June 26, 2023

The Wild West of Health Data for Sale? Not So Fast!

by Jon Neiditz

Background: The pandemic era ushered in exponential growth in the use of remote capabilities for all areas of life, with one of the most critical being the rise in telemedicine. Along with that expansion came an explosion in health-related apps and services, many of which purported to be "privacy-compliant," "HIPAA-compliant," or made similar claims. Many did not make *any* such claims. While the U.S. has a statutory framework in place to protect health information (HIPAA and the HIPAA Rule), HIPAA contains numerous exceptions, does not apply broadly outside the healthcare provider, carrier and health plan contexts, and is considered to be outdated and inadequate in some ways for the purposes of regulating the world of digital health apps and services. In 2016, Office of Civil Rights of the Department of Health and Human Services (HHS) provided scenarios for health app developers designating the developers regulated business associates depending on the degree and manner of consumers' interactions with providers or health plans (perhaps unintentionally driving health apps away from integration with the health care system).

What's changed?

- Health apps (and "health-adjacent" apps) long predated the pandemic – and several had notably come under fire for data sharing practices – but the stampede of health apps handling particularly sensitive data drastically expanded during that time, especially reproductive and mental health related services.
- The pandemic coincided with the U.S. Supreme Court's reversal of the longstanding reproductive rights decision *Roe v. Wade* in 2022 (*Dobbs v. Jackson Women's Health Organization* (the *"Dobbs"* decision)), instantly rendering any reproductive related information all the more sensitive. As many states moved to criminalize and restrict abortion, health and location data became central to potential criminal or civil liability surrounding reproductive health services provision and access.
- The rapidly advancing capabilities of AI, including generative AI, to profile and target individuals based on relatively few data points has the potential to amplify these issues and speed up the timeline for change.
- While the *Dobbs* decision was devasting for reproductive rights and called into question Fourteenth Amendment doctrine on privacy, it has also spurred a renewed scrutiny and action on sensitive data protection from agencies and jurisdictions at the federal and state level.
- Regulators, in particular the FTC, have increased their focus on aggressively wrangling the wild west of health data sales and sharing, with significant fines, crushing data deletion orders, and high-profile takedowns. The FTC is actively seeking to shore up its authority to enforce against health apps, and is using all current tools at its disposal, including enforcing for the first time the authority given it in 2009 over

non-HIPAA-covered health breaches discussed below, to enforce against data privacy and security violations. Notably, the FTC is moving beyond simply requiring more transparency around data use, and actively requiring violators to stop unauthorized sharing and get rid of ill-gotten data and algorithms based on that data. The Department of Justice (DOJ) and HHS have also been active in issuing guidance and assisting regulators like the FTC in enforcement efforts. HHS issued formal guidance on the use of online tracking technologies that dramatically expands the regulation of such technologies as business associates, covering apps tracking health or anything else, and much broader than the 2016 scenarios but still always ultimately tying back to a HIPAA-covered entity.

- States, also in the absence of federal legislation to increase protection for sensitive health data, have begun to put a lasso around the collection and sharing of health information, enacting new legislation targeting the rise of unauthorized use (and some states acting specifically to protect reproductive health access).

Takeaways:

- Organizations should review and refresh their data maps to see if their data practices fall within the scope of the new state laws and make any necessary adjustments.
- Organizations should carefully assess existing privacy policies to make sure they are transparent and accurate with respect to any representations about how sensitive data is collected, used and disclosed, and determine whether additional consent procedures are needed or if certain sharing practices should be curtailed altogether. The FTC has indicated that the traditional notice and consent regime does not protect the interests of individuals, as lengthy privacy policies place too much of a burden on people who may have little or no choice in actually utilizing such services.
- Organizations should assess their collection practices around sensitive health data and determine if this can be minimized or eliminated to the extent possible.

Want more? Read on for a closer look at some of the key regulatory, legislative, and judicial developments in the health data sharing rodeo.

