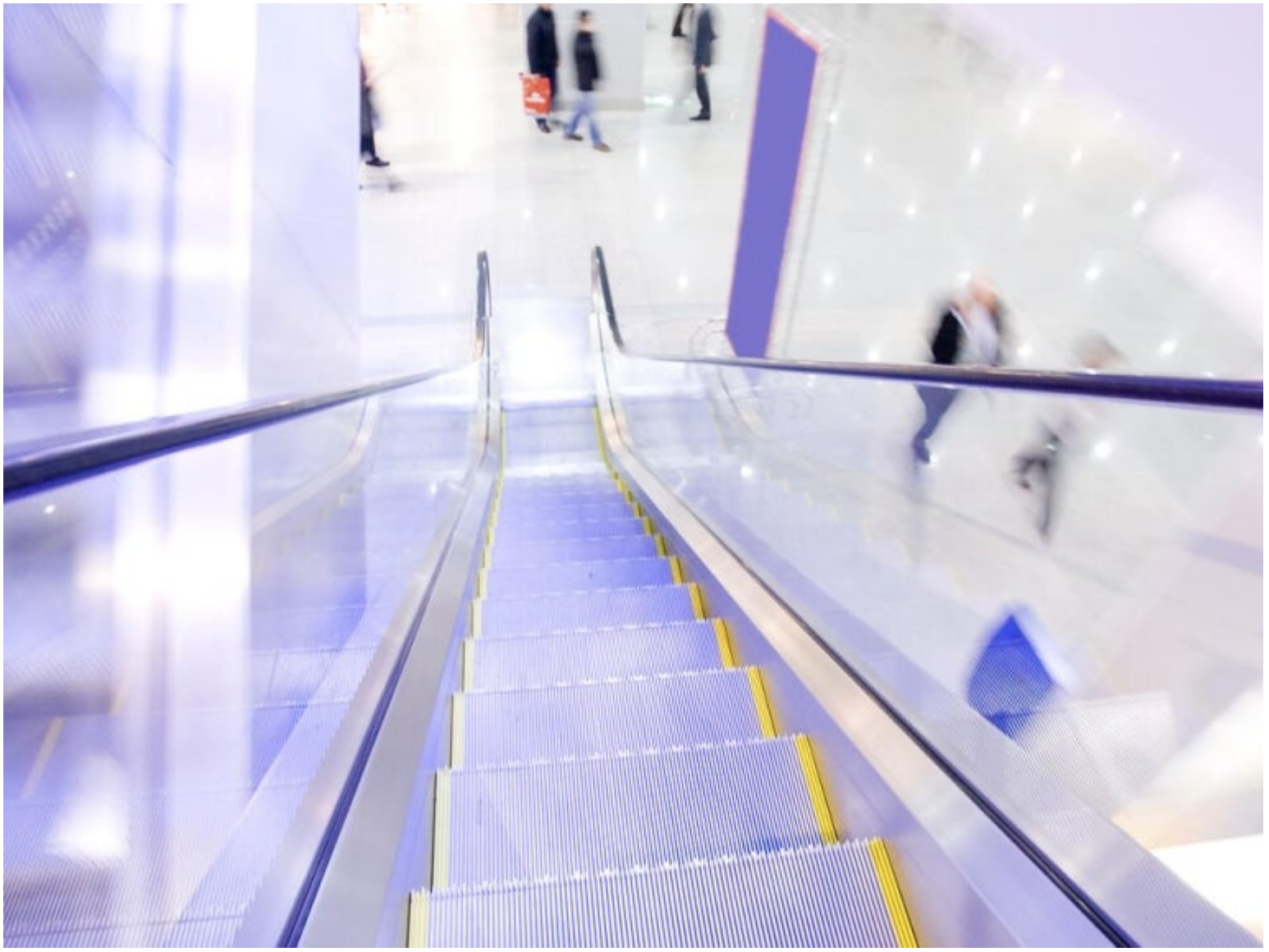

As detailed in Part 1 of this ongoing series, Washington Governor Jay Inslee signed the state's My Health My Data Act (the Act) into law on April 27, 2023. The Act is a first-of-its-kind law that creates new privacy protections relating to the collection, sharing, and selling of "consumer health data." Because of the Act's potentially broad reach and private right of action, this legislation is expected to have national implications and may be the most important American privacy law enacted since the California Consumer Privacy Act (CCPA).

