# "MY HEALTH, MY DATA" IS FIRST OF ITS KIND PRIVACY LAW FOCUSED ON PROTECTING CONSUMER HEALTH DATA

Date: 2 May 2023

**US Policy and Regulatory and Intellectual Property Alert**

By: Whitney E. McCollum, Gina L. Bertolini, Jane E. Petoskey

## SUMMARY

On 27 April 2023, Washington Gov. Inslee signed into law House Bill 1155, referred to as the "My Health, My Data" Act (the Act), which takes effect on 31 March 2024. The Act aims to protect Washington consumer health data, particularly data related to reproductive healthcare.

1. The Act will have a significant impact on entities that collect consumer health data but are not governed by HIPAA, in most cases requiring implementation of a fulsome compliance infrastructure.
2. Entities will need to obtain separate consumer consents to collect and share data, and will be required to ensure a technical process is in place for managing revocation of consents and deletion requests.
3. The Act gives consumers increased rights to their data and enforcement rights through a private right of action.

## BACKGROUND AND CONTEXT

For over two decades, health information created or received by "Covered Entities"—defined as health plans, health care clearinghouses, and health care providers that transmit health information through certain electronic transactions—has received protection under a federal law known as the Health Insurance Portability and Accountability Act (HIPAA). HIPAA, however, only protects health-related information when that information is created or received by a Covered Entity. So even though the scope of data HIPAA covers is large (information relating to an individual's past, present, or future physical or mental health, the provision of health care, and payment for same), HIPAA does not regulate health information that is not created or received by a Covered Entity. For example, HIPAA does not cover health information in employment records; health information created, accessed, or maintained by technology companies; and digital health and other health care providers that do not transmit health information through certain HIPAA-governed transactions. In recognition of the proliferation of services offered through these and other non-traditional health care models—such as through mobile applications, web-based services, and cash-only services, as well as the host of "health-adjacent" services such as fitness and lifestyle apps and wearable devices—Washington legislators announced that they wanted to address this gap "by providing stronger privacy protections for all Washington consumers' health data."

## WHAT IS COVERED BY THE ACT?

The Act regulates any legal entity that collects, processes, or shares or sells "consumer health data" and either conducts business in Washington or targets products or services to Washington consumers. Consumer health data under the Act has a broad definition that 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." "Physical or mental health status" is also broadly defined and includes, among other things, use or purchase of prescribed medications; gender-affirming care information; reproductive or sexual health information; "precise location information" that could "reasonably indicate" a consumer's attempt to receive health services or supplies; and data that identifies consumers seeking health care. A "consumer" is a natural person, acting in "an individual or household context," who is a Washington resident or whose consumer health data is collected in Washington, not including an individual acting in an employment context.

## KEY PROVISIONS

- Entities regulated by the Act may not collect or share consumer health data without consumer consent, except as necessary to provide a product or service that the consumer requested; consents to collect and share must be "separate and distinct," obtained in advance, and include several provisions not unlike HIPAA authorizations.
- Consumers have a right to access their consumer health data; confirm whether entities regulated by the Act are collecting, sharing, or selling their consumer health data and receive a list of all third parties to whom their data has been sold or shared; withdraw their consent to collect or share consumer health data; and have their consumer health data deleted. Regulated entities are required to respond to such consumer requests within 45 days, with one 45-day extension when "reasonably necessary."
- Entities regulated by the Act have additional obligations related to transparency of collection, sharing, and disclosure of consumer health data; limitations on use; ensuring data security protections and access controls; prohibition on the sale of data; and subprocessor flow-down protections.
- The Act prohibits geofencing around any entity that provides in-person health services for the purposes of identifying and tracking consumers seeking health services, collecting consumer health data, or sending messages or advertisements to consumers related to their consumer health data or health services.
- Certain data is excluded, including protected health information governed by HIPAA, substance use disorder records governed by federal law, information governed by federal laws regarding human subjects research, and health related information collected for quality improvement, peer review, and quality assurance committees under state law, among others.
- The Washington attorney general may enforce violations of the Act through its state consumer protection laws, and consumers have a private right of action for violation of any provision of the Act.

## IMPLICATIONS

The United States, unlike many other countries with comprehensive privacy laws, continues to take a sectoral approach to privacy regulation, focusing on industries (*e.g.*, healthcare, financial institutions) instead of the data itself. While there have been attempts to create broader privacy protection at the federal level—for example, the

American Data Privacy and Protection Act, initially introduced in Congress in June of 2022 and expected to be reintroduced before the end of this session—states have been active in recent years in taking matters into their own hands. To date, California, Colorado, Connecticut, Utah, and Virginia have enacted—and Indiana, Montana, and Tennessee have passed, but not yet signed—comprehensive privacy laws. These comprehensive state laws do not, however, include specific protections for consumer health data that the Act creates.

Washington is the first state to address the specific issues around perceived gaps in protection of consumer health care data, including third parties' practices of identifying and targeting consumers based on personal health choices. The My Health, My Data Act goes into effect on 31 March 2024.

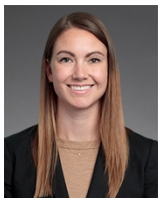
## KEY CONTACTS

**WHITNEY E. MCCOLLUM**
PARTNER

SEATTLE, SAN FRANCISCO
+1.206.370.7595
WHITNEY.MCCOLLUM@KLGATES.COM

**GINA L. BERTOLINI**
PARTNER

RESEARCH TRIANGLE PARK
+1.919.466.1108
GINA.BERTOLINI@KLGATES.COM



**JANE E. PETOSKEY**
ASSOCIATE

SEATTLE
+1.206.370.7853
JANE.PETOSKEY@KLGATES.COM

