WILMERHALE

FTC Emerges as Leader in Health Privacy Enforcement

AUGUST 4, 2023

Over the past year, the Federal Trade Commission (FTC) has emerged as a leading actor in the health privacy enforcement space, spearheading enforcement actions, policy statements, and regulatory changes all aimed at companies' (mis)uses of consumer health data and related information types. In the past several weeks, the FTC has taken two additional actions that further signal its emergence as a leading regulatory force for health data. First, on July 20, the Commission issued a joint letter with the Department of Health and Human Services' Office for Civil Rights (HHS OCR) pertaining to the use of online tracking technologies by hospitals and telehealth providers. Second, on July 25, the Commission published a blog post highlighting key takeaways from its recent health data enforcement actions. Taken together, these actions indicate that the FTC's recent interest in health privacy enforcement is no fluke — rather, companies should expect the FTC to remain an active regulator in this space for the foreseeable future. Accordingly, companies that handle health data (as broadly defined by the FTC) — particularly those outside of the scope of HIPAA — should ensure that their health data privacy and security programs are robust.

In this post, we summarize key points and takeaways from the FTC's joint letter with HHS and enforcement takeaways blog post. We are happy to answer any questions you might have about your company's health data compliance programs. To keep up-to-date on the FTC's latest health privacy enforcement activities, be sure to subscribe to the WilmerHale Cybersecurity and Privacy Law Blog.

Joint Letter With HHS

The FTC and HHS OCR circulated a letter to approximately 130 hospital systems and telehealth providers regarding potential risks associated with the use of online tracking technologies. In particular, the letter highlights that these technologies — which the letter describes as "gather[ing] identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users" — may be present on a given entity's website or app and "impermissibly disclosing

consumers' sensitive personal health information to third parties." The letter goes on to raise the following key points:

- **HIPPA compliance required in use of online tracking technologies.** The letter makes clear that HIPAA-regulated entities "are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules." Here, the letter directs HIPAA-regulated entities to a December 2022 bulletin published by HHS OCR, which offers more guidance on how these online tracking technologies intersect with the HIPAA Rules.
- **Non-HIPAA entities must still monitor their use of online tracking technologies.** The letter emphasizes that, even if a company is not subject to HIPAA, it must still "protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule" — another indication of the FTC's interest in regulating uses of health data by non-HIPAA entities. The letter further warns that that obligation applies even if the company's website or app is designed by a third party, and even if the company does not use any of the information obtained through its trackers for marketing purposes.
- **Companies should ensure compliance with relevant legal obligations.** The letter concludes by warning that recipients using online tracking technologies should "review the laws cited in this letter and take actions to protect the privacy and security of individuals' health information."

Enforcement Takeaways Blog Post

The FTC's recent post on its Business Blog ("Protecting the privacy of health information: A baker's dozen takeaways from FTC cases") highlights several themes from the Commission's recent health privacy enforcement actions (including those in the BetterHelp, GoodRx, and Vitagene cases, among others). As the FTC tries to build new law through its guidance and enforcement actions, this post is an effort to protect the reach of its new activity — by clearly and explicitly telling companies about the FTC's views on these issues. Key points from this post include:

- **Broad Definition of "Health Information"**: The post makes clear that the FTC views the bounds of "health information" as extending beyond prototypical examples like medical history or lists of medications. Rather, the FTC views "health information" as encompassing "anything that conveys information – or enables an inference – about a consumer's health." Notably, that definition could include information such as location data, or even the mere fact that an individual is using a particular service (e.g., an online therapy app).
- **Use of Tracking Technologies**: Picking up where its joint letter with HHS left off (see above), the FTC emphasizes that companies should be wary of how they collect and use consumers' sensitive health information. In particular, the post highlights companies' use of tracking technologies such as pixels and software development kits, warning that the use of these and similar technologies "may run afoul [of] the FTC Act [and the Health Breach Notification Rule] if they violate privacy promises or if the company fails to get consumers' affirmative express consent for the disclosure of sensitive health information."
- **Affirmative Express Consent**: The post highlights the need for companies to obtain affirmative express consent from consumers before disclosing their sensitive health information. And such consent, the FTC counsels, can only follow "a clear and conspicuous disclosure of all material

facts" — "[h]idden euphemisms" and "enigmatic references" buried within lengthy privacy policies are insufficient.

- **Robust Data Privacy and Security Programs**: The FTC encourages companies to implement formalized data privacy and security programs to protect health information. Specifically, the Commission counsels that such programs should include data protection safeguards, risk assessments, and employee training and supervision, as well as policies pertaining to data retention, purpose, and use limitations. Notably, as a preliminary step, the post recommends that companies perform data flow analyses to understand "how data comes into your company and how it moves once it's there."
  • HIPAA Compliance Claims: The FTC cautions companies about making claims to be HIPAA compliant, noting that only HHS OCR has the authority to make such determinations. Accordingly, the FTC counsels, companies should be wary of making claims to be HIPAA complaint and should cast a skeptical eye towards entities that claim to provide HIPAA seals and certifications.
- **Special Attention to Sensitive Data**: The post highlights the FTC's particular focus on biometric data (including genetic data), as well as reproductive health information, highlighting enforcement actions and guidance that the Commission has spearheaded in these arenas.

These efforts reflect the FTC's continuing efforts in the health privacy space to expand its reach and define its views of inappropriate practices outside the scope of specific laws and/or regulations. While there may be many ways for impacted companies to challenge these views, it will be critical for any company gathering and using any data that the FTC views as health data to be evaluating these views and assessing how the company's practices fit within these new standards being defined by the FTC.

Authors

Kirk J. Nahra
PARTNER
Co-Chair, Artificial Intelligence Practice
Co-Chair, Cybersecurity and Privacy Practice
kirk.nahra@wilmerhale.com
+1 202 663 6128

Ali A. Jessani
SENIOR ASSOCIATE
ali.jessani@wilmerhale.com
+1 202 663 6105

Samuel Kane
ASSOCIATE
samuel.kane@wilmerhale.com
+1 202 663 6114