Bloomberg Law

Washington My Health My Data Act's Impact on Life Sciences Companies

*Contributed by **Christine Moundas**, **David Peloquin**, **Kevin Angle**, and **Elizabeth Whitkin**, Ropes & Gray*

March 2024

The deadline is quickly approaching to comply with Washington State's comprehensive new privacy law, the **My Health My Data Act** (the "Act"), the first state privacy law that specifically safeguards consumer health data. The **Act** will take effect on March 31, 2024 for "regulated entities" and on June 30, 2024 for "small businesses," as explored further in this article along with the new law's scope, applicability, and ensuing company obligations. Notably, the Act will apply to many life sciences companies and is enforceable through a private right of action, creating a risk of class action litigation related to potential violations.

The Act purports to close the enforcement gap for entities that collect significant amounts of health data but fall outside the jurisdiction of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended (**HIPAA**), such as pharmaceutical manufacturers, medical device manufacturers, health technology companies, and other life sciences companies.

Given the breadth of the Act's scope, pharmaceutical and medical device manufacturers of all sizes will likely be subject to the Act and will thus have to comply with its onerous requirements. In particular, the Act requires regulated entities and small businesses to develop a website privacy policy; secure opt-in consent prior to collecting or sharing identifiable consumer health data; obtain prior authorization to sell consumer health data; create mechanisms to track, respond to and grant consumer rights; implement reasonable security measures; ensure data protection agreements are in place with processors; and eliminate any geofences around entities that provide in-person health care services.

Scope

Entities Governed by the Act

The Act applies to “regulated entities” and “small businesses” that collect or process consumer health data in Washington or about Washington residents.

• “Regulated entities are defined as “any legal entity that (i) conducts business in Washington or produces, or provides products or services, that are targeted to consumers in Washington and (ii) alone or jointly with others, determines the purposes and means of collecting, processing, sharing or selling consumer health data.”

• “Small businesses” are defined as regulated entities that either “(i) collect, process, sell or share consumer health data of less than 100,000 consumers during a calendar year or (ii) derive less than 50 percent of gross revenue from the collection, processing, selling or sharing of consumer health data and control, process, sell or share consumer health data of less than 25,000 consumers.”

• A “consumer” is a Washington resident or an individual whose consumer health data is “collected” in Washington. The definition expressly excludes individuals acting in an employment context. Since the definition of a “small business” is tied to the number of individuals whose consumer health information is processed by an entity rather than a revenue threshold or similar, even some larger life sciences companies with limited contacts to Washington state may qualify as a “small business,” meaning that they have three more months to comply. Qualifying as a “small business,” though, will only delay, not limit, compliance requirements.

Distinct from other consumer state privacy laws, regulated entities and small business of all sizes, irrespective of revenue threshold, for-profit status or physical presence in the state, are governed by the Act if they meet the above criteria.

Data Governed By the Act

Of note, the Act regulates a broader swath of health data than HIPAA and many **other privacy laws** and protects categories of data that are only tangentially or incidentally related to health. Consumer health data is defined to include the following extensive, *non-exhaustive* types of information:

• Individual health conditions, treatment, diseases, or diagnosis;

• Social, psychological, behavioral, and medical interventions;

• Health-related surgeries or procedures;

• Use or purchase of prescribed medication;

• Bodily functions, vital signs, symptoms, or measurements of the information described herein;

• Diagnoses or diagnostic testing, treatment, or medication;

• Gender-affirming care information;

• Reproductive or sexual health information;

• Biometric data;

• Genetic data;

• Precise location information 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, which means any service provided to "assess, measure, improve, or learn about a person's mental or physical health" and includes, for example, use or purchase of medication; and

• Any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the aforementioned data categories that is derived or extrapolated from non-health information—such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning.

