wiley

NEWSLETTER

With Health Apps on the Rise, Consumer Privacy Remains a Central Priority

February 2021

Privacy In Focus®

During the COVID-19 pandemic, many Americans have increasingly relied on digital health apps to manage their personal health and wellness. These apps include traditional telehealth apps through which patients can complete virtual visits with their medical providers, but they also include other apps that provide consumers with non-clinical resources to manage their health and wellness journeys. The total number of apps that are available for download is in the hundreds of thousands. Searching terms like "glucose tracker," "calorie counter," "fertility," or "fitness plan" yields a lengthy list of options from which consumers can choose, and new apps are constantly being developed.

While convenience and functionality likely heavily influence consumer decision-making around the use of health and wellness apps, consumer privacy is potentially an overlooked consideration. Significantly, many health apps are not required to be compliant with the privacy and security requirements enumerated under the federal Health Insurance Portability and Accountability Act (HIPAA), as the apps often do not contain medical records held by a doctor's office or other health care providers and affiliates. (Wiley's data protection team has a handy primer on the scope and applicability of HIPAA.) With that said, mobile health apps may be subject to the less widely known federal Health Breach Notification Rule, which requires vendors of unsecured health information, including mobile health apps, to notify users and the Federal Trade Commission (FTC) if there has been an unauthorized disclosure of health information.

Practice Areas

Digital Health
Health Care
Privacy, Cyber & Data Governance

Even where federal law may be inapplicable, some state privacy laws provide protections to consumers that go beyond the protections outlined in HIPAA. So health and wellness app developers will need to exercise considerable care in ensuring that their apps comply with applicable state law and also meet federal regulatory expectations concerning the handling of personal information. Under the privacy laws of various states, including, for example, Texas, New York, and Massachusetts, any person or entity that obtains or stores protected health information (even if that person or entity is not a health care provider or affiliate) is required to implement certain privacy and cybersecurity controls designed to prevent the inadvertent disclosure of personal health information. In addition, certain states have passed (e.g., California) or are close to passing (e.g., Virginia) broad privacy laws that protect a wide range of personal information, including health information.

With the California Attorney General's settlement with Glow, Inc., in September 2020, and the FTC's settlement with Flo Health, Inc., in January 2021, mobile app developers find themselves navigating a challenging regulatory landscape. The developers of these fertility health apps allegedly failed to honor the privacy commitments that they made to their consumers, and the settlements involve a range of significant monetary and injunctive relief provisions. In a blog post relating to the Flo settlement, the FTC provided five compliance tips to health app developers, and those are worth repeating.

- "**When it comes to health information, wear kid gloves.** Health-related apps can offer benefits to consumers, but only if companies clearly disclose how consumers' personal information will be used and scrupulously substantiate the privacy claims they convey to consumers."
- **"Your privacy representations must line up with how your app operates behind the scenes – and must stay in line over time."**
- **"Consider third parties' terms of service."**
- **"Live up to the standards you agree to when you choose to participate in a privacy program."**
- **"Honor your privacy promises and exercise particular care when it comes to highly sensitive personal health information. Period."**

Health and wellness apps have substantially enhanced the ability of consumers to manage their health from their home, but app developers should avoid rushing an app into distribution before taking the steps necessary to implement strong controls to protect personal health information. To the extent that health information is shared with third parties, necessary disclosures should be clearly made to consumers and authorizations obtained, where required.