Sharing Health Data: Who could forget the New York Times breaking a story on Target's pregnancy prediction analytics? However, the issues now span from overcollection to the widespread sharing of health data with third parties, service providers, and apps who have very little restriction on how health data may be used and most of which are not covered by HIPAA. Many services have geolocation enabled, and are able to match numerous other data points, allowing for a range of inferences and alarmingly comprehensive profiles. As noted, those inferences drastically increased the risk for those involved in or seeking reproductive health services post-*Dobbs*, as a wave of states began to ban or enact strict limitations on access to abortion, reproductive and transgender healthcare. Previously, such data was at risk of being sold or shared indiscriminately among private entities, but now implicate the risk of litigation and criminal penalties as well.

Recent Regulatory Action: While these uses enjoyed a period of virtual free reign, regulators have taken notice and are actively enforcing against such violations. The FTC reiterated reproductive health and health data as part of its mandate, has been actively patrolling health apps and recently issued a series of significant enforcement actions related to health data app data use and sharing.[1] Many of the FTC enforcements relate to misleading claims about how information is being used, which falls squarely within FTC jurisdiction e.g., Section 5 of the FTC Act, but the FTC is now making us of the full range of its powers, targeting companies for "unfair" as well as "deceptive" data practices. In addition to Section 5, the FTC enforces the Safeguards Rule, Health Breach Notification Rule, and Children's Online Privacy Protection Rule (COPPA), among others. In a new development, the FTC brought two cases under the existing Health Breach Notification Rule (HBNR), in addition to the FTC Act, the *GoodRx* (Feb. 2023) and *Premom* (May 2023) cases described below. The FTC is now seeking to shore up its authority under the HBNR. The agency issued a policy statement in 2021 that health apps and similar tech are covered by the HBNR, and proposed changes in May 2023 to the HBNR to codify that position and fend off challenges to its enforcement power going forward.[2] The changes include expanded definitions of covered health data, "health care provider" and "health care services or supplies".

In May 2023, the FTC filed a complaint against Easy Healthcare Corporation, developer of the Premom fertility app, with which it reached a proposed settlement banning the sharing of health data with third parties for advertising purposes, in addition to several fines. *U.S. v. Easy Healthcare Corp.* ("Premom") alleges that Premom promised not to share highly sensitive data (e.g., menstrual cycles, reproductive health conditions, ovulation data), but actually shared data with a leading technology provider, AppsFlyer, and two firms in China. In *U.S. v. GoodRx Holdings, Inc.* ("GoodRx") and *In the Matter of BetterHelp, Inc.* ("BetterHelp"), the FTC penalized GoodRx and BetterHelp for sharing sensitive heath data without affirmative express consent for primarily advertising purposes.

In *GoodRx*, the telehealth and prescription drug discount provider stated in its privacy policy it would never disclose personal health information with advertisers or other third parties, but it used data it shared with social media companies to target users with personalized advertisements and failed to report unauthorized disclosures to such advertisers and other third parties.

In *BetterHelp*, the online counseling service promised consumers during the sign-up process it would not use or disclose their personal health data except for limited purposes, such as providing counseling services, but it actually shared consumers' email addresses, IP addresses, and health questionnaire information with third parties for advertising. As a result, GoodRx and BetterHelp were required to pay $1.5 million and $7.8 million penalties, respectively, were each permanently prohibited from sharing user health information with third parties for advertising, and required to obtain users' express consent before disclosing user health information with applicable third parties for other purposes. The FTC previously penalized period tracker app Flo Health in 2021, which launched an "anonymous mode" in 2022.

In addition to the FTC's public commitments to enforcing violations related to sensitive health data post-*Dobbs*, various other executive branch entities made similar statements, including the White House and the Department of Health and Human Services (HHS). President Biden issued the Executive Order on Protecting Access to

Reproductive Healthcare Services in July 2022, and HHS issued guidance on protecting patient privacy post-*Dobbs*.[3]

States attorneys general and state consumer protection agencies have also taken fairly aggressive action against health data sharing. Although too extensive to cover in this alert, one key example is Premom's recent settlement with several state attorneys general in conjunction with the FTC's settlement. Connecticut, Oregon and the District of Columbia all reached settlements with the Premom developer, and a separate class action in Illinois may settle as well.

