Beyond HIPAA: What Businesses Need to Know as States Join Trend to Protect Consumer Health Data

Insights
8.11.23

For decades, medical providers and other covered entities have satisfied their health-data privacy obligations by complying with the federal Health Insurance Portability and Accountability Act (HIPAA) — but this is changing as more states pass their own laws to shield such information. Notably, these new laws often aim to protect data related to reproductive services following the SCOTUS abortion ruling in 2022. As a result, covered businesses are left with a patchwork of duties and possible liability, both within the states that enacted these new laws and beyond. Read on to learn more about new consumer health data protections in Washington, Nevada, and Connecticut — as well as seven steps you should consider taking now to comply.

Washington Leads the Way

Washington took the lead in this recent trend when Governor Inslee signed the Washington My Health My Data Act on April 27. Here are a few key points to note about the act, which takes effect on March 31, 2024, and notably excludes employee data:

Broad Coverage. The new law covers a broader category of entities than those already covered by HIPAA. It extends to all "regulated entities," defined as any entity that conducts business in Washington or targets products or services towards Washington consumers, collects shares or sells consumer health data (CHD), or determines the purpose or means of processing CHD. Data processors must also comply with the act unless they are acting under a contract with a regulated entity that ensures such compliance.

Included Information. Protected CHD includes any information that is reasonably linked to a consumer's past, present, or future physical or mental health. This includes information about health conditions, treatment, diagnoses, surgeries, procedures, mental/behavioral health interventions, medication purchased or used, health measurements, gender-affirming care, reproductive and sexual health, biometrics, genetic data, and location data within 2,000 feet of a physical facility showing a consumer's attempt to acquire or receive health services (thus potentially including pharmacies and gyms, amongst other locations).

Cloud Data. The Washington act grants a broad host of rights to natural persons residing 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 that are connected to the state only through the presence of their data on Washington-based Cloud platforms.

Excluded Data. The act's definition of "consumer" expressly excludes employees. Additionally, CHD excludes de-identified information or information that is either protected by HIPAA or other federal or state law, or information that is expressly permitted to be collected by a regulated entity. CHD used in properly conducted scientific, historical, or statistical research is also excluded.

Disclosures. A regulated entity must maintain and publish a Consumer Health Data Privacy Policy on its internet homepage that discloses the categories of consumer health data the entity collects, the purpose of collection, the use of collected data, the sources of collection, categories of data that may be shared, entities with whom data may be shared, and consumer rights under the act.

Consent. 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. However, the act 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.

Consumer Access. 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.

Sharing 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. To share CHD externally, regulated entities will require consumers' specific and separate consent, unless necessary to provide a requested product or service, or for security and safety. To sell CHD, such consent must be in writing, and identify the CHD at issue, online contact information for both buyer and seller, the purpose of the sale, the buyer's intended use of the data, a statement that the 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. Even still, such consent will expire after a year, and can be revoked at any time.

Deletion Requests. The act also includes an exceptionally broad "right to forgotten." Consumers can ask regulated entities to delete their CHD without limitation. Facing such a request, regulated entities have 30 days to comply, unless technical issues require more time. In complying with deletion requests, regulated entities must also direct third parties who received the relevant data to delete the data.

Enforcement. Unlike the statutes discussed below, both the State Attorney General and private consumers may bring actions to enforce its terms.

Nevada Law Includes Several Key Differences

The Nevada Legislature recently passed an amended version of Senate Bill 370, which will take effect on March 31, 2024, and is based in large part on Washington's act. However, there are several key differences that may ease the burden on businesses. Here's what you need to know about Nevada's new law:

Coverage. SB 370 applies to any entity conducting business in Nevada or targeting products or services towards Nevada consumers, which determines the purpose and means of processing, sharing, or selling consumer health data. Additionally, digital wellness services, gyms, and fitness companies might also have obligations under the act.

Broad Exemptions. Unlike Washington's act, however, SB 370 includes a broad host of exemptions. It excludes any entity already covered by HIPAA or the Gramm-Leach-Bliley Act, whereas Washington only exempts ***data*** that itself is already regulated by these statutes from further regulation. Law enforcement, police contractors, and certain gaming operators are excluded from complying with the Nevada act. And it does not apply to CHD that is used to:

- allow individuals to access or play on video game platforms; or
- identify the shopping habits or interests of a consumer, if that information is not used to identify the specific past, present or future health status of the consumer.

Additionally, the Nevada law does not apply to information regulated under the Social Security Act, Fair Credit Reporting Act, or Family Educational and Privacy Act.