Exemptions

The Act does not contain any entity-level exemptions—e.g., for HIPAA covered entities, non-profit entities, etc. The Act does, however, **exempt** from its scope certain categories of data, including:

• Protected health information under HIPAA;

• Patient identifying information regulated by **42 C.F.R. Part 2** (the federal regulations on Confidentiality of Substance Use Disorder Patient Records);

• Identifiable private information under the Common Rule (**45 C.F.R. Part 46, Subpart A**);

• Identifiable private information otherwise collected as part of human subjects research pursuant to the good clinical practice guidelines issues by the international council for harmonization, as well **as 21** C.F.R. Parts 50 or 56;

• Information and documents created specifically for, and collected and maintained by FDA-regulated device or drug manufacturers, when collected, used or disclosed for certain purposes set forth in Washington's medical records privacy law—e.g., for treatment, payment, health care operations, public health purposes; and

• Data de-identified pursuant to the standards set forth in HIPAA

Compliance Obligations

The Act imposes several requirements on regulated entities and small business governing the method of collection and sharing of consumer health data. Many of these companies will either need to create or enhance their current data privacy and security compliance frameworks to comply with the Act.

Develop a Health Privacy Policy

Regulated entities and small businesses must publish a separate, prominent link on their websites to a **consumer health privacy policy** that discloses:

(i) The categories of consumer health data collected and the purposes of collection, including how the data will be used;

(ii) The categories of sources from which the consumer health data are collected;

(iii) The categories of consumer health data that are shared;

(iv) A list of the categories of third parties and specific affiliates with whom the entity shares consumer health data; and

(v) How consumers can exercise the rights granted under Act.

Additionally, as per **guidance** issued by the Washington Attorney General, the privacy policy may not contain additional information that is not required by the Act. While many regulated entities and small businesses have been required to draft a website privacy policy addressing substantially the same requirements under the **California Consumer Privacy Act** of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA), they will now have to, first, review their practices regarding the collection, use and disclosure of consumer health data and, second, create a distinct consumer health privacy policy disclosing such practices accordingly.

Obtain Opt-in Consent to Collect or Share Consumer Health Data

Pursuant to the Act, regulated entities and small businesses must obtain **opt-in consent to collect or share** consumer health data for purposes other than to provide the requested product or service; this is in contrast to other state privacy laws, which generally only require opt-out consent. The request for consent must disclose:

(i) The categories of consumer health data collected or shared;

(ii) The purpose of the collection or sharing of the consumer health data, including the specific ways in which the data will be used;

(iii) The categories of entities with whom the consumer health data are shared; and

(iv) How the consumer can withdraw consent from future collection or sharing of the consumer's health data.

These opt-in requirements may be burdensome for some regulated entities and small businesses, thereby forcing these companies to assess whether the collection or sharing of consumer health data should be limited to those which are necessary to provide a product or service. Alternatively, if it is determined that the consumer health data will be used for additional purposes, regulated entities and small businesses must implement or update their opt-in consent processes.

Obtain Authorization to Sell Consumer Health Data

Similar to the CCPA/CPRA, the Act broadly defines “sale” as the exchange of consumer health data for “monetary or other valuable consideration.” This definition may capture not only traditional data

sales but also the use of consumer health data for other marketing-related purposes, such as in the use of website analytics or advertising cookies and tracking technologies, particularly in light of **guidance** recently issued by the Federal Trade Commission regarding the use of online tracking technologies.

However, unlike the CCPA/CPRA, which requires that consumers be provided the opportunity to opt out, the Act requires that regulated entities and small businesses obtain a consumer's valid opt-in authorization to sell consumer health data, which, among other requirements, includes:

(i) The specific consumer health data to be sold and the purpose for such sale;

(ii) Contact information for the person(s) collecting, selling or purchasing the consumer health data;

(iii) The consumer's signature, and

(iv) A one-year expiration date.

Note that this authorization to sell consumer health data must be separate and distinct from the consent obtained to collect or share consumer health data, as discussed above. These authorization requirements may deter regulated entities and small businesses from selling consumer health data or using it for targeted marketing and analytics purposes.

