STINSON

News & Insights

First of its Kind Privacy Law Signals Fundamental Shift in Protection of Consumer Health Data

Alert

02.15.2024

By Jennifer Brown, Ph.D., Jessica Kracl & Jenifer McIntosh, CIPP

As more and more states consider consumer privacy laws, the first-of-its kind My Health My Data Act (the Act) could be a harbinger of health and wellness compliance requirements to come. The ramifications of Washington state's law will be felt far beyond its borders, impacting businesses across the country.

The Act spells out new rules for businesses that are not subject to the federal Health Insurance Portability and Accountability Act (HIPAA), as well as HIPAA entities that process consumer data. While this Act may not impact you yet, other states are expected to follow Washington with consumer health data protection laws of their own. It is important to get ahead of these unique laws and regulations before they are implemented in your state—and act now if processing Washington data.

The Act gives consumers several rights, including the right to access their health data, to correct or delete their health data and to opt out of having it sold or shared. Businesses likely to be affected by the Act, or laws like it, include wearable technology, fitness applications, exercise studios, med spas and retail stores.

While small businesses have until June 30, 2024, to comply, larger businesses have only until March 31, 2024. The Act has a broad private right of action that could incentivize consumers to look for violations. Even businesses with only tenuous connections to Washington need to understand how the law works.

This alert will explore what qualifies as health data and data processing as well as help you to determine whether Washington's Act applies to your business.

First of its Kind Privacy Law Signals Fundamental Shift in Protection of Consumer Health Data

DOES THE ACT APPLY TO YOUR BUSINESS?

My Health My Data applies to you if your business:

1. Conducts business in the state of Washington, or targets products or services to Washington consumers.

2. Collects or processes consumer health data.

WHAT DOES "CONDUCTING BUSINESS" OR "TARGETING PRODUCTS OR SERVICES" MEAN?

Unfortunately, neither definition is provided in the statute itself, but if you are headquartered in Washington, have a storefront in Washington, are registered as a foreign corporation in Washington or perform business operations in Washington, you likely ″conduct business″ there. The definition of ″targeting″ is still somewhat nebulous, although it will likely be interpreted in concert with other privacy laws and in conjunction with how a company utilizes targeted advertising. There is an open question whether offering products or services via a website accessible by WA consumers means a business is targeting consumers or conducting business within that state. Given the number of lawsuits related to health care data breaches and wire-tapping privacy violations, there is a chance courts will construe these terms broadly, impacting businesses with only minimal presence or a small customer base in Washington.

WHO IS A "CONSUMER?"

A consumer is any person who lives in Washington or any person whose data is collected while they are physically in Washington. To be a consumer, a person must be acting on their own behalf rather than on behalf of an employer. Even people passing through the state temporarily are protected by the Act, meaning that complaints of non-compliance could come from an affected person in any state whose data was collected by an entity in Washington. For example, an Oregon resident visiting a med spa in Washington state would qualify as a consumer for purposes of the Act.

WHAT IS “HEALTH DATA?”

Health data encompasses information about consumers’ past, present or future health status. This definition goes beyond actual diagnoses—and even purchases of medication—because health status includes information ″derived or extrapolated from non-health information.″ Under this definition, Washington brings activities of daily living, such as going to the grocery store, exercising and online shopping, under the auspices of the Act when data about those activities is reasonably linkable to a consumer′s health. For example, grocery store purchases alone are not traditionally considered health data. But if an individual′s purchasing or browsing history allowed a company to infer that the consumer is overweight, has a higher likelihood of developing type 2 diabetes, or has a knee injury or a gluten allergy,

that purchasing history would be related to health status, and therefore covered by the Act.

Data about nutrition, personal habits, health, wellness, fitness and general activity level could all fit the definition of "consumer health data" under the Act because such information can be used to draw inferences about an individual's health status. The inclusion of such inferences make the Act much broader than HIPAA, so even HIPAA-compliant businesses will need to pay attention, particularly when marketing procedures not covered by insurance, such as certain cosmetic, esthetic, and wellness treatments.

WHAT DOES IT MEAN TO "COLLECT" OR "PROCESS" HEALTH DATA?

Businesses not traditionally operating in health-related fields need to be aware that data they collect, share, sell or otherwise "process" may now be considered consumer health data, and subjects them to the Act. This can be the case if a business is acting jointly with another, or at the direction of another. For example, a marketing company in Texas working for a med spa in Washington is subject to the Act as a processor. The marketing company would need to comply with the Act as well as support clients in their efforts to comply with the Act, similar to how a business associate would operate under HIPAA.

The definition of "collect" is broad and includes the buying, accessing, deriving and processing of consumer health data. The term "processing" is broadly construed and includes "any operation or set of operations performed" with the data, including storage, analysis, collection and disclosure. The Washington state attorney general guidance suggests a company that only stores data in Washington is not a regulated entity under the Act; however, as soon as a business does more than store data, they are considered to be "collecting" and would fall under the Act's provisions. Data analyses and data de-identification are also likely to be within the scope of the definition of "collect," such that merely processing data in order to de-identify it could mandate compliance.

While the Act excludes de-identified data and data that is publicly available, there is still a long list of requirements for compliance. A complete understanding of where covered health data comes from, who controls it and what entities use it will be crucial to businesses understanding whether the Act applies to their conduct. If your business collects or processes data related to health status and well-being, you should be prepared to comply with specific provisions of the Act.

For more information on the Act, its impact, or compliance questions, please contact Jennifer Brown, Ph.D., Jessica Kracl & Jenifer McIntosh, CIPP, Steve Cosentino, CIPP or one of the attorneys listed below or the Stinson LLP contact with whom you regularly work.

CONTACTS

Jennifer L. Brown, Ph.D.

First of its Kind Privacy Law Signals Fundamental Shift in Protection of Consumer Health Data

Jessica Kracl

Jenifer McIntosh, CIPP

RELATED CAPABILITIES

Health Care & Life Sciences

Intellectual Property & Technology

Private Business