Bloomberg Law News 2023-05-02T12:28:01381222369-04:00

Washington’s Health Data Privacy Law Raises Compliance Hurdles

2023-05-02T04:00:28000-04:00

The state of Washington’s My Health My Data Act, signed April 27 by Governor Jay Inslee, is poised to transform the privacy landscape. The act’s broad scope and definitions will expand its reach to data not normally considered health data, and to businesses that don’t traditionally consider themselves health-care providers.

The breadth and vagueness of the act is coupled with challenging implementation requirements and enforcement through a plaintiff-friendly private right of action.

Businesses from every sector should pay close attention to this new privacy law.

Sweeping Applicability

Rather than basing its applicability on the thresholds established by other states, the act, with just a few exclusions like governmental agencies and tribes, applies to any legal entity that conducts business in Washington or produces or provides products or services that are targeted to Washington consumers, and alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data.

Even more broadly, the term “consumer” encompasses Washington residents as well as any person whose health data is “collected” in Washington. Collected, however, doesn’t mean collected—it means to “buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any manner.”

Businesses that do not consider themselves to be “doing business” in Washington or collecting data from “Washington consumers” may fall within the purview of the act. One example could be those using Washington-based cloud service providers or with online stores through Washington-based online retailers.

Broad Definition of Consumer Data

Many of the act's core terms rely on a broad definition followed by a non-exclusive list of examples. The most important term is "consumer health data," which is defined as "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."

For example, "physical or mental health status" includes data derived from non-health information including precise location information that could reasonably indicate a consumer's attempt to receive health services or supplies. Based on its plain language, this could include data identifying a consumer as having purchased vitamins or being near a place that offers gauze and bandages for sale.

The breadth of "consumer health data" means that covered businesses operating in industries ranging from athletic or sports equipment; footwear and apparel; and over-the-counter skin or hair products to groceries, food, and beverages could all potentially be within the purview of the act.

Ultimately, the courts will determine the act's scope. The act's private right of action for violations will provide significant incentive for the plaintiffs' bar to test expansive interpretations.

Strict Restrictions for Covered Businesses

The following restrictions and obligations are likely to have significant impacts on a company's data collection, processing, sharing, and storage practices.

Opt-In Consent. Organizations will need to obtain a consumer's opt-in affirmative consent before collecting or sharing a consumer's health data, unless such collection or sharing is necessary to provide a product or service requested by the consumer. As a result, covered businesses will need to update policies and procedures to account for an opt-in requirement.

Prohibition on Sale. The act makes it unlawful for any person to sell consumer health data without a valid written authorization signed by the consumer which must also be separate from the consent obtained to collect or share consumer health data in the first place. The authorization contains

onerous content requirements including purchaser contact information and an explanation of how the sold data will be gathered and used by the purchaser.

Further, because a "sale" is "the exchange of consumer health data for monetary or other valuable consideration," the authorization requirement will likely apply in a wide range of data transfers that would not normally be considered a "sale." Covered businesses will need to carefully think through data disclosure practices to determine what consent and authorization obligations might be triggered by a "sale" of data.

Deletion Rights With Virtually No Exceptions. The act provides consumers with the right to delete their consumer health data, requiring that the covered business delete the consumer's health data upon request, and notify all processors, affiliates, and third parties with which the consumer health data has been shared—which must then also delete the data.

The act's deletion right is significantly broader that other state privacy laws in that it has virtually no exceptions. The lack of exceptions for common preservation requirements (such as for litigation) could present a significant legal dilemma.

Prohibition on Geofencing. Geofencing is the process of establishing a virtual geographic boundary around a specified location. The act will entirely prevent covered companies from using geofencing to target advertising to consumers seeking medical care.

Most of the act's provisions will take effect on March 31, 2024. Small businesses will receive a brief reprieve and must comply by June 30, 2024. The geofencing restrictions become effective 90 days after enactment.

This article does not necessarily reflect the opinion of Bloomberg Industry Group, Inc., the publisher of Bloomberg Law and Bloomberg Tax, or its owners.

Author Information

Wynter L. Deagle is a partner and Anne-Marie D. Dao and Dane C. Brody Chanove are associates on Sheppard Mullin's privacy and cybersecurity team.

Write for Us: Author Guidelines