Disclosures: As in Washington, entities covered by SB 370 must publish CHD privacy policies that describe, among other things:

- categories of CHD collected;
- how the collected CHD will be used;
- categories of sources from which the consumer health data is collected;
- categories of CHD shared with other entities;
- categories of entities with which the consumer health data is shared;
- purposes for collecting, using, and sharing CHD;
- how consumers may exercise their CHD rights; and
- whether third parties "may collect consumer health data over time and across different Internet websites or online services when the consumer uses any Internet website or online service of the regulated entity."

Consent. SB 370 generally prohibits the collection and sharing of CHD without the consumer's affirmative, voluntary consent (with separate consent required for collection and sharing) and prohibits the sale of CHD without the consumer's written authorization.

Included Information. SB 370 covers the same categories of CHD protected by the Washington act, including biometric, geolocational, and derived information. It defines geolocational data somewhat more narrowly than Washington, covering any such data showing a consumer's location within 1,750 feet of a physical facility. It specifically prohibits the use of geolocational data for marketing purposes.

Limits and Exclusions. Whereas the Washington Act grants rights to any resident of that state or person whose CHD was collected in Washington, Nevada's act only applies to natural persons who actually requested a product or service from a regulated entity. It excludes any person acting in their capacity as an employee or government agent.

Consumer Access. As in Washington, Nevada's act empowers consumers to access a list of all third parties their CHD has been sold to or shared with; to stop a business from processing, sharing, or selling their CHD, to have their CHD deleted (as in Washington, without limitation); and to confirm if a covered business under the act is sharing, collecting, or selling their CHD.

Deletion Requests. Should a consumer request deletion of their CHD, covered businesses must comply and notify affiliates, contractors, and processors of the request within 30 days. They must respond to the consumer no later than 45 days after the request is authenticated.

Enforcement. The state attorney general may impose financial penalties for noncompliance. A violation of the act is considered a deceptive trade practice under Nevada law. Notably, there is no private cause of action.

Connecticut Amends Data Privacy Act to Include Consumer Health Data

The Connecticut Data Privacy Act (CTDPA) was amended in June – shortly before its July 1 effective date — to impose further duties on organizations that collect and use consumer health data. Here are the key factors to consider:

Included Information. Connecticut defines CHD as "any personal data that a controller uses to identify a consumer's physical or mental health condition or diagnosis, and includes, but is not limited to, gender-affirming health data and reproductive sexual health data." As in Nevada, the law covers the collection of geolocational data up to 1,750 feet, and only from a physical location of a mental, reproductive, or sexual health facility.

Consent. Regulated entities must obtain consumers' opt-in consent before collecting, processing, or selling their health data.

Enforcement. The CTDPA lacks a private right of action. Until December 31, 2024, the Connecticut Attorney General shall take an educational approach. If a cure is possible, that office will issue a notice of violation to the regulated entity with 60 days to cure before taking any further action.

7 Compliance Steps to Consider Taking Now

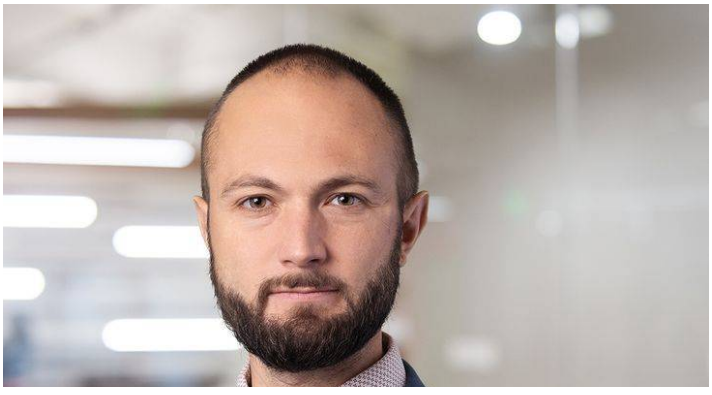
Plaintiffs' attorneys and state regulators, as well as the Federal Trade Commission, have ramped up their search for companies that may not be adequately protecting consumer health data. Class actions and steep enforcement actions have made headlines and underscore the need for companies to move towards compliance sooner rather than later. Accordingly, you should urgently consider taking the following seven steps:

1. Review and revise your internet privacy policies;
2. Review or develop your opt-in procedures;
3. Implement annual consent reminders for data sales;
4. Implement procedures to delete CHD upon request;
5. Review your recordkeeping obligations to make policy determinations of when CHD data must be deleted on request;
6. Take steps to limit employee access to CHD on a need-to-know basis, consistent with policies drafted for that purpose and industry best practices; and
7. Review where your CHD is stored, as well as who processes it and how.

Conclusion

For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's Consumer Privacy Team. We will continue to monitor consumer privacy legislation impacting employers and will provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox.

Related People



Jeremy F. Wood
Associate
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Related Offices

Las Vegas

Seattle