Report on Patient Privacy Volume 23, Number 9. September 07, 2023 WA, NV and CT Enact Sweeping Health Data Laws, While Seven Additional States Tackle Privacy

By Jane Anderson

Lawmakers in multiple states focused heavily on consumer data privacy and health data privacy this spring, as 10 states bolstered their consumer data protections by enacting new laws.

Three states—Washington, Nevada and Connecticut—led the pack by approving significant new restrictions and requirements for entities that handle consumer health data. Meanwhile, seven additional states—Delaware, Oregon, Iowa, Indiana, Montana, Tennessee and Texas—enacted more general data privacy legislation, and Florida approved a new law banning offshore storage of medical data.

Washington kicked off the busy legislative season in April with the passage of an amended version of the My Health My Data Act (HB 1155).[1] The new law, signed by Gov. Jay Inslee (D) on April 27, is set to impose "sweeping new requirements on the collection, processing, and sale of consumer health data in the state," according to attorneys Kirk Nahra, Ali Jessani and Samuel Kane, all of whom practice with WilmerHale.[2]

"While we have seen an increased interest in the regulation of health data by the Federal Trade Commission, the My Health My Data Act would represent a novel step towards regulating health data at the state legislative level," the three attorneys wrote shortly before the bill was signed.

The legislation imposes "robust requirements on the collection, sharing, and sale of consumer health data, including separate affirmative opt-in consent requirements for collection and sharing, as well as a distinct requirement for 'valid authorization' of sale" Nahra, Jessani and Kale wrote. Most importantly, the law would be enforceable through a private right of action—potentially exposing regulated businesses to substantial legal exposure for violations.

The Washington legislation expands on the HIPAA framework by "supplementing the limited protections for health data offered by HIPAA," the attorneys wrote. It employs an expansive definition of "consumer health data," which covers any "personal information that is linked or reasonably linkable to a consumer and that identifies a consumer's past, present, or future physical or mental health."

New Definition Includes Apps

This definition includes not just information like health conditions, treatment history, and medication prescriptions but also, among other things, "[p]recise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies" or other health-related information "that is derived or extrapolated from nonhealth information," the three attorneys said. Information subject to HIPAA is exempt.

The consumers protected by the act include both Washington residents and individuals "whose consumer health data is collected in Washington," and the act was written to encompass health-related websites and apps that go largely unregulated under HIPAA, Nahra, Jessani and Kale wrote.

"The Act provides that regulated entities must obtain separate consents 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). And the Act's definition of 'consent' is a robust one, requiring 'a clear affirmative act that signifies a consumer's freely given, specific, informed, opt-in, voluntary, and unambiguous agreement,'" they wrote.

The legislation also imposes distinct preconditions for the sale of consumer health data, requiring that sales be preceded by a "valid authorization from the relevant consumer" that includes information such as the "specific consumer health data to be sold, the name and contact information of the buyer and seller, the purpose of the sale, and an expiration date for the authorization itself," the attorneys said.

Finally, the new law is enforceable through a private right of action under the Washington Consumer Protection Act. "The bill's inclusion of a private right of action greatly increases the compliance risk for regulated entities, as it exposes these companies to lawsuits from individual litigants," Nahra, Jessani and Kale wrote. "For a rough analogue, companies can look to the impact of the Illinois Biometric Information Privacy Act (BIPA), a biometric privacy law that similarly includes a private right of action and has created massive potential legal exposure for violators."

Washington State Attorney General Bob Ferguson issued FAQs on the new law on June 30, clarifying the dates its provisions will take effect and elaborating on the definition of "consumer health data."[3]

The section of the law that prohibits tracking of individuals by geofencing data took effect on July 23, Ferguson said. Regulated entities that are not small businesses must comply with other provisions beginning March 31, 2024, and small businesses must comply beginning June 30, 2024, he said.

Washington officials are taking an expansive view of "consumer health data," Ferguson said: "Ordinarily, information limited to the purchase of toiletry products would not be considered consumer health data. [But] while information about the purchase of toilet paper or deodorant is not consumer health data, an app that tracks someone's digestion or perspiration is collecting consumer health data."