Washington to Pass Benchmark Privacy Protections for Consumer Health Data: The 10 Most Important Questions for Businesses

Insights
4.17.23

Washington State lawmakers just passed the most consequential privacy legislation in the country since the California Consumer Privacy Act (CCPA) was adopted in 2018, which will soon require businesses to take significant action in order to stay in compliance. The Washington Senate voted to approve the My Health My Data Act on April 5 after the House passed a similar bill in March. Once the two bills are reconciled, Governor Inslee is likely to sign it into effect, expanding the privacy rights for medical information – and expanding employer obligations – well beyond the federal HIPAA law. Here are the answers to the 10 biggest questions Washington businesses are likely to have – including what you need to do to comply.

1. What Entities Does the Act Cover?

HIPAA covers just a narrow host of entities including health providers and others in the healthcare sector. Washington's Act goes further than HIPAA and applies broadly to "regulated entities." This is defined as any legal entity that:

- conducts business in Washington or produces or provides products or services that are targeted to consumers in Washington;
- collects, shares, or sells consumer health data ("CHD"); and
- determines the purpose and means of the processing of CHD.

Like HIPAA, the Act also covers data processors. A processor can only process CHD pursuant to a contract with a regulated entity. If the processor violates or acts beyond the scope of its contract, it can be held liable to the same extent as a regulated entity for any violation of the Act.

2. What Data Does the Act Protect?

The Act protects CHD, defined as any information that links or reasonably links a consumer to their past, present, or future physical or mental health. This includes information about health conditions, treatment, diagnoses, surgeries, procedures, mental/behavioral health interventions, medication purchase or use, health measurements, gender-affirming care, reproductive and sexual health,

biometrics, genetic data, and location data showing a consumer's attempt to acquire or receive health services.

This last example (location data) could conceivably include any data showing a consumer's visit to a grocery store, pharmacy, or e-commerce website selling pharmaceuticals or contraceptives. It also includes any of this information that is extrapolated from non-health information.

Protected CHD does not include de-identified information or information that is either protected by HIPAA or other federal or state law, or which such laws expressly permit a regulated entity to collect. CHD used in properly conducted scientific, historical, or statistical research is also excluded.

3. Who Does the Act Protect?

The Act protects CHD of "consumers," defined as natural persons who reside in Washington or whose health data is collected in Washington. As Washington is a major hub for Cloud data storage, this definition could encompass many entities whose only connection to the state is the presence of their data on Washington-based Cloud platforms.

The Act's definition of consumers expressly excludes consumers acting in their capacity as employees. It is unclear at this time how a court will decide when a consumer has provided CHD purely as a consumer and when they have done so as an employee. It is also undetermined how this exclusion will affect an employer's liability when the employer acquires an employee's CHD from a regulated entity.

4. How Will the Act Be Enforced?

Any consumer injured by a violation of the Act can bring a private action for damages and equitable relief under the Washington Consumer Protection Act. The Washington Attorney General also may file an action to enforce the Act.

5. What Must Covered Entities Include in Their Policies?

A regulated entity must maintain and publish a Consumer Health Data Privacy Policy on its internet homepage that discloses:

- The categories of consumer health date the entity collects;
- The purpose of collection;
- The use of collected data;
- The sources of collection;
- The categories of data that may be shared;

- The entities with whom data may be shared; and
- A consumer's rights under the Act.

If a regulated entity violates its own policy in collecting, using, or sharing CHD, it must first inform consumers and obtain their affirmative opt-in consent.

6. When Can a Regulated Entity Collect Consumer Health Data?

Regulated entities will need to obtain a consumer's affirmative opt-in consent before collecting CHD, preferably in writing. Consumers may revoke this consent at any time.

The Act, however, provides several exceptions. Consent is not required when a regulated entity must collect CHD to provide a requested service or product, to detect or respond to security incidents, or to identify illegal activity.

Upon request from a consumer, regulated entities must confirm whether they are collecting CHD and allow the consumer to access their own CHD within 45 days. Regulated entities must provide this requested information twice annually for free but may charge a reasonable administrative fee should requests become excessive.

7. When Can a Regulated Entity Share or Sell Consumer Health Data?

A regulated entity can only share CHD internally with employees or processors on a need-to-know basis, consistent with the stated purpose for which the CHD was collected.

Regulated entities will only be able to share CHD externally with the consumer's specific consent. Again, however, the Act includes exceptions where necessary to provide a requested product or service, or for the security and safety.

Whereas a regulated entity can ***share*** CHD based on opt-in consent in various reasonable forms, they will require written consent before ***selling*** that CHD. That written consent must identify the CHD at issue, the name and online contact information for both buyer and seller, the purpose of the sale, the buyer's intended use of the data, a statement that provision of goods and services is not conditional on the consumer granting consent, and a statement that the CHD may be redisclosed by the buyer to third parties without the protection of the Act.

Such written consent is valid for one year, and the consumer may revoke it at any time. Regulated entities must retain copies of these written consent for six years from the date of signature, or when the consent was last effective, whichever is later.

As with information about collection, consumers may request confirmation whether a regulated entity is selling or sharing their CHD, and the regulated entity must respond within 45 days.

8. When Must a Regulated Entity Delete Consumer Health Data?

The Act includes a "right to forgotten" broader than any counterpart on the planet. Consumers have the right to ask regulated entities to delete their CHD without limitation. Even the European Union's General Data Protection Regulation (GDPR) allows a company holding data to decline a request for deletion when the company has a legal duty to preserve the records, or such preservation furthers various public interests.

The Act's broad deletion requirements may put regulated entities in a bind when a consumer requests deletion of CHD that the entities are legally obligated to maintain.

Facing a deletion request, regulated entities will have 30 days to comply, unless they can show that deletion would require restoring backup systems that may take longer. In complying with deletion requests, regulated entities will have to direct third parties who received the relevant data as well – so these requirements should be laid out in contracts with those third parties.

9. When Will the Act Come into Effect?

Assuming Washington's Governor Jay Inslee signs the Act, its current effective date is unclear. While some commentators have speculated that it could come into force in March 2024, the bill itself includes no effective date.

Unless this is revised, the Act will come into effect 90 days after the end of the current legislative session. As the session runs until April 23, the Act could come into effect as soon as July 22, 2023.

Fisher Phillips will be tracking this issue along with our general coverage of the Act.

10. How Can Regulated Entities Prepare?

We recommend you spend the next few months considering the following action steps.

- Review and revise your internet privacy policies;
- Review or develop your opt-in procedures;
- Implement annual consent reminders for data sales;
- Implement procedures to delete CHD upon request;
- Review your recordkeeping obligations to make policy determinations of when CHD data must be deleted on request; and
- Review where your CHD is stored as well as who processes it and how.

Need More Help?

For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's Consumer Privacy Team.

Fisher Phillips will continue to monitor consumer privacy legislation impacting employers and will provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insights to get the most up-to-date information direct to your inbox.

Related People

Jeremy F. Wood
Associate
Email

Annie Ziesing, CIPP/US, CIPP/E
Associate
212.899.9966
Email

Service Focus

Consumer Privacy Team

Privacy and Cyber

Related Offices

Seattle