Updates
November 13, 2023
The New Health Privacy Landscape—Out of the Frying Pan and Into the Fire

Just a few years ago, the legal landscape governing health-related personal information was relatively simple: Protected Health Information (PHI) was regulated under Health Insurance Portability and Accountability Act (HIPAA), a discrete set of rules that applies to a specified set of healthcare plans, clearinghouses, and providers.

While narrowly targeted statutes governed particular types of health data and the Federal Trade Commission (FTC) maintained broad oversight over personal information, any data that could reveal or suggest a health condition or treatment was largely free of regulatory scrutiny and litigation risk. Today, by contrast, the privacy of health-related personal information is under close scrutiny by the FTC, the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights, and state regulators.

Heating Up

As the primary federal privacy regulator, the FTC has long asserted that health information is sensitive and, thus, warrants heightened protection. Its recent focus on consumer health data is nevertheless unprecedented. In the past year alone, the FTC announced several privacy-related enforcement actions against entities in the healthcare ecosystem, broadly conceived. Three such actions—*GoodRx*, *BetterHelp*, and *Easy Healthcare (d/b/a Premom)*—were based on the alleged sharing of health-related information through ad tracking technologies like pixels or cookies. In a blog post discussing these enforcement actions, the FTC advanced a broad definition of health data as "anything that conveys information–or enables an inference–about a consumer's health," stating that, "the fact that a consumer is using a particular health-related app or website – one related to mental health or fertility, for example–or how they interact with that app (say, turning 'pregnancy mode' on or off) may itself be health information." Further, in both the *GoodRx* and *Premom* complaints, the FTC asserted for the first time that disclosures to ad platforms that were intentional but not authorized by the data subjects constituted a "breach of security" under the FTC's Health Breach Notification Rule. Meanwhile, an in-progress enforcement action against data broker Kochava alleges that the sale of precise location data that indicates visits to medical

providers (among other kinds of sensitive data) may violate the law—suggesting another potential avenue for future health-related enforcement.

The agency is also flexing its rulemaking muscle. In May, it released a Notice of Proposed Rulemaking to update the Health Breach Notification Rule. As part of that process, the agency has proposed to broaden the scope of the rule to more clearly cover health-related services provided through applications and other new technologies, and to expressly state that unauthorized disclosures may constitute security breaches under the rule, which would bring disclosures like the ones alleged in *GoodRx* and *Premom* under the rule.

Into the Fire

In parallel, several states have entered the health privacy space by passing new consumer health laws, led by Washington's My Health My Data Act (MHMD). MHMD features (1) broad definitions of "consumer health data" and of "physical or health status," with correspondingly narrow, entity-level exemptions, making nearly all businesses potentially subject to its requirements; (2) onerous obligations that could effectively ban certain processing of health information, particularly for advertising-related purposes; and (3) enforcement through a private right of action and by the Washington Attorney General. Considered together, these features of MHMD sweep troves of consumer health data that previously fell outside the proverbial frying pan that was HIPAA directly into the fire of health privacy regulation and litigation. For example, even businesses that merely process the "consumer health data" of Washington residents might now risk class action litigation for activities that were previously commonplace, such as sharing data about purchases of over-the-counter medication, health supplies, or diet-related purchases or collecting information about consumer's visits to health-related websites and applications. For more detail, see our previous overview of the law.[1]

While MHMD reflects the current high watermark for consumer health privacy in the United States, Washington is not alone. Shortly following MHMD's passage, New York and Nevada passed their own (albeit narrower) consumer health privacy laws, and Connecticut updated the Connecticut Data Privacy Act to include new protections for health data. Although specific definitions and restrictions vary across these laws, all four statutes restrict the use of geofencing technology—technology that uses any form of spatial or location detection to establish a virtual boundary around a specific physical location or to locate a consumer within a virtual boundary—to (1) identify or track a consumer seeking healthcare services; (2) collect consumer health data from consumers; or (3) send notifications, messages, or ads related to consumer health data or healthcare services. Because these restrictions are the first of their kind, entities should quickly review their use of precise geofencing technology and assess whether its usage could come under the laws.

Old Rules, New Tech

Not one to be left behind, HHS, which is responsible for enforcing HIPAA, has also issued new guidance regarding the use of pixel-tracking technologies by HIPAA-regulated entities and joint warnings with the FTC to 130 healthcare providers alerting them that tracking technologies integrated into their websites and/or mobile applications may be improperly disclosing personal health data to third parties in violation of recent HHS guidance. That guidance, which is currently being challenged as applied to unauthenticated websites and applications, underscores that some—but not all—data that HIPAA-regulated entities send through ad-tracking technologies may constitute PHI, *even where they lack a patient relationship with the visitor to their site or app*. Where such data constitutes PHI and is transmitted by a HIPAA-regulated entity, HHS takes the position that HIPAA rules apply, including the requirements to enter into Business Associate Agreements with the technology providers; where they do not, they are likely to fall under one or more of the other legal regimes discussed in this Update.

Takeaway

The legal landscape is heating up when it comes to health privacy—between new HHS guidance, evolving FTC enforcement practices, and an array of new state consumer privacy laws. These developments will transform the health privacy landscape and bring new entities, new data, and new activities in scope for potential litigation and regulatory enforcement. Because many of these laws and guidelines are already in effect and the PI- and health-related litigation and regulatory landscapes are active, all entities, regardless of whether they are subject to HIPAA, should review their consumer health privacy practices to ensure they are complying with this new legal landscape and brace for the new world of consumer health privacy.

Endnotes

[1] See the following Updates for further information on MHMD: Part 1: *Washington State Joins the Biometric Litigation Fray*; Part 2: *Consumer Rights and Business Obligations*; Part 3: *The Wide Reach of the New Washington Privacy Legislation*; Part 4: *Washington State's New My Health My Data Act Will Likely Result in Insurance Coverage Disputes*.

Authors

Explore more in

Technology Transactions & Privacy Law Privacy & Security My Health My Data Act (MHMD) Technology & Communications Healthcare

Related insights

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law

Update

February Tip of the Month: Federal Court Issues Nationwide Injunction Against Trump Executive Orders on DEI Initiatives