Updates
June 07, 2023
The Wide Reach of the New Washington Privacy Legislation

This Update is the third installment of the ongoing series covering Washington state's new My Health My Data Act (the Act). Part 1 provided a high-level outline of the entities regulated under the Act and the corresponding requirements, as well as a detailed discussion on biometric data processing. Part 2 explored the consumer rights and business obligations created by the Act. In this installment, we address the Act's scope and its future implications for covered entities.

The original impetus for the Act was the protection of reproductive rights, and it was signed into law alongside several other pieces of legislation focused on providing abortion and gender-affirming protections. However, because of the broad and vague definition of "consumer health data" covered by the legislation and because it applies to a wide range of entities, the Act may reach much further than might be justified by its original purpose.

Scope of the Act

The Act opens with a reiteration of the Washington state constitution's explicit right to privacy and a statement on the limitations of privacy protections on health data under the Health Information Portability and Accountability Act (HIPAA). It is with these limitations in mind that the Act "works to close the gap" and provide stronger privacy protections for consumer health data.

In closing this gap, however, the Act's provisions could be interpreted to encompass: (1) data that is not typically thought of as health data, (2) entities that are not typically considered healthcare entities, and (3) people and organizations that are not conventionally considered to exist or operate within the state of Washington. Understanding the potentially broad scope of the Act requires close analysis of its terms, especially in its definition of "consumer health data" and the entities it regulates.

What Is "Consumer Health Data"?

The Act defines "consumer health data" to mean "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."

The Act elaborates on this definition by providing a lengthy but nonexhaustive list of data categories that qualify as relating to "physical or mental health status," namely (as quoted from the statute):

1. Individual health conditions, treatment, diseases, or diagnosis;
2. Social, psychological, behavioral, and medical interventions;
3. Health-related surgeries or procedures;
4. Use or purchase of prescribed medication;

5. Bodily functions, vital signs, symptoms, or measurements of the information described in this subsection (8)(b) [of the Act];
6. Diagnoses or diagnostic testing, treatment, or medication;
7. Gender-affirming care information;
8. Reproductive or sexual health information;
9. Biometric data;
10. Genetic data;
11. Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies;
12. Data that identifies a consumer seeking health care services; or
13. 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 (b)(i) through (xii) of this [definition] subsection that is derived or extrapolated from nonhealth information (such as proxy, derivative, inferred, or emergent data by any means, including algorithms or machine learning).

These data categories include data identifying consumers seeking "health care services," which is defined to include any service provided to "assess, measure, improve, or learn about a person's mental or physical health" and includes, among other things, the use or purchase of medication. Also included is nonhealth information from which a consumer's health status and data may be inferred or derived, which in turn may include data possessed by entities not traditionally thought of as providers or purveyors of healthcare products or services.

What Is Not "Consumer Health Data"?

The Act contains several exclusions for data collected under specified Washington state healthcare laws as well as certain federal laws, including the Gramm-Leach-Bliley Act (the GLBA, generally applicable to financial institutions), the Fair Credit Reporting Act (the FCRA, generally applicable to consumer information collected by consumer reporting agencies), the Family Educational Rights and Privacy Act (FERPA, generally applicable to educational data), and HIPAA.

Consistent with its intent of filling gaps in current privacy laws, the Act carves out from its application "Protected Health Information" (PHI) as defined under HIPAA's Privacy Rule as "individually identifiable health information" held or transmitted by a covered entity or its business associate. "Individually identifiable health information" means information, including demographic data, that relates to:

- The individual's past, present, or future physical or mental health or condition.
- The provision of healthcare to the individual.
- The past, present, or future payment for the provision of healthcare to the individual and that identifies the individual, or for which there is a reasonable basis to believe it can be used to identify the individual.

The HIPAA Privacy Rule specifies 18 identifiers, including name, address, birth date, and Social Security number, that can transform health information into personally identifiable PHI within the scope of the law.

The Act's carve-out of all PHI is a significant exclusion, as this will exclude most—but not necessarily all—consumer health information processed by HIPAA-covered entities, including healthcare providers, hospitals and clinics, pharmacies, health insurance entities, and more. Additionally, this exclusion will apply to a majority of the healthcare information processed by "business associates" under HIPAA, which are entities that

perform functions or activities on behalf of or provide certain services to a covered entity that involves access to PHI.

The Act contains other notable exclusions. For example, the definition of consumer health data does not include certain personal information used in public or peer-reviewed scientific, historical, or statistical research in the public interest.

The Act also excludes "deidentified data" and "publicly available information"—each as defined under the Act—from the definition of consumer health data. The law also appears to exclude data pertaining to employees or individuals acting in a business context by defining "consumer" to mean a "natural person who acts only in an individual or household context" and "does not include an individual acting in an employment context." This suggests that employee and business-to-business (B2B) data are not afforded the same protections as consumer health data.

Scope of Regulated Entities and Small Businesses

As noted in Part 2 of this series, the Act lays out a series of compliance obligations for regulated entities and small businesses. Unlike other state privacy laws, the Act does not set quantitative standards to determine which entities must comply. Instead, the Act generally applies to "regulated entities," which means "any legal entity that: (a) conducts 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." The definition of regulated entities excludes "government agencies, tribal nations, or contracted service providers when processing consumer health data on behalf of the government agency."

"Small business" means any "entity that (i) collects, processes, sells, or shares consumer health data of fewer than 100,000 consumers during a calendar year; and/or (b) derives 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."

Some provisions of the Act will not be effective for small businesses until June 30, 2024, whereas other regulated entities must comply with such provisions by March 31, 2024.

Takeaways

The Act may have a very broad reach and encompasses organizations that may not expect to be covered because they are not typically considered to be healthcare-related. Due to the wide scope of the Act and its impending effective dates, we encourage companies to promptly review the data they may "collect" or "process," consider whether it may qualify as consumer health data under the Act, and, if so, evaluate their privacy practices to ensure they meet the requirements of the Act.

We will continue to monitor developments related to the law's implementation and publish corresponding analyses and updates.

This Update is the third in a series.

Authors

Explore more in

Privacy & Security Healthcare Biotechnology & Pharmaceutical Medical Device

Related insights

Update

FTC Announces New Children’s Privacy Requirements in Updated COPPA Rule

Update

Securities Enforcement Forum New York 2025: A New Era Looms