It's Not Just HIPAA Anymore — Here's What You Need to Know About the New Consumer Health Data Laws

By:Kevin S. Olson
July 30, 2024

Adding to the complex patchwork of state privacy laws, Washington state, Nevada, and Connecticut have recently passed laws that regulate "consumer health data". The Washington My Health My Data Act (MHMD Act), Nevada S.B. 370, and the amended Connecticut Data Privacy Act (CTDPA) significantly change the landscape of how organizations will need to approach the collection and use of consumer health data.

1. Background

Passed in the wake of the Supreme Court's *Dobbs v. Jackson Women's Health Organization* decision, these consumer health data laws specifically target health data not otherwise protected under the Health Insurance Portability and Accountability Act (HIPAA).

Although a driving force behind the passage of these laws was to protect consumers' access to reproductive or sexual healthcare, the expanded scope of what is considered "health data" means that a much wider range of businesses that might otherwise be outside of the traditional healthcare space must assess compliance with these laws.

2. What is Consumer Health Data?

Consumer health data is broadly defined as any information relating to an identified or identifiable individual and that identifies that individual's health status.

Examples of consumer health data include:

- information or data regarding:
  - individual health conditions, treatment, status, diseases, or diagnoses;
  - social, physiological, behavioral, and medical interventions;health-related surgeries or procedures;use or purchase of prescribed medication;bodily functions, vital signs, symptoms, or measurements;
  - diagnoses or diagnostic testing;
- 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; and
- any consumer health data information that is derived or extrapolated from non-health information, such as proxy, derivative, inferred, or emergent data.

As illustrated by the list above, the scope of data that can identify an individual's health status is extensive. Apps that track an individual's fitness, fertility, medical conditions, etc. are likely handling consumer health data. For example, the Washington Attorney General has noted that "an app that tracks someone's digestion or perspiration is collecting consumer health data."

Moreover, consumer health data includes inferences based on products an individual has purchased. The Washington Attorney General has also indicated that a pregnancy prediction score assigned to a shopper by a retailer based on products purchased "is protected consumer health data even though it was inferred from nonhealth data".

3. Who Do These Laws Apply To?

These consumer health data laws generally apply to any websites, apps, or any other businesses that collect the consumer health data of Washington and Nevada consumers (including non-residents if their data is collected in those states) and Connecticut residents. This broad application is distinct from HIPAA which specifically regulates "covered entities" (e.g., health plans, health care clearinghouses, health care providers, and their business associates).

Also, it is worth noting that these laws do not contain threshold triggers tied to revenue or number of individuals whose data the business processes. Although there are certain exemptions in these laws for businesses that are otherwise regulated by laws such as HIPAA, the Gramm-Leach Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA), etc., if a business handles consumer health data it must comply with these consumer health data laws regardless of the scope of its processing operations.

4. Why Should You Care?

All three of the Washington, Nevada, and Connecticut laws may be enforced by each state's Attorney General. However, a defining feature of the Washington MHMD Act is that it includes a private right of action. A private right of action allows individuals to bring suits directly against businesses for violation of the Washington MHMD Act as an unfair or deceptive trade practice. And if a plaintiff is successful in a lawsuit alleging an unfair or deceptive trade practice, there is the potential to recover statutory damages and attorneys' fees.

5. What are the Compliance Obligations?

Major compliance obligations under these laws include:

- **Consumer Health Data Policy** – A separate consumer health data privacy policy that discloses (among other things) the categories of consumer health data collected, how it is used, who the data is shared with, and a notice of consumer rights.
- **Collection Requirements** – A business may not collect health data except:
  - with the consumer's consent; or
  - to the extent necessary to provide a consumer-requested product or service.
- **Security Requirements** – Businesses are required to:
  - restrict access to consumer health data to personnel who require access to such data; and
  - establish, implement, and maintain reasonable administrative, technical, and physical data security practices.

- **Data Subject Requests** – Comply with consumer requests, including requests to access their data, withdraw consent, or request deletion.
- **Contractual Requirements** – All processors receiving consumer health data must be bound to a contract that sets out the processing instructions and limits how they may use that data.
- **Connecticut Specific Obligations:**
  - Because consumer health data is also considered "sensitive data" under the CTDPA, entities will need to conduct a data protection impact assessment (DPIA);
  - The CTDPA explicitly requires opt-in consent to process consumer health data even if it is required to provide a service; and
  - All personnel with access to consumer health data must be subject to a statutory or contractual duty of confidentiality.

All three of the Connecticut, Nevada, and Washington laws are all currently in effect. Although the Washington law had an extended compliance deadline for certain small businesses, that deadline passed on June 30, 2024. If you have any questions on these consumer health data laws, are curious about how you can get your organization in compliance, or if you have any other data privacy or security related questions, please reach out to Kevin S. Olson or another member of the Privacy and Data Security Team.

The author would like to acknowledge the contributions to this article by Shelby Bourgeois, Northeastern University School of Law (NUSL) 2025.