wiley

ALERT

FTC and HHS Caution Hospitals and Telehealth Providers on Tracking Tech

July 28, 2023

This month, the Federal Trade Commission (FTC) and the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights sent letters warning about privacy and security risks related to online tracking technologies used by hospitals and telehealth providers. These warnings continue the FTC's increased focus on health data and could indicate further enforcement efforts in this area.

Specifically, on July 20, 2023, the FTC, in conjunction with HHS, sent letters to hospital systems and telehealth providers stating that there are privacy and security risks with online tracking technologies in websites or apps that may be disclosing consumers' sensitive personal health data to third parties without permission. An accompanying FTC press release is available here.

The letters reiterate that entities covered by the Health Insurance Portability and Accountability Act (HIPAA) must comply with HIPAA privacy, security, and breach notification rules. The letters also explain that entities not covered by HIPAA still have obligations to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule (HBNR). In particular, the agencies' letters cite recent FTC enforcement actions against companies that have allegedly disclosed personal and health information to third parties without authorization. For example, the FTC alleged that GoodRX and BetterHelp engaged in such practices, claiming that the alleged actions violate both Section 5 of the FTC Act and the HBNR.

Authors

Dorthula H. Powell-Woodson
Partner
202.719.7150
dpowell-woodson@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

FTC and Consumer Protection

Health Care

Health Care Risk Management and Regulatory Compliance

Privacy, Cyber & Data Governance

These actions stem from greater FTC scrutiny of health data. In a 2021 policy statement, the FTC stated that the HBNR requires "vendors of personal health records" – which include health apps and connected devices – to notify affected individuals when such entities experience a "breach of security" of covered health-related data. The policy statement explains that a "breach" means acquisition of that information without users' authorization, and this includes both privacy and security "breaches." In May 2023, the FTC released a Notice of Proposed Rulemaking that would build on the policy statement and this expanded breach definition.

The joint agency letters signal further potential FTC enforcement related to the unauthorized disclosure of consumer health data, even if not done for marketing purposes. Importantly, the FTC is underscoring that, even if a company is not covered by HIPAA – or it collects health-related data in ways that fall outside of HIPAA coverage – it still has health data privacy and security obligations, including when using a website or mobile app developed by a third party. Additionally, the agencies are working together to address these practices regardless of whether a particular practice falls under the authority of the FTC or HHS. Companies dealing with any kind of health data should ensure that they fully understand and appropriately address the potential disclosure of health information to third parties, including through analytics tracking technologies in their websites and apps.

***

Wiley's Privacy, Cyber & Data Governance and Health Care Risk Management and Regulatory Compliance teams have helped companies of all sizes from various sectors proactively address risks and address compliance with new privacy laws. Our FTC team represents companies in responding to FTC requests and regularly advocates before the agency. Please reach out to any of the authors with questions.