is 2,000 feet or less from the perimeter of the physical location.”

Exemptions/Exclusions. The law provides several key exemptions. Notably, it does not apply to personal data governed by specified federal and state laws, including HIPAA, the Gramm-Leach-Bliley Act, the Social Security Act, the Family Educational Rights and Privacy Act, as well as health-related Washington state laws. In addition, the MHMD does not apply to personal information used in public or peer-reviewed scientific research, publicly available information, deidentified data, or consumer health data used in an employment context.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky

216.566.5646

202.263.4126

Steve.Stransky@ThompsonHine.com

Certified Information Privacy Professional/Government (CIPP/G)

Certified Information Privacy Professional/United States (CIPP/US)

Thomas F. Zych

216.566.5605

Tom.Zych@ThompsonHine.com

Thora Knight

212.908.3971

Thora.Knight@ThompsonHine.com

Marla Izbicky

312.998.4253

Marla.Izbicky@ThompsonHine.com

This advisory bulletin may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgment of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions.

© 2023 THOMPSON HINE LLP. ALL RIGHTS RESERVED.