Akin®

Washington State Expands Privacy Protections for Health Data

May 25, 2023

Reading Time : **10 min**

By: John R. Jacob, Natasha G. Kohne, Jo-Ellyn Sakowitz Klein

On April 27, 2023, Washington Governor Jay Inslee signed the My Health My Data Act (the "Act") into law, establishing new limits on the collection, use and sharing of "consumer health data" and creating numerous compliance obligations for entities that are in scope. The Act will take effect on July 23, 2023 and specifies that compliance is mandated for most sections by March 31, 2024 generally and June 30, 2024 for small businesses. However, the Act's prohibitions on geofencing appear to take effect on July 23, 2023. Below, we have provided a summary of key aspects of the Act and outlined some steps potentially impacted entities may want to take.

Scope of the Act

The Act protects Washington residents and other natural persons whose "consumer health data" is collected in Washington, and specifies that "consumers" are natural persons acting in the individual or household context, however identified, including any unique identifiers, and does not include individuals acting in an employment context.[1] "Consumer health data" is defined broadly to include 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"[2] and includes information such as:

- Individual health conditions, treatment, diseases or diagnosis.
- Use or purchase of prescribed medication.
- Diagnoses or diagnostic testing, treatment or medication.

- "Biometric data," which is defined to include a broad range of identifiers such as voice recordings if "an identifier template can be extracted" and gait patterns or rhythms that contain identifying information.[3]
- Bodily functions and vital signs.
- "Genetic data," defined as "any data, regardless of its format, that concerns a consumer's genetic characteristics."[4]
- Social, psychological, behavioral and medical interventions.
- "Reproductive or sexual health information."[5]
- "Precise location information"[6]that could reasonably indicate a consumer's attempt to acquire or receive certain health services or supplies.
- Data that identifies a consumer seeking "health care services."[7]

The definition of consumer health data also includes a far-reaching category of "any information that a regulated entity or a small business, or their respective processor, processes to associate or identify a consumer with the data described in [the definition of consumer health data] that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning)."[8]

The Act provides several data-level exemptions including, but not limited to, exemptions for protected health information as defined under HIPAA,[9] publicly available information (which is excluded from the definition of "personal information"), certain personal information used for research in the public interest as well as identifiable private information for purposes of the federal policy for the protection of human research subjects (among other research-related data-level exemptions) and personal information governed by other privacy laws such as the Gramm-Leach-Bliley Act (and implementing regulations), the Fair Credit Reporting Act, and the Washington state health benefit exchange and applicable statutes and regulations.[10] The Act also does not apply to "deidentified data," which is defined as data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable consumer, or a device linked to such a consumer, so long as the regulated entity or the small business that possesses such data (a) takes reasonable measures to ensure that such data cannot be associated with a consumer, (b) publicly commits to process such data only in a deidentified fashion and not attempt to reidentify such data and (c) contractually

obligates recipients of such data to satisfy criteria described in (a)-(b).[11] Notably, the Act also includes a separate and more fulsome carve-out for data that is deidentified to the standard set forth in HIPAA.[12]

Additionally, the Act includes a couple of special circumstances exemptions, focused on information used for public health activities as well as on data is part of a HIPAA limited data set (which may be used or disclosed for research, public health, or health care operations purposes if certain conditions are met).[13]

The Act applies to "regulated entities," which are defined as "any legal entity that (a) [c]onducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington; and (b) alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data."[14] The Act also applies to certain "small businesses" and, based on the breadth of the definitions of "regulated entity" and "consumer," appears to include nonprofit organizations as well. However, the Act includes a few entity-level exemptions, as the definition of "regulated entity" does not include government agencies, tribal nations or contracted service providers when processing consumer health data on behalf of the government agency.[15] Unlike other state comprehensive privacy laws, there are no revenue or consumer data amount thresholds that will put businesses in scope.[16] The Act also includes exemptions for certain information maintained by HIPAA covered entities or business associates, or by health care facilities or health care providers as defined under Washington law.[17]

Key Requirements of the Act

The Act includes specific requirements for regulated entities that use concepts similar to those seen in the growing number of state comprehensive privacy laws, drawing inspiration from HIPAA and Federal Trade Commission (FTC) privacy regulation. Key requirements under the Act for regulated entities include:

- *Privacy Policy Requirements*. Regulated entities and small businesses are required to post a "Consumer Health Data Privacy Policy" (Privacy Policy) through a prominent link on its homepage. Such privacy policy must "clearly and conspicuously disclose[]" certain information to consumers, including the categories of consumer health data collected, purposes for the collection, how the data will be used, sources of the data,

how and with whom the data will be shared and how a consumer can exercise their rights under the Act.[18] Regulated entities are prohibited from collecting, using or sharing additional categories of consumer health data or for additional purposes not disclosed in the Privacy Policy without first disclosing the additional categories and purposes and obtaining the consumer's affirmative consent.[19]

- *Consent for Collection and Sharing*.[20] The Act sets limits on circumstances under which regulated entities and small businesses can collect and share consumer health information. Specifically, regulated entities and small businesses are prohibited from collecting consumer health data unless they obtain consumer consent "for such collection for a specified purpose" or the collection is necessary to provide a product or service requested by the consumer. Regulated entities and small businesses may also not share any consumer health data unless they have obtained consent from the consumer for such sharing "that is separate and distinct from the consent obtained to collect consumer health data" or the sharing is necessary to provide a product or service requested by the consumer.[21] Valid consent must meet certain requirements as specified under the Act.[22]
- *Authorization to Sell*[23] *Consumer Health Data*. The Act prohibits "any person"[24] from "selling" consumer health data without "valid authorization" from the consumer that is "separate and distinct from the consent obtained to collect or share consumer health data."[25] The Act sets out specific elements for what constitutes a "valid authorization" including, for example, that it must contain the specific elements of consumer health data that will be sold, the name and contact of the person purchasing the consumer health data, and a description of the purpose for the sale, including how the consumer health data will be gathered and how it will be used by the purchaser.[26]
- *Geofencing Prohibition*. The Act makes it unlawful for any person to implement a geofence[27] around an entity that provides in-person "health care services"[28] where such geofence is used to (a) identify or track consumers seeking health care services; (b) collect consumer health data from consumers; or (c) send notifications, messages or advertisements to consumers related to their consumer health data or health care services.[29]
- *Contracts with Processors*. Under the Act, a processor may only process consumer health data pursuant to a binding contract with the regulated entity or small business

and in a manner consistent with the instructions set forth in the contract.[30]

- *Consumer Rights*. The Act provides consumers with various rights similar to those available under state comprehensive privacy laws, state health information privacy laws, and HIPAA. Specifically, the Act provides consumers a right to (a) access their consumer health data, including to receive a list of all third parties and affiliates who receive their data; (b) withdraw consent to the collection or sharing of their health data; and (c) have their consumer health data deleted.[31] Notably, if a consumer requests to have their consumer health data deleted, the regulated entity must also delete the data from archives and backups, and notify all "affiliates, processors, contractors, and other third parties," who must also honor the request.[32]
- *Security Measures*. The Act requires that regulated entities and small businesses restrict access to consumer health data to only those employees, processors and contractors necessary to further the purposes for which the consumer provided consent or where necessary to provide the product or service.[33] Regulated entities and small businesses must also "[e]stablish, implement, and maintain administrative, technical, and physical data security practices that, at a minimum, satisfy reasonable standard of care within the regulated entity's or the small business's industry to protect the confidentiality, integrity, and accessibility of consumer health data appropriate to the volume and nature of the consumer health data at issue."[34]

Governmental Enforcement and Private Right of Action

The Washington State Attorney General may enforce violations through the state's Consumer Protection Act (CPA) and consumers have a private right of action to seek damages for violations of the law under the CPA.[35] The Act also establishes a joint committee to review enforcement actions, and that will create a report about the impact and effectiveness of the Act's enforcement provisions.[36]

Looking Ahead: Action Items for Impacted Entities

The Act imposes significant compliance obligations on businesses that are within its scope. Businesses should evaluate whether they are a regulated entity and assess the extent to which they can leverage current compliance with existing privacy laws. Specifically, ahead of the compliance deadline, affected entities may want to:

- Evaluate the extent to which any of the exemptions provided under the Act are relevant to the entity's operations.
- Implement a compliant privacy policy and update related internal policies and procedures, as needed to support the privacy policy as well as to comply with the Act more generally.
- Reassess privacy and security controls.
- Assess and address the impact on agreements with processors.
- Ensure that sufficient policies are in place to obtain and manage affirmative consent and valid authorizations, when appropriate.