Honor Broad Consumer Rights

Regulated entities and small businesses must grant consumers the right to:

(i) Confirm whether a regulated entity or small business collects, shares or sells its consumer health data, including providing a list of all third parties and affiliates with whom the regulated entity or small business has shared or sold such data and contact information;

(ii) Withdraw consent from the entity's collection and/or sharing of their consumer health data; and

(iii) Delete consumer health data, with no limitations.

Importantly, the Act provides more limited exemptions for responding to consumer rights than other state privacy laws, which may necessitate regulated entities and small businesses to update their current data subject rights request policies and practices.

Implement Security Measures

Regulated entities and small businesses must implement industry standard administrative, technical and physical **data security practices**, including ensuring that only the minimum amount of consumer health data is accessed by employees, processors or contractors to further the purposes for which the consumer provided consent or as necessary to provide a product or service the consumer has requested.

Establishing, implementing and maintaining reasonable administrative, technical and physical data security practices may be costly and time-intensive for regulated entities and small businesses that are not already subject to HIPAA's stringent security requirements. Additionally, while regulated entities and small businesses may have already been required to implement "reasonable security procedures" under the CCPA/CPRA, California has yet to issue regulations further defining these measures.

Enter Into Contracts With Service Providers

Regulated entities and small businesses must enter into service provider agreements with **processors**, which must include certain required security and privacy provisions, including, without limitation, limiting the actions the processor may take with respect to the consumer health data. Per the Act, a "processor" is "a person that processes [i.e., performs any operation or set of operations] consumer health data on behalf of a regulated entity or a small business."

While the Act does not prescribe exactly what must be included in the contracts, the Act does state that if a service provider does not adhere to the contractual obligations, it will be considered a regulated entity or small business subject to the Act's requirements.

Prohibit the Use of Geofencing

Effective July 23, 2023, regulated entities and small businesses must **prohibit the use of geofences**—e.g., digital location-based trackers that show ads according to the person's proximity to a designated location—around entities that provide in-person health care services when used to:

(i) Identify or track consumers seeking health care services;

(ii) Collect consumer health data from consumers; or

(iii) Send notifications, messages or ads to a consumer related to their health care data or health care services. Note that there is no consent exception for this geofencing prohibition.

Violations of the Act

Failure to comply with the Act **constitutes** an "unfair or deceptive act in trade or commerce and an unfair method of competition" under Washington's Consumer Protection Act and may result in civil penalties of up to $2,000 per violation and/or in private and class action litigation. In particular, the Act provides for a broad private right of action for violation of any of its provisions.

Additionally, in accordance with Washington's Consumer Protection Act, plaintiffs could recover actual damages, certain treble damages, costs of the lawsuit and attorney's fees. Given the high monetary upside for plaintiff's counsel, it is very likely that many lawsuits will be filed against regulated entities and small businesses for alleged noncompliance with the Act; although, unlike some privacy claims—such as the data breach cause of action under the CCPA/CPRA—there are not statutory damages available, meaning that plaintiffs must prove they were actually harmed by the alleged violation.

Key Takeaways

Pharmaceutical manufacturers, device manufacturers, and other life sciences companies that either do business in Washington or target products or services to Washington residents should urgently assess their data collection, use, disclosure, and processing practices to determine whether they collect consumer health data of Washington residents and/or otherwise process consumer health

data in Washington. These companies must create and implement an infrastructure to comply with the Act's stringent privacy and security requirements, which includes:

(i) Updating their privacy policies,

(ii) Creating a mechanism to secure opt-in consent to collect, sell or share consumer health data as well as authorizations to sell such data,

(iii) Implementing or revising consumer privacy right request processes,

(iv) Employing reasonable data security practices,

(v) Implementing or updating service provider agreements, and

(vi) Eliminating the use of geofencing.

*With assistance from **Elana Bengualid**, Ropes & Gray*