CLIENT ALERTS & INSIGHTS

REMINDER: Washington's "My Health My Data" Act Now In Effect

APRIL 1, 2024

Washington's My Health My Data Act implements strict-and separate-consent requirements for the collection and sharing of an individual's health data, with few exceptions.

As of March 31, 2024 the Washington My Health My Data Act is in effect, with regulated entities required to now meet the law's strict consent requirements.

The law is unlike recent US state laws, which broadly regulate the collection and processing of any type of personal data. The My Health My Data Act only acts to regulate specific categories of consumer health data.

However, the new law's seemingly narrow focus on just consumer health data is a bit of a misnomer as the law could have broad impacts. Unlike the other recent US state laws, the My Health My Data Act has **no** threshold triggers-meaning it applies to any business collecting or processing any amount of consumer health data-and applies to any collection or processing occurring in the state of Washington. The latter could give the law extra-territorial scope in that it could apply to health data collected about individuals traveling to Washington, but who are not residents of Washington.

Further, the law's broad definition of "consumer health data" extends to categories of data that practitioners typically don't tie to "health data", such as biometric information and precise geolocation information.

The My Health My Data Act also introduces familiar concepts such as specific privacy notices related to a business's collection and use of health data, and implementation of reasonable and appropriate technical and organizational security measures to protect health data.

However, the biggest takeaway is that the My Health My Data Act requires prior consent for the processing and sharing of consumer health data. The new law also puts geofencing prohibitions and consumer health data privacy rights in place.

Entities that operate in the state of Washington should take note, and businesses operating in the US should keep their eye on similar consumer health data protection laws that are popping up. Especially given the fact that the law is enforceable under the state of Washington's general consumer protection laws, which allow for a private right of action.

Regulated Data and Entities

The My Health My Data Act only applies to "Regulated Entities," which is broadly defined as any entity that (1) conducts business in the state of Washington **or** produces or provides products or services that are targeted to Washingtonians; **and** (2) collects, processes, shares, or sells consumer health data.

There are **no** threshold triggers. Other, broader, US state data protection laws typically don't apply to a business until that business collects a certain amount of personal data. For example, the Colorado Privacy Act does not regulate a business until it collects, annually, 100,000 or more Colorado resident's personal data. Broader, US state data protection laws have been drafted in a manner to avoid impacting small businesses. Without the threshold triggers, the My Health My Data Act will apply to any business no matter how much consumer health data they interact with.

Although, the My Health My Data Act provides small businesses a three month extension until the law's requirements are effective-meaning small businesses have until the end of June 2023 to build out their compliance.

The new law may also have extra-territorial effects in the sense that it applies to protect an individual's health data even where such person is not a resident of Washington. Importantly, the definition of "consumer" includes both individuals who are residents of Washington **and** those whose consumer health data is collected in the state of Washington. The state of Washington's Attorney General's Office issued guidance earlier this year confirming that extra-territorial effect.

This takes on added importance in the aftermath of the US Supreme Court overturning Roe v. Wade as individuals seek reproductive health care services across state lines.

The definition of "consumer health data" is also broad. It includes "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."

Below is the My Health My Data Act's non-exhaustive list of consumer health data categories:

1. Individual health conditions, treatment, diseases, or diagnosis;
2. Social, psychological, behavioral, and medical interventions;
3. Health-related surgeries or procedures;
4. Use or purchase of prescribed medication;
5. Bodily functions, vital signs, symptoms, or measurements of such information;
6. Diagnoses or diagnostic testing, treatment, or medication;
7. Gender-affirming care information;
8. Reproductive or sexual health information;
9. Biometric data;
10. Genetic data;
11. Precise location information that could reasonably indicate a consumer's attempt to acquire or receive health services or supplies; and
12. Data that identifies a consumer seeking health care services.

Consumer health data can also include information derived from non-consumer health data, if such non-consumer health data is processed with any data falling into the above categories. Meaning, any processing of consumer health data with non-consumer health data may pull in consent and other data protection requirements to data not otherwise falling into the above categories.

Consent and Necessity

The biggest shift in practices will certainly stem from the new law's consent requirements. A business is only permitted to collect and process consumer health data in two circumstances:

1. Where it has obtained the consumer's prior consent; or
2. It is necessary to provide a product or service the consumer requests from the specific business.

The same circumstances apply to when a business is permitted to share or disclose consumer health data to a third party-meaning a business either needs to obtain a separate consent for sharing the consumer health data, or the consumer needs to request such sharing as part of the provision of services.

Consent under the My Health My Data Act must be obtained via prior, express opt-in consent. Businesses cannot rely on implied consent, pre-checked boxes, or combined consents (e.g., consent for marketing activities combined with consent for collecting consumer health data under one check box option).

Businesses are permitted to disclose consumer health data to "processors"-similar to the same concept instituted under other US data protection laws-that act as service providers and vendors, provided such entities enter into written contracts that strictly regulate and limit what the processor can do with the consumer health data.

Consumer Health Data Rights

Consumer privacy rights have become common place under US and other data protection laws-such as the right to access personal data, delete personal data, and correct personal data.

The My Health My Data Act is no different, and it provides consumers the following rights to:

1. **Confirm** whether a business is collecting, sharing, or selling consumer health data;
2. **Access** the consumer health data a business has collected about them;
3. **Delete** the consumer health data a business holds about them; and
4. **Withdraw** consent for collection and/or sharing of their consumer health data.

Businesses must respond to any such requests within 45 days from receipt of the request-but are permitted to seek an additional 45 days if warranted due to the complexity or volume of the request.

Geofencing Prohibitions

The My Health My Data Act also makes it unlawful for any business to use geofencing in or around any facility that provides in-personal health care services. A “geofence” is defined to mean technology that uses global positioning coordinates, cell tower connectivity, cellular data, radio frequency identification, Wi-Fi data, or any other form of spatial or location detection to either (1) establish a virtual boundary around a specific physical location, or (2) to locate a consumer within a virtual boundary.

For purposes of this definition, "geofence" means a virtual boundary that is 2,000 feet or less from the perimeter of the physical location.

Under the My Health My Data Act, it is unlawful for a business to use such geofencing technology to (1) identify or track consumers seeking health care services; (2) collect consumer health data; or (3) send notifications, messages, or ads to consumers related to or derived from their health data or use of health care services.

Enforcement

The My Health My Data Act will be enforceable by the Washington Attorney General. However, the new law is also regulated under the state’s general consumer protection law, which **does** include a private right of action whereby consumers themselves can bring suit against businesses that allegedly violate the My Health My Data Act.

Conclusion

With the My Health My Data Act in effect, businesses operating in the state of Washington and that touch the health care industry or that provide services related to health care in any way must ensure they have processes and procedures in place to comply with the consent and other requirements.

Unlike other US state data protection laws, the private right of action may see the My Health My Data Act allow for a new, robust litigation space to grow as courts grapple with the depth and breadth of the new law.

As more US states continue to implement new-and amend existing-data protection requirements, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.