In this installment, we provide an overview of the consumer rights bestowed by the Act and the obligations it imposes upon regulated entities and small businesses. Additionally, we identify some of the more important ambiguities and uncertainties of the Act and provide key takeaways for organizations seeking to comply. In our upcoming Updates, we explore the boundaries of "consumer health data" as well as how the Act defines "regulated entities" and "small businesses."

As noted in Part 1 of this series, the Act has multiple effective dates. Most of the provisions take effect on March 31, 2024. However, small businesses have an additional three months to come into compliance. Importantly, some provisions of the law may take effect earlier, including the restrictions related to geofencing, which become effective on July 23, 2023.

Who Qualifies as a "Consumer"?

The Act protects "consumers," defined as natural persons who reside in Washington state or whose consumer health data is collected or otherwise processed in Washington. "Collect" and "process" are broadly defined under the Act. "'Collect' means to buy, rent, access, retain, receive, acquire, infer, derive, or otherwise process consumer health data in any manner." "Process" means any operation or set of operations performed on consumer health data. Consequently, the Act might be interpreted to extend to data of Washington residents that is maintained outside of Washington and to any consumer health data that is collected or processed in Washington, regardless of the residency of the consumer.

Similar to several other state privacy laws, the definition of "consumer" is limited to persons acting in an individual or household context and expressly excludes those acting in an employment context.

What Rights Do Consumers Receive Under the Act?

The Act provides consumers with the following new rights:

- To confirm whether a regulated entity or a small business is collecting, sharing, or selling their consumer health data.
- To access their consumer health data, including a list of all third parties and affiliates with whom the regulated entity or the small business has shared or sold the consumer health data and an active email address or other online mechanism that the consumer may use to contact these third parties.
- To withdraw consent from the collecting and sharing of their consumer health data.
- To not be unlawfully discriminated against for exercising their rights.
- To appeal a regulated entity's refusal to action a rights request.
- To delete their consumer health data (with very limited exceptions).

Notably, the law's exemptions for responding to these rights may be narrower than those accorded by other states' privacy laws, so entities covered by the Act should consider updating the procedures they already have in place accordingly.

Business Obligations

Similar to other comprehensive state privacy laws, the Act lays out a series of compliance obligations for regulated entities and small businesses. We describe these requirements in more detail below.

Honoring Consumer Privacy Rights

As noted above, the Act grants consumers a series of privacy rights, including the rights to access and delete their consumer health data and to appeal an organization's refusal to honor a rights request. The law also prohibits discriminating against consumers for exercising their rights. The law reflects narrower exemptions for responding to these rights, potentially requiring organizations to update data subject rights request procedures they already have in place.

Opt-In Consent Requirements

Under the Act, organizations must obtain consent to collect consumer health data unless that collection is necessary to provide a product or service that the consumer has requested. The law also mandates a separate consent before sharing consumer health data. "Sharing" is defined to include most disclosures of consumer health data other than to service providers. These obligations will force companies to carefully consider whether their collection and sharing practices are necessary to provide a product or service and/or to adopt or update consents for such processing.

Valid Authorization Requirements for Data "Sales"

The Act imposes onerous requirements related to "sales" of consumer health data. Under the Act, a "sale" of data means the exchange of consumer health data for monetary or other valuable consideration. There are certain exceptions for what constitutes a "sale," including, most notably, disclosing consumer health data to a processor. The definition of sale under the Act mirrors the CCPA, which has been interpreted to cover a wide array of activity, including disclosures to third parties for purposes of displaying targeted ads. Regulated entities and small businesses that sell consumer health data are required to obtain valid authorization from consumers. The law sets a high bar for such authorization. First, the authorization must provide detailed disclosures about how and why consumer health data is sold, including the name and contact information of the person purchasing the consumer health data and how the data will be gathered and used by the purchaser. Second, authorizations are valid for one year, requiring regulated entities and small businesses to seek new authorizations after such time. Third, the Act requires sellers and purchasers of consumer health data to retain copies of all valid authorizations for six years. Because of the burdens associated with the authorization requirement, the Act might have the practical effect of precluding sales of consumer health data altogether.