If you have any questions, please contact a member of the Akin health regulatory or cybersecurity, privacy and data protection teams.

---

[1] H.B. 1155 (2023), Sec. 3(7).

[2] H.B. 1155 (2023), Sec. 3(8).

[3] H.B. 1155 (2023), Sec. 3(4).

[4] H.B. 1155 (2023), Sec. 3(13).

[5] H.B. 1155 (2023), Sec. 3(24).

[6] H.B. 1155 (2023), Sec. 3(19).

[7] H.B. 1155 (2023), Sec. 3(15).

[8] H.B. 1155 (2023), Sec. 3(8)(b)(xiii).

[9] "HIPAA" refers to the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and their implementing regulations (codified at 45 C.F.R. parts 160 and 164). *See* 45 C.F.R. § 160.103 (defining "protected health information").

[10] H.B. 1155 (2023), Secs. 3(8)(c), 3(18)(b), 12(1)(a).

[11] H.B. 1155 (2023), Sec. 3(10).

[12] H.B. 1155 (2023), Sec. 12(1)(a)(viii).

[13] H.B. 1155 (2023), Sec. 12(1)(c).

[14] H.B. 1155 (2023), Sec. 3(23).

[15] H.B. 1155 (2023), Sec. 3(23).

[16] See, e.g., H.B. 1155 (2023), Sec. 3(23).

[17] H.B. 1155 (2023), Sec. 12(1)(b).

[18] H.B. 1155 (2023), Sec. 4(1)(a).

[19] H.B. 1155 (2023), Sec. 4(1)(b)-(c).

[20] Note that "collect" and "share" are specifically defined under the Act.

[21] H.B. 1155 (2023), Sec. 5(1)(a)-(b).

[22] H.B. 1155 (2023), Sec. 5(1)(a)-(c).

[23] The Act defines "sell" as "the exchange of consumer health data for monetary or other valuable consideration." H.B. 1155 (2023), Sec. 3(26)(a).

[24] The Act defines "person" as "natural persons, corporations, trusts, unincorporated associations, and partnerships." H.B. 1155 (2023), Sec. 3(17).

[25] H.B. 1155 (2023), Sec. 9(1).

[26] H.B. 1155 (2023), Sec. 9(2).

[27] The Act defines "geofence" 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. For purposes of this definition, 'geofence' means a virtual boundary that is 2,000 feet or less from the perimeter of the physical location." H.B. 1155 (2023), Sec. 3(14).

[28] Note that "health care services" is defined broadly to include "any service provided to a person to assess, measure, improve, or learn about a person's mental or physical health, including but not limited to: (a) Individual health conditions, status, diseases, or diagnoses; (b) Social, psychological, behavioral, and medical interventions; (c) Health-related surgeries or procedures; (d) Use or purchase of medication;(e) Bodily functions, vital signs, symptoms, or measurements of the information described in this subsection; (f) Diagnoses or diagnostic testing, treatment, or medication; (g) Reproductive health care services; or (h) Gender-affirming care services." H.B. 1155 (2023), Sec. 3(15).

[29] H.B. 1155 (2023), Sec. 10.

[30] H.B. 1155 (2023), Sec. 8.

[31] H.B. 1155 (2023), Sec. 6(1)(a)-(c).

[32] H.B. 1155 (2023), Sec. 6(1)(a).

[33] H.B. 1155 (2023), Sec. 7(1)(a).

[34] H.B. 1155 (2023), Sec. 7(1)(b).

[35] H.B. 1155 (2023), Sec. 11 (specifying that a violation of the Act is an "unfair or deceptive act in trade or commerce and an unfair method of competition for the purpose of applying the consumer protection act, chapter 19.86 RCW").

[36] H.B. 1155 (2023), Sec. 13.

Categories

State Privacy Policy | Health Information Privacy & Security | HIPAA & HITECH