

# Employee Benefit Plan Review

## Beyond HIPAA and the State Consumer Privacy Laws: Washington State's New "My Health, My Data Act"

BY JAMI VIBBERT, NANCY L. PERKINS, GEORGE EICHELBERGER AND JASON T. RAYLESBERG

The State of Washington has taken a significant step toward increasing regulation in the United States governing personal health data, enacting the "Washington my health, my data act"<sup>1</sup> (the Act). The Act is intended to provide protection for consumer health data that currently is exempt from medical/health privacy laws, including the federal privacy regulations implementing the Health Insurance Portability and Accountability Act (HIPAA). As stated in the Act, "HIPAA only covers data collected by specific health care entities, including most health care providers. . . . This Act works to close the gap . . . by providing stronger privacy protections for all Washington consumers' health data."

The Act is actually broader in scope than this statement may suggest, however. It applies not only to health data about Washington State residents; it also applies to health data about a natural person that is "collected in Washington." So, if the collection happens while a person is in Washington State, it is covered. In this way, the Washington State law is broader in jurisdictional reach than most of the recently enacted, generally applicable state

consumer privacy laws, which define a "consumer" as a resident of the state.

The Act contains many elements that are common to the generally applicable state consumer privacy laws, including requirements for privacy notices/policies, data protection assessments, and responses to consumer requests for access to, or correction, deletion, or transfer of, their personal health data. But the Act has at least six elements that are notably distinct from the other state privacy laws, as outlined below.

The Act affects nearly all organizations that provide products or services to Washington consumers and others located in Washington

The Act has a comparatively broad jurisdictional scope. The Act applies to all "regulated entities," which are defined to include both for-profit and non-profit organizations (excluding government agencies, government contractors, and native American tribes) that (1) conduct business in Washington or produce or provide products or services that are targeted to consumers in Washington, and (2) alone or jointly determine the purpose and means of collecting and processing consumer health data. Unlike many of the other state privacy laws, the Act applies regardless of whether a business

collects data from a certain number of consumers or derives a certain percentage of its gross profits from the sale of data.

### **THE ACT DEFINES CONSUMER HEALTH DATA BROADLY**

The Act also establishes a broad definition of “consumer health data.” Under the Act, “consumer health data” is information that is linked or reasonably linkable to a “consumer” and relates to the consumer’s past, present, or future physical or mental health status. As stated in the Act, this includes (but is not limited to) genetic data, biometric data, information related to gender-affirming care, and data related to reproductive or sexual health, as well as data related to medical treatment, disease, and diagnosis generally.

### **THE ACT REQUIRES CONSENT FOR DATA COLLECTION**

Importantly, the Act prohibits regulated entities from collecting or sharing consumer health data without the express, affirmative consent of the consumer to whom the data pertains, unless the collection or sharing is necessary to provide a product or service that the consumer has requested. This affirmative consent must be obtained prior to the collection or sharing of the data and must contain specific disclosures to the consumer, including notice of how the consumer can withdraw consent for future collection or sharing. Notably, the consent must be separate (i.e., it cannot be consent to the entire privacy notice or policy), cannot be granted by hovering over or closing a piece of content, and cannot be obtained through dark patterns. However, consent is not required to share data with third parties for the purposes of providing the products or services to the consumer.

### **THE ACT REQUIRES AFFIRMATIVE, WRITTEN CONSUMER CONSENT FOR EACH SALE OF DATA**

The Act separately prohibits businesses from selling (exchanging for monetary or valuable consideration) consumer health data without obtaining consent. To be valid, such a consent (called an authorization) must be “separate and distinct” from the consumer’s consent to the collection of the data, and must, in plain language, state:

- (1) What specific consumer health data will be sold;
- (2) The name and contact information of the seller;
- (3) The name and contact information of the purchaser;
- (4) The purpose of the sale, including how the sold data will be gathered and used by the purchaser;
- (5) A statement that goods and services cannot be conditioned on the consumer’s consent;
- (6) The consumer’s right to revoke their consent;
- (7) The fact that the consumer’s information may be redisclosed by the purchaser and no longer be protected by the Act; and
- (8) An expiration date for the consent that expires one year from when the consumer signs the authorization.

A business must obtain a new authorization each time it seeks to conduct a separate sale of a consumer’s data.

### **THE ACT IS ENFORCEABLE THROUGH A PRIVATE RIGHT OF ACTION**

The Act includes a private right of action, allowing consumers to enforce their rights under the Act directly. The Act creates this private right of action by making a violation

of the Act an unfair or deceptive act or practice under the Washington Unfair Business Practices law, which allows for enforcement by either a consumer directly or by the Washington Attorney General.

---

## **The Act includes a private right of action, allowing consumers to enforce their rights under the Act directly.**

---

The Act prohibits any person from establishing a “geofence” around any in-person provider of health care services

The Act makes it unlawful for any person to establish a “geofence” – a virtual boundary marker – around any location that provides in-person health care services when the geofence is used to identify or track consumers seeking health care services, collect health data from consumers, or send messages to the consumers related to their health data or health care services.

A “geofence” is defined by the Act as any technology that establishes a virtual boundary around a specific physical location or to locate an individual within a virtual boundary. Health care services is also broadly defined as any service related to a person’s mental or physical health, including services related to the use or purchase of medication and services related to bodily functions, vital signs, symptoms, or measurements of health-related information. Notably, this prohibition has a broader scope than the other provisions of the Act; rather than only affecting “regulated entities,” this provision prohibits any “person” from establishing this kind of geofence around a health care provider.

The majority of the Act is scheduled to go into effect on March 31, 2024. However, small businesses will not be required to comply with the law until June 30, 2024. The prohibition against “geofencing” went into effect immediately upon the

enactment of the law on April 28, 2023. 🌐

### NOTE

1. <https://lawfilesexternal.wa.gov/biennium/2023-24/Pdf/Amendments/Senate/1155-S.E%20AMS%20ENGR%20S2826.E.pdf>.

The authors, attorneys with Arnold & Porter Kaye Scholer LLP, may be contacted at [jami.vibbert@arnoldporter.com](mailto:jami.vibbert@arnoldporter.com), [nancy.perkins@arnoldporter.com](mailto:nancy.perkins@arnoldporter.com), [george.eichelberger@arnoldporter.com](mailto:george.eichelberger@arnoldporter.com) and [jason.raylesberg@arnoldporter.com](mailto:jason.raylesberg@arnoldporter.com), respectively.

Copyright © 2023 CCH Incorporated. All Rights Reserved.  
Reprinted from *Employee Benefit Plan Review*, July-August 2023, Volume 77, Number 6, page 20–21, with permission from Wolters Kluwer, New York, NY, 1-800-638-8437, [www.WoltersKluwerLR.com](http://www.WoltersKluwerLR.com)

