Questions You Should be Asking about the Groundbreaking My Health, My Data Act

Related Professionals

Marcel C. Duhamel

Christopher A. LaRocco

Gretchen Rutz Leist

Related Services

Data Strategy, Privacy and Security

Related Industries

Health Care

CLIENT ALERT | 5.4.2023

Last week, Washington State passed a novel health privacy law titled the "My Health My Data Act." The Act, which will come into effect on March 31, 2024, provides protections for consumer health data that is collected by businesses not expressly covered by the Health Information Portability and Accountability Act of 1996 (HIPAA). Essentially, The Act is intended to serve as a supplement to HIPAA to apply to more entities, but it goes much farther than that. The Act borrows concepts from HIPAA, state consumer privacy laws, and biometric privacy laws, such as Illinois' Biometric Information Privacy Act, to create the most restrictive state regulation of consumer health and biometric information to date. Importantly, the law includes a robust private right of action for violations. Below are the questions you should be considering if you collect any consumer health data in the U.S.

Who does this law apply to, anyway?

This Act applies to "regulated entities" or entities that conduct business in Washington, produce or provide products or services that are targeted to consumers in Washington, and alone or jointly with others, determine the purpose and means of collecting, processing, sharing, or selling of consumer health data. This broad scope of applicability, without any revenue threshold, means that this law applies to businesses inside and outside of Washington. The Act does not have revenue or consumer quantity thresholds like in certain state privacy laws; however, the law does contain exemptions for small businesses which extend the time to prepare for the law.

Whose information is protected?

Consumers are defined as (1) natural persons who are Washington residents; or (2) natural persons whose consumer health data is collected ***in Washington***. Note that – in applying to natural persons whose information happens to be collected in Washington – this definition is more expansive than the definition of "consumer" in other recent state privacy laws. Consumers do not, however, include

individuals acting in an employment context.

What information is protected?

This law protects several categories of "consumer health data", which is defined as any 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. This definition expressly and expansively includes:

- Individual health conditions, treatment, diseases, or diagnosis
- Social, psychological, behavioral, and medical interventions
- Health-related surgeries or procedures
- Use or purchase of prescribed medication
- Bodily functions, vital signs, symptoms, or measurements of such information
- Diagnosis or diagnosis testing, treatment, or medication
- Gender-affirming care information
- Reproductive or sexual health information
- Biometric data
- Genetic data
- Precise location information (if it can reasonably indicate a consumer's attempt to acquire or receive health services or supplies)
- Data that identifies a consumer seeking health care or services
- Any information that a business processes to associate or identify a consumer with the data listed above that is extrapolated from non-health information

Like other state privacy laws, the act contains several data level exemptions which exempt information subject to other laws such as the GLBA, the Social Security Act, title XI, FERPA, and FCRA.

What rights does this law provide to consumers with respect to their health data?

The Act provides consumers with several familiar rights:

- the right to confirm whether a regulated entity collects, shares, or sells the consumer's health data
- the right to access that data, including a list of all third parties and affiliates with whom the regulated entity has shared or sold the consumer health data and contact information for those third parties
- the right to withdraw consent from the collection and sharing of health data
- the right to request that consumer health data be deleted

What changes should be made to my website?

This Act requires regulated entities to post a Consumer Health Data Privacy Policy on their website homepage. Much like the other state privacy laws, the Act requires that the privacy policy clearly and conspicuously disclose: (1) the categories of consumer health data collected and the purpose of collection, including how the data will be used; (2) the categories of sources of the consumer health data; (3) the categories of consumer health data shared; (4) a list of the categories of third parties and specific affiliates with whom the regulated entity shares consumer health data; and (5) how consumers can exercise their rights. It is unclear if this consumer health privacy policy can be combined with an entity's existing privacy policy or biometric information policy.

When is consumer consent required?

The Act requires regulated entities to have a consumer's consent to any collection or sharing of consumer health data, unless such collection or sharing is necessary to provide a product or service that the consumer requested from the regulated entity. Consent to the sharing of data is required to be separate to consent to the collection of data. "Consent" is defined as a clear, affirmative act "that signifies a consumer's freely given, specific, informed, opt-in voluntary, and unambiguous consent, which may include written consent provided by electronic means."

Regulated entities must also have "valid authorization" signed by the consumer to "sell or offer to sell" consumer health data. The Act defines "sell" to include the sharing of consumer health data "for monetary or other valuable consideration." A "valid authorization" is a document signed by the consumer that contains a host of information, including the specific data at issue, the name of the purchaser, the purpose of the sale, an expiration date within one year of the signature, and a statement that the consumer has the right to revoke authorization at any time.

What other protections need to be implemented to protect consumer health data?

Under the Act, regulated entities must permit individuals to access data only as necessary to provide a requested product or service or further the purposes for which a consumer provided consent. Regulated entities are also required to implement data security measures to protect consumer health data. Further, regulated entities must enter into data processing agreements with processors that set forth the processing instructions and limit the actions the processor may take with respect to consumer health data.

What is "geofencing", and why is it important?

"Geofencing" is defined as "technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, wifi data, and/or any other form of location detection to establish a virtual boundary around a specific physical location." A "geofence" is a "virtual boundary that is 2,000 feet or less from the perimeter of the physical location."

The Act prohibits any person from implementing geofencing around any entity that provides in-person health care services when the geofence is used to (1) identify or track consumers seeking health care services; (2) collect consumer health data from consumers; or (3) send notifications, messages, or

advertisements to the consumers related to their consumer health data or health care services.

How is this Act enforced?

The Attorney General's office has the ability to investigate violations and pursue litigation. Importantly, individuals may also bring civil claims under Washington's Consumer Protection Act which allows for treble damages.

Conclusion

Momentum for the passage of state privacy laws is at an all-time high. In March, Iowa became the sixth state to pass a comprehensive privacy law. Since then, the Indiana and Tennessee legislatures have passed similar laws that await their respective governors' signatures. While Washington has been unable to pass its own comprehensive privacy law because of disagreements over the inclusion of a private right of action, the My Health My Data Act is a first-of-its-kind law that signals Washington will continue to be on the forefront of consumer privacy. For more information, or other questions about the My Health, My Data Act, please contact Marcel Duhamel, Christopher LaRocco, Gretchen Rutz Leist, or your Vorys attorney.