GT GreenbergTraurig

Alert | Health Care & FDA Practice

August 2023

FTC Urges Companies to Protect Sensitive Health Data

Go-To Guide:
• Changes in FTC regulation and enforcement increase the burden on companies that engage with sensitive health data (meaning companies that collect, use, or process sensitive health data), and the FTC expects these companies to be responsible for the proper use of that data. • The FTC has recently taken action against companies that fail to protect sensitive health data or explicitly disclose data practices to consumers. • Companies need to remain vigilant in tracking the FTC's regulatory and enforcement activities along with state rules regarding privacy and consumer protection.

On July 25, 2023, the Federal Trade Commission (FTC) issued a list of key takeaways from its recent enforcement actions that relate to sensitive health data. The list comes on the heels of the FTC's issuance of a proposed rule that would expand the existing Health Breach Notification Rule (HBNR) to cover health applications ("apps") and other similar technologies. The proposed rule, along with the FTC's recent cases involving sensitive health data, signals the FTC's continued interest in regulating companies that are increasingly operating in the health space by handling consumer health data. Companies that engage with consumer health data should take note of the FTC's current positions and approach to enforcement.

Key takeaways from the FTC's "baker's dozen list" are highlighted below.

Companies that collect consumer health information have an obligation to protect that information.

Simply put, companies that collect or use consumer health information must take proactive steps to protect that information. This includes assessing and documenting any risks to that data and implementing safeguards to protect data. The FTC specifically notes the importance of having a written privacy program in place, as well as privacy training and supervision, and data retention, purpose and use limitations. Key to complying with this obligation is interweaving all technology decisions with privacy considerations.

Companies can face liability for unauthorized disclosure of health data, as well as receiving data that was improperly disclosed.

Recent cases, including those involving the companies BetterHelp, GoodRx, Premom, and Flo, highlight the liability risks for companies that actively share sensitive health data and do not adequately disclose those practices to customers. The FTC also makes clear that recipients of health data that has been improperly disclosed can also face liability under Section 5 of the FTC Act. Companies that receive data from other companies for purposes of advertising or marketing may be required to ensure they are not engaging in the unauthorized receipt, use, or onward disclosure of the sensitive information. To comply, companies should assess policies and practices that govern both the disclosure and receipt of sensitive information.

Technology and compliance teams should work in tandem.

The flow of health information across a company can create compliance concerns when teams are siloed and there is no broad understanding of how information comes in and out of the company. Compliance teams should work closely with technology teams so there is a clear understanding of the types of data in the company's possession at any given time, how that information is used and protected, and whether there are any compliance gaps in the data structure.

Companies that make HIPAA-related claims should ensure those claims are substantiated.

The FTC specifically cites problematic examples of companies offering health-related products and services that claim to be "HIPAA compliant" or "HIPAA secure," or that make similar claims that are deceptive to consumers. These claims can be deceptive when companies are not actually covered by HIPAA or are not actually HIPAA compliant (a determination that only the Department of Health & Human Services (HHS) Office of Civil Rights can officially make).

Similarly, companies that provide HIPAA compliance certifications and seals to other companies can also be liable for deceptive representations, particularly when certificates or seals are sold without substantiating that the companies who are buying the "label" are actually HIPAA compliant. The FTC states that "if a company provides a health-related seal or certification to others that falsely implies the recipient is covered by HIPAA, is complying with HIPAA, has been reviewed by a government agency, or has received government approval, both the certifier and the user of that false certification could be subject to FTC enforcement action."

To comply with concerns regarding HIPAA-related claims, companies should confirm they are covered by HIPAA before making related claims and also ensure that all claims can be substantiated. Companies seeking HIPAA-related certifications should fully vet the companies offering those certifications, seals, or

similar titles, and companies currently offering these services companies should assess the "products" they are offering to ensure they do not run afoul of the FTC or HHS.

Companies cannot reserve the right to make significant changes to privacy policies and must be upfront with customers about data practices.

Specifically, companies cannot use a broad privacy policy to reserve the right to change health data practices such that a customer's continued use of services constitutes consent to the changes. Customers must explicitly agree to a company's data-sharing practices.

Companies must also ensure they are using clear and specific language when disclosing data practices to customers. Broad terms in privacy practices, such us "disclosure of information about the use of services," do not provide consumers with a distinct understanding of exactly how a company may be using their health data, and consumers therefore cannot consent to that use. Companies should be as precise as possible when disclosing this information.

Further, the FTC makes clear that companies can be liable for deceiving customers by withholding information. Companies must disclose all material information to consumers about how sensitive health information is used and disclosed.

Companies that collect biometric data, as well as reproductive information, should be especially concerned with keeping that information safe.

Given the sensitive nature of this information, the FTC is particularly concerned about how companies are protecting biometric data (including voice, video, and DNA information), and data related to reproduction (particularly information collected by fertility-tracking applications). Companies that handle this type of information should be particularly vigilant about protecting customer data.

Looking Ahead

The FTC's recent actions, both on the enforcement and regulatory fronts, indicate they are focused on company use of sensitive health data and will hold companies accountable that fail to comply with FTC requirements. Companies that engage with this type of data should assess current compliance practices and address any noted gaps before issues arise that could carry liability.

Authors

This GT Alert was prepared by:

- Eleanor (Miki) A. Kolton | +1 202.331.3134 | koltonm@gtlaw.com
- Tess Dillon Meyer | +1 202.533.2319 | Tess.Meyer@gtlaw.com