Legislative Controls: Legislators at the federal level struggle to pass significant privacy legislation or to update the HIPAA framework, but states have begun to act in the absence of federal leadership in this space. At least nine states have currently enacted comprehensive privacy laws, most or all of which contemplate additional protections and restrictions on the use of sensitive personal data, including health data. Texas and Florida have also passed privacy laws and several states regulate certain areas of health related data such as biometrics or genetic information, e.g., Illinois' Biometric Information Privacy Act (BIPA).

However, likely the most significant state legislation is Washington's My Health, My Data Act (MHMD), which, while not a comprehensive privacy law (that is, it does not regulate ALL "personal data") contains very broad definitions of health data and covered organizations, and has the potential to have the most substantial impact on privacy in the U.S. to date. It was intended to close the gap in federal privacy law (HIPAA) post-*Dobbs*. MHMD applies to any legal entity that conducts business in Washington or targets products or services to Washington consumers, and determines the purpose and means of collecting, processing, sharing, or selling **consumer health data.** "Consumer health data" is broadly defined as "personal information that is linked or reasonably linkable to a consumer that identifies the consumer's past, present or future physical or mental health status."[4] MHMD features a private right of action and carries requirements for impacted entities, including a consumer health data privacy policy, signed authorization for sale of consumer health data, and other enhanced consumer rights. Processing of consumer health data requires consent for collection or sharing or must be necessary to perform a service. MHMD also makes it unlawful to utilize a geofence around a facility that provides in-person "health care services." The effective dates are drafted in a somewhat ambiguous manner, but the obligations are intended to impact larger companies first. Depending on whether the effective dates are clarified, some of the provisions could come into effect as early as July of 2023.

Modeled on Washington's MHMD, Nevada just passed a consumer health data privacy bill on June 5, 2023 (pending governor's signature at the time of this writing). SB 370 has a slightly narrower definition of "consumer health data" in that it covers data that the entity actually "uses to identify" the person's health status, and thus appears to be geared toward entities that have a business use for the data. There is no private right of action, and there are exemptions for HIPAA and GLBA-covered entities, among other specific exclusions. SB 370 also prohibits geofencing medical facilities within 1,750 feet.

New York and Connecticut have also passed laws related to geofencing healthcare facilities, a practice which notably came to light in, for example, 2017, when the Massachusetts AG settled with a marketing company over

their use of technology that identified when people crossed a secret digital "fence" by an abortion clinic and sent them targeted advertising related to abortion alternatives.[5] A number of other states and the District of Columbia have acted to protect abortion access, although they do not necessarily address data privacy as such.

Judicial Activity: While the full scope of court activity around reproductive health data is too extensive to cover in this alert, a number of cases are making their way through the judicial systems in various states. Many involve issues beyond privacy, and several trends bear watching, including cases related to third party tracking, particularly due to the prevalence of this type of data sharing and sale, and the extent to which criminal prosecutions (and other legal and non-legal forms of persecution or harassment) related to reproductive health now depend upon access to data and inferences relating to a person's health status, geolocation, and digital footprint.

We expect to see further judicial and regulatory activity with respect to sensitive information, so it is important to closely monitor any such developments and understand how they may impact your organization.

Footnotes

---

[1] See FTC, *Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data*, July 11, 2022, https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

[2] FTC, *FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule*, May 18, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposes-amendments-strengthen-modernize-health-breach-notification-rule.

[3] U.S. Dept. of Health and Human Services, *HHS Issues Guidance to Protect Patient Privacy in Wake of Supreme Court Decision on Roe*, June 29, 2022, https://www.hhs.gov/about/news/2022/06/29/hhs-issues-guidance-to-protect-patient-privacy-in-wake-of-supreme-court-decision-on-roe.html.

[4] This includes a wide range of examples.

[5] See Massachusetts Office of the Attorney General, AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities, April 4, 2017, https://www.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts-healthcare-facilities.