Washington Governor Jay Inslee signed into law House Bill 1155, also known as the My Health My Data Act (the Act), on April 27, 2023. The Act goes into full effect for "regulated entities" on March 31, 2024 (and later for "small businesses"). Its stated purpose is to protect "consumer health data" collected by entities not subject to the federal Health Insurance Portability and Accountability Act (HIPAA).

One less obvious consequence of the Act is that it may make Washington state a new hot spot for class-action litigation involving biometric privacy. As discussed further below, the Act imposes several new requirements and restrictions on entities that collect and use biometric data. And unlike virtually every other state privacy law passed in recent years (including Washington's own preexisting biometric privacy law), the Act includes a broad private right of action authorizing consumers to sue for damages and other relief. In that way, the Act is similar to the Illinois Biometric Information Privacy Act (BIPA), which also includes a broad private right of action and has generated more than 2,000 class actions since 2015.

Who Does the Act Protect?

The Act protects consumers. A consumer is defined as any natural person who is a Washington resident **or** any natural person whose consumer health data is collected in Washington. The definition only includes persons acting in an individual or household context and does not include individuals acting in an employment context.

Which Entities Are Regulated?

The Act's requirements apply principally to "regulated entities" and "small businesses." Fewer requirements apply to "processors," which are entities that process consumer health data consistent with instructions from a regulated entity or small business.

Under the Act, a "regulated entity" is any legal entity that meets both of the following criteria:

1. Conducts business in Washington, or produces or provides products or services that are targeted to consumers in Washington.
2. Alone or jointly with others, determines the purpose and means of collecting, processing, sharing, or selling of consumer health data.

Regulated entities do not include government agencies, tribal nations, or service providers when contracted to process consumer health data on behalf of the government agency.

A "small business" is an entity that meets one or both of the following criteria:

1. Collects, processes, sells, or shares consumer health data of fewer than 100,000 consumers during a calendar year.
2. Derives less than 50% of gross revenue from the collection, processing, selling, or sharing of consumer health data, and controls, processes, sells, or shares consumer health data of fewer than 25,000 consumers.

Regulated entities and small businesses are subject to the same substantive requirements and restrictions. But, regulated entities are required to begin complying with the Act sooner than small businesses.

What Is "Biometric Data" Under the Act?

The Act regulates "consumer health data," which means "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," in turn, is defined to include "biometric data." And finally, "biometric data" means data that is generated from the measurement or technological processing of an individual's

physiological, biological, or behavioral characteristics and that identifies a consumer, whether individually or in combination with other data.

Biometric data includes, but is not limited to, the following:

1. Imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template can be extracted; or
2. Keystroke patterns or rhythms and gait patterns or rhythms that contain identifying information.

This complex and ambiguous definition of "biometric data" invites many questions that are likely to be decided by courts, including under what circumstances personal information is "reasonably linkable to a consumer" and which measurements of "behavioral characteristics" qualify as biometric data within the meaning of the law.

Some provisions of the Act narrow the scope of covered data in important ways. For example, data is considered "biometric" only if it "identifies a consumer, whether individually or in combination with other data." Further, because the definition of "consumer" is limited to "a natural person who acts . . . in an individual or household context" and specifically excludes "an individual acting in an employment context," the Act likely does not apply to biometric data collected and used solely in business-to-business (B2B) and employment contexts. Relatedly, the Act makes clear that it is not intended to prevent covered entities from processing any type of consumer health data, including biometric data, for certain security-related purposes like preventing and responding to security incidents, detecting identity theft, and combating fraud, harassment, and illegal activities.

These and other exceptions and limitations will likely exempt from the Act's scope some of the use cases that have spawned litigation under BIPA, such as facial identity verification for financial transactions and biometric timekeeping.

What Does the Act Require?

The Act imposes numerous restrictions and requirements on covered entities when they collect and use consumer health data, including the subset of consumer health data that qualifies as biometric data. The most important restrictions and requirements are summarized below.

Notice. Regulated entities must provide consumer health data privacy policies disclosing, among other things, the categories of health data collected, the purpose of collection, the intended use of the data, and how the consumer can withdraw consent from the future collection or sharing of their health data.

Consent. Consumer health data (including biometric data) may not be collected except (1) with opt-in consent from the consumer *for a specified purpose* **or** (2) to the extent necessary to provide a product or service that the consumer has requested.

Notably, the Act's consent requirements are strict. To be effective, consent must be obtained via a clear and affirmative act. Consent may not be obtained through the acceptance of general or broad terms of use, ambiguous acts such as closing a text box, or through "deceptive designs." Consent also must be obtained prior to the collection of covered data and must conspicuously disclose (1) the categories of consumer health data collected or shared; (2) the purpose of the collection or sharing of the consumer health data, including the specific ways in which it will be used; (3) the categories of entities with whom the consumer health data is shared (if applicable); and (4) how the consumer can withdraw consent from future collection or sharing.

Restrictions on sales and sharing. The Act also places strict limits on the sharing and selling of consumer health data. For example, the Act prohibits sharing consumer health data without obtaining separate consent and prohibits selling consumer health data without obtaining an even more onerous authorization.

Other data subject rights. In addition, the Act gives consumers several new rights regarding their covered data, including (1) the right to confirm whether a covered entity is collecting, sharing, or selling their consumer health data (including a list of *all* third parties and affiliates with whom such data has been shared or sold); (2) the right to withdraw consent; and (3) the right to have their consumer health data deleted. While the basic contours of these rights are similar to the rights enumerated under other consumer privacy laws, including California's Consumer Privacy Act (CCPA), Washington's new law includes fewer exceptions limiting the scope of those rights.

How Is the Act Enforced?

The Act is the first law of its kind, besides BIPA, to offer a wide-ranging private right action to enforce violations. The Act is enforced through the Washington Consumer Protection Act (WCPA), Wash. Rev. Statutes §§ 19.86, *et seq*. A violation of the Act is, by its terms, an "unfair or deceptive act in trade or commerce and an unfair method of competition" for purposes of the WCPA, meaning a consumer can sue under the WCPA for violations of the Act. Under the WCPA, prevailing parties may seek actual damages (including treble damages up to $25,000 per violation, in some cases), injunctive relief, and attorneys' fees. The WCPA authorizes class actions. In addition to a private right to action, violations are enforceable by the Washington attorney general, who can also investigate and litigate under the Act.

When Does the Law Go Into Effect?

The answer is not entirely clear. Most sections of the law will take effect on March 31, 2024. However, due to what may be clerical errors, some provisions applicable to regulated entities may become effective in July 2023. Entities that may be subject to the Act should consult experienced counsel to determine whether and when they will be required to comply.

This Update is the first in a series.

Authors

Nicola Menaldo

Partner
NMenaldo@perkinscoie.com 206.359.8000

Ryan Spear

Partner
RSpear@perkinscoie.com 206.359.3039

Bipasana Sakya Joshee

Counsel
BJoshee@perkinscoie.com 206.359.3285

Ida Knox

Associate
IKnox@perkinscoie.com 206.359.3473

Explore more in

Privacy & Security Technology Transactions & Privacy Law Healthcare

Related insights

Update

FERC Meeting Agenda Summaries for October 2024

Update

New White House Requirements for Government Procurement of AI Technologies: Key Considerations for Contractors