Notice Requirements

The Act requires regulated entities and small businesses to maintain a consumer health data privacy policy that clearly and conspicuously discloses how such information is processed. The Act does not specify whether this consumer health data privacy policy can be folded into a company's general privacy policy or presented as a standalone privacy policy. However, regulated entities and small businesses must publish a link to the consumer health data privacy policy on the homepages of their websites and on any subsequent webpages that collect personal information. For mobile applications, the consumer health data privacy policy must be linked from within the app (such as from the settings menu) and on the app's download page.

Security and Access Requirements

The Act imposes a need-to-know access requirement for consumer health data. Regulated entities and small businesses must restrict access to consumer health data to employees, processors, and contractors for which access is necessary to provide a product or service that the consumer has requested or further the purposes for which the consumer provided consent.

Similar to other privacy laws, regulated entities and small businesses must also establish, implement, and maintain administrative, technical, and physical data security practices that, at a minimum, satisfy reasonable

standards of care within the regulated entity's industry to protect the confidentiality, integrity, and accessibility of consumer health data.

Contractual Obligations With Processors

The Act requires processors to enter into contracts with regulated entities or small businesses. Similar to other comprehensive privacy laws, such contracts must set out processing instructions and limit the actions a processor may take with respect to the consumer health data it processes on behalf of a regulated entity or small business. If a processor fails to adhere to these processing instructions and limitations, it will be considered a regulated entity in its own right and subject to all of the provisions under the Act.

Geofencing Restrictions

The Act prohibits implementing a geofence around an entity that provides in-person healthcare services if the geofence is used to identify or track consumers seeking healthcare services, collect consumer health data, or send notifications, messages, or advertisements to consumers about their consumer health data or healthcare services. The Act broadly defines a "geofence" as any technology that uses global positioning, cellular tower connectivity, radio frequency identification, cellular or Wi-Fi data, or other spatial or location detection to establish a virtual boundary around a physical location that is 2,000 feet or less from the perimeter of such location. Companies should note that, unlike many other provisions in the Act, the geofencing restrictions take effect at the end of July.

Enforcement

Consumers and the Washington attorney general are empowered to enforce the Act through an action under the Washington Consumer Protection Act (WCPA), Wash. Rev. Statutes §§ 19.86, et seq. The WCPA permits private plaintiffs to recover actual damages (which may be trebled up to $25,000 in appropriate cases) and provides for civil penalties of up to $7,500 per violation (which may be enhanced in certain cases). It also provides for costs and reasonable attorneys' fees to a successful plaintiff, although in actions brought by the attorney general, a prevailing defendant may recover fees as well. In actions brought by the private parties or the attorney general, injunctive relief is also available. For more detailed information on a consumer's private right of action, please see Part 1 of this series.

Takeaways

Because the Act is expected to significantly increase the compliance burden for companies that are already addressing their obligations under other state and federal privacy laws—and because some of its provisions take effect as soon as July 2023—we strongly encourage companies to promptly review their privacy practices to ensure they comply with the Act's requirements.

We will continue to monitor developments related to the law's implementation and publish corresponding analyses and Updates.

This Update is the second in a series.

Authors

David B. Robbins

Partner
DRobbins@perkinscoie.com 206.359.6745

April A. Goff

Partner
AGoff@perkinscoie.com 214.259.4954

Peter Hegel

Counsel
PHegel@perkinscoie.com 312.324.8683

Akua N. Asare-Konadu

Associate
AAsareKonadu@perkinscoie.com 206.359.3252

Explore more in

Privacy & Security Healthcare Biotechnology & Pharmaceutical Medical Device

Related insights

Update

Wrapping Paper Series: Issues and Trends Facing the Retail Industry During the Holiday Season

Update

CISA Security Requirements for Restricted Data Transactions Under New DOJ Rule