Health Data Privacy: What We're Hearing

Aaron J. Burstein, Alysa Z. Hutnik, Laura Riposo VanDruff

March 12, 2024

U.S. privacy developments are moving quickly, but *health* data privacy is racing forward. Companies that come into contact with consumers' health data need to track and respond to a variety of developments. Most notably, these include Washington's My Health My Data (MHMD) Act, a similar law in Nevada, "sensitive data" and "sensitive personal information" requirements under comprehensive state privacy laws, and FTC enforcement actions and guidance that assert that a broad range of health data is sensitive. How a company responds to these developments is likely to be iterative given the lack of clarity or harmonization with these requirements, and substantial resources required to implement changes.

In terms of what is visible, regulators expect companies to make detailed, specific disclosures and obtain opt-in consent for most health data collection, use, and sharing. Getting these disclosures and consents right, however, requires a lot of preparatory work, starting with identifying health data that a company controls.

A few steps can be helpful in managing this uncertainty. First, adopting a framework to classify health data will lead to greater consistency and efficiency in this cornerstone compliance activity. Second, taking a clear-eyed view of the difficulty of obtaining a consent will help set realistic business expectations for the use of health data in this challenging regulatory environment. Third, documenting a health data privacy program will help to maintain the program over time and demonstrate compliance to regulators and commercial partners.

Framework for Data Classification: Is It Health Data?

For many companies, determining whether they process health data, and which elements of their data inventories constitute health data, is a daunting task. The exercise can involve reviewing thousands of variables, segments, or personal data elements.

At present, there is little regulatory guidance and no common taxonomy of health data definitions, making it difficult to benchmark. In addition, health data definitions vary across state and federal regulators, and adopting a national approach based on the broadest definition might be infeasible from a business perspective.

A few strategies can help manage the uncertainty:

- **Work from explainable factors.** Using factors that capture the overlap among different health data definition will be helpful in establishing consistent classifications and educating business stakeholders about when they're encountering health data. Factors that are based on the current range of health data definitions include:

- Does the data reveal a ***specific*** health condition?
- Does the data reveal a ***past*** or ***present*** health condition?
- Does the data relate to a ***specific consumer***?
- Does the data relate to a ***sensitive*** health matter?
- What kinds of ***harm*** (if any) could use or disclosure of the data reasonably cause to an individual.
- Particularly important for Washington and Nevada: Does the data relate to a consumer's past, present, or ***future*** health status?

- **Think holistically about classification.** Classifying health data in a vacuum can lead to trouble. Regulatory definitions are broad, and it may be insufficient to analyze a data element on its own. Rather, it may be necessary to consider the *purpose* of using or disclosing a specific data element bears on whether it is health data. It's also possible that a data element is "health data" when under the control of one entity but not another. Understanding the business processes, contractual commitments, data sources, and other factors surrounding potential health data is therefore critical. In many cases, there won't be a clear answer to whether a data element is health data. Being able to identify what's clearly in, and out, of this category allows businesses to devote more time to genuinely debatable cases.
- **Think about scalability and sustainability.** A one-time classification effort, even if it encompasses thousands of variables, might be feasible for many companies. Maintaining these classifications over time is another story. For companies with relatively static data inventories, maintenance over time is likely less challenging. When inventories change quickly, however, a case-by-case review of data elements might be impractical. Consider setting a cadence for review and how one might designate privacy champions within the business to apply the framework on an ongoing basis, in coordination with legal support.

There's Consent, and Then There's *MHMD Consent*

While the FTC and states with comprehensive privacy laws are moving toward requiring opt-in consent for most health data processing, MHMD creates particularly stringent consent requirements. The difference between MHMD and other health data regulations lies not in the *action* required for consent – it must be voluntary and unambiguous – but in the narrow scope of consent that is permissible and the details that must be disclosed to make the consent informed. (Although other regulators have not been as explicitly restrictive, there is a clear trend in this direction, as we discussed in our recent posts on the FCC's one-to-one consent order.)

Specifically, a business must disclose the following to obtain consent to collect or share consumer health data:

1. The categories of consumer health data collected or shared;
2. The purpose of the collection, including the specific ways in which it will be used;
3. The categories of entities with whom the consumer health data is shared; and
4. How the consumer can withdraw consent from future collection or sharing of consumer health data.

Meeting these standards might be infeasible for many businesses, particularly those that do not have direct relationships with consumers.

MHMD's requirements to *sell* consumer health data are even more stringent. The law requires a valid ***authorization***, which must include the name and contact information of the purchaser, be signed by the consumer, and expire within one year of signatures, among other requirements. Obtaining an authorization outside of limited circumstances is unlikely to be practical for most companies.

The main alternative to consent or authorization is to restrict collection of health data under MHMD to what fits under the necessity exception. Washington has not provided further guidance on the scope of this exception, but we expect regulators to interpret this exception narrowly.

Documentation is Key

We get it: companies are reluctant to create discoverable documents that might be used to prove that they misinterpreted health data regulations. The alternative, however, is far worse and could be used to support the argument that a company systemically failed to govern health data in a reasonable fashion. It can also lead to inconsistent practices within a company and time-consuming back-and-forth between business and legal teams.

Key documents include health data definitions, consent requirements, partner diligence processes, data subject request procedures, and model contract terms. Many of the consumer health data practices that should be documented are likely extensions of current privacy programs and processes, such as data protection assessments.

Of course, some discussions warrant protection under attorney-client privilege. Maintaining clear lines between discussions that provide legal advice and operational guidance to business teams will help draw defensible lines around privilege.

* * *

The acceleration in health data privacy regulation is adding to demands to privacy teams that are already stretched thin. Confronting the breadth of "health data" definitions and the impact of these regulations on business operations in the absence of regulatory guidance is especially challenging. For better or worse, the boundaries of health data privacy regulations will be clarified through enforcement and MHMD's private right of action. In the meantime, understanding these laws' core purposes and keeping a close watch on statements from regulators will be helpful starting points to setting compliance priorities.