ROPES & GRAY

ALERT

May 9, 2023

Latest Washington Privacy Law Sets New, Broad Course for State-Based Health Information Regulation

Attorneys
Christine Moundas
Richard Harris
Matt Cin
Kris Kenn

On April 27, 2023, Washington Governor Jay Inslee signed into law the "My Health My Data Act," (the "Act"), beginning the 11-month countdown until this new, broad privacy law takes effect. The Act distinguishes itself from other recent state privacy law legislation in that it is specifically health care focused—aiming to protect health data that falls outside the scope of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). In attempting to safeguard this category of information, Washington has enacted a broad law that will require robust compliance efforts from entities generally considered outside of traditional health care regulatory regimes. Further, the private right of action present in the Act sets a new stage for potential litigation and subsequent changes based on judicial interpretation.

In this Alert, we provide a summary of key provisions of the new law, compliance concerns, and actions businesses can take to prepare for the March 31, 2024 effective date.

Who and What is Being Regulated?

Regulated entities are defined broadly. Spurned by post-*Dobbs* privacy concerns, the stated intent of the Act is to "close the gap" between the health information that individuals believe is protected and what actually is. To this end, the scope of the Act is broad, applying to "regulated entities," which are defined as any entities that conduct business or target consumers in Washington and—jointly or unilaterally—determines the purpose and means of collecting, processing, sharing, or selling consumer health data. Unlike other state laws, the Act does not have a threshold for annual revenue, the number of impacted consumers, or the amount of revenue attributable to sharing health information for regulated entities. While so-called small businesses have a slightly longer time in which to become compliant (not until June 30, 2024 for small businesses compared to March 31, 2024 for all other entities), regulated entities are otherwise treated similarly throughout the law, irrespective of size. In terms of exceptions, there are certain data-based exceptions, including data subject to HIPAA, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Family Educational Rights and Privacy Act, and Washington's own health benefit exchange law.

Consumers include individuals whose data are "collected" in Washington. While "consumer" includes Washington residents, it also covers a person whose consumer health data are collected in Washington. "Collected" is defined expansively and includes buying, renting, accessing, retaining, receiving, acquiring, inferring, deriving, or otherwise processing consumer health data in any manner. There is no clarity given within the law on what actions would be considered "inferring" or "deriving"; however, it is noted that "consumer" does not include individuals acting in an employment context. Businesses should take special care in evaluating their relationship to any kind of health data in order to better vet whether their processes could fall under this broad definition of "collection."

Consumer health data includes health adjacent information. The definition of "consumer health data" is expansive and includes information that is "linked or reasonably linkable" to a consumer that identifies the consumer's past, present, or future physical or mental health. The categories included under this definition range from individual health conditions or treatments, the use or purchase of medications, measurements of bodily functions or vital signs, precise locations that could "reasonably indicate" a consumer's attempt to acquire health services or supplies, and they can also include information that is "derived or extrapolated from nonhealth information." Similar to the definition of "collection," little detail is given on what the broader categories actually mean in application.

Compliance Requirements

Robust notice and consent for collecting and sharing consumer health data. Under the Act, entities will be required to provide detailed consumer health data privacy policies. In addition, opt-in consents will need to be separately and distinctly obtained for (a) the collection and (b) sharing of consumer health data. Further, both the consumer health data privacy policies and the consents must detail the categories of health data that are being collected or shared, how the data will be used, the categories of data that will be shared, and how consumers can withdraw consent from said processes.

Sale of consumer health data requires consumer authorization. Similar to HIPAA authorizations, the sale of consumer health information will require a consumer's specific authorization. These authorizations must specify the consumer health data to be sold, the purchaser's details, and the intended use of the consumer health data being purchased. Additionally, the authorizations are revocable at any time and are valid only for at most one year.

Absolute right of deletion. Consumers will have the right to withdraw consent to the collection and sharing of their consumer health data as well as the right to request deletion of such data. Upon receiving such a request, entities must delete the consumer health data from their records, including from backup and archived systems, and must notify all affiliates of the deletion request.

Compliance Concerns

Prohibits the use of geofencing. The Act prohibits the use of a geofence around an entity that provides in-person health care services wherein the geofence technology is used to identify or track consumers; collect consumer health data; or send notifications, messages, or advertisements relating to health data or health care services. Entities that have combined retail and clinic spaces—more common with the advent of the quick-clinic—should take special care to make sure they do not run afoul of such a requirement.

Violating a contract with a regulated entity renders the processor a regulated entity itself. Processing consumer health data on behalf of a regulated entity requires a contract that enumerates the processing instructions specific to what is necessary per the consumer's consent or to provide the requested product or service. A violation of said contract renders the processor a covered entity and, as such, subject to all of the regulated entity's obligations under the Act. Accordingly, data processors must take special care in regard to their adherence to such contractual terms.

The Act includes a private right of action. Similar to the Illinois Biometric Information Privacy Act ("BIPA"), which has seen extensive litigation, the Act includes a private right of action under Washington's Consumer Protection Act. Individuals can bring claims against entities for damages of up to $7,500 per violation. The definition of a "violation" is not prescribed in the Act and, as has been seen in recent BIPA cases, whether a violation is defined as the general collection of information or each instance of collection of information may have drastic effects on the final damages calculation.

Next Steps

The Act separates itself from the privacy pack as a unique, expansive privacy law attempting to target areas of sensitive health data that have become of greater concern in the post-*Dobbs* world. Considering the pervasive fear of the misuse of data surrounding reproductive health care, it is unlikely that this Act will be the only legislation of its type. Instead, it is more likely the first of a newly chartered course into health data regulation. Other states like Illinois are also considering similar legislation. While those who fall under the definition of regulated entity within the Washington context should begin preparing for implementation of the law, those outside of the Act's reach should still take notice of it as a sign of a new form of privacy regulation that may spread to other similarly concerned states.

To begin preparing for enforcement, entities should evaluate the extent to which they collect, share, or sell consumer health data or any data that may be reasonably interpreted to be considered consumer health data. As BIPA litigation in Illinois has shown, the vagueness of terms should lead entities to be overly cautious in evaluating whether the data they collect are related to health information. Additionally, entities should begin vetting their current privacy policies and notice and consent procedures and seek advice on formulating new, compliant disclosures. Further, the right of deletion within the Act is robust to the extent that laying the groundwork in order to make such a process as efficient as possible cannot begin soon enough. Overall, the Act demonstrates the growing trend toward greater and more granular oversight of private information—entities should keep a close eye on this trend and prepare accordingly.

* * *

If you have any questions concerning this Alert, please do not hesitate to contact one of the authors or your regular Ropes & Gray advisor.