Coping with the Clampdown: FTC's New Guidance for Health Data Privacy

Coping with the Clampdown:

FTC's New Guidance for Health Data Privacy

In recent years, the Federal Trade Commission (FTC) has emerged as a formidable enforcer in the healthcare privacy arena, taking action against companies like Flo Health, BetterHelp, GoodRx, Premom, and Vitagene for inadequate protection of consumers' sensitive health data. This has included using its broad authority under Section 5 of the Federal Trade Commission Act and enforcing its Health Breach Notification Rule. This Rule, which was long overlooked, has gotten significant attention of recent FTC activity, because it fills a gap by addressing businesses that may fall outside the narrower reach of the Health Insurance Portability and Accountability Act (HIPAA), including health and fitness apps and other consumer platforms or online products or services.

As a consequence, it has become critical for businesses that collect, use, store or disclose consumer health data to fully understand and implement practices to protect consumer health data privacy and security. In late July 2023, the FTC provided new practical guidance to help businesses stay within evolving regulatory guidelines and maintain the trust of their consumers. Here are some of the main points:

Changing a Privacy Policy Retroactively: The FTC warns against businesses relying on provisional agreements within thei privacy policies, where consent to future changes is assumed based on continued use of the service. Similarly, securing consumer approval to allow the company to make extensive alterations at will to its privacy policy does not equate to adequate consumer consent. A prominent case illustrating this is Vitagene (a genomic testing company) where as part of the proposed settlement with the FTC, the Director of the FTC's Bureau of Consumer Affairs stated: "The FTC Act prohibits companies from unilaterally applying material privacy policy changes to previously collected data." Building on previous actions like those against Gateway Learning (a company selling educational products for children) in 2004 and Facebook in 2012, the FTC identified provisional agreements as deceptive, even before they are implemented. The lesson here is that announcing broad future data-sharing practices without clear consumer agreement can lead to potential regulatory scrutiny.

Misleading Euphemisms: Clear and unambiguous disclosure of data practices is vital for businesses. Using vague terms or euphemisms in privacy policies, such as merely mentioning the "disclosure of information about the use of the services" can risk being construed as deceptive by the FTC. Instead, it should be explicitly stated if a company shares health information with third-party advertising companies. According to the FTC's lawsuit against Henry Schein Practice Solutions, Inc., a provider of dental software solutions, the company claimed their customers' data was securely "encrypted." However, it later shared this same supposedly secure information with third parties. Similarly, in the BetterHelp case, the company represented to customers that their sensitive conversations with counselors and personal information were considered "Protected Health Information," when it fact it used this information for their own advertising and shared this data with third parties, including Facebook and other online advertisers. To maintain transparency and avoid potential violations, companies should exercise caution when making similar descriptive claims about sensitive health information that can easily be misinterpreted by consumers as assurances not to divulge personal information.

Beware of Making Misleading HIPAA Claims: Companies should be wary of using terms such as "HIPAA Compliant" or "HIPAA Secure," even if they are compliant with HIPAA's legislative stipulations. Such labels can mislead consumers into assuming an official certification that does not exist. In reality, only the Department of Health & Human Services' Office for Civil Rights can formally confirm a company's HIPAA compliance. The FTC has also raised red flags over entities not directly regulated by HIPAA, but which use phrases such as "HIPAA Safe" to convey a sense of robust data security. For instance, the FTC took action against SkyMed, a travel emergency services provider, for its usage of a "HIPAA Compliance" seal prominently displayed across every page of its digital platform. These declarations leverage the common misperception about HIPAA as an overarching assurance of privacy, despite its protections not being as comprehensive as generally believed. Misleading claims and deceptive practices not only damage consumer trust but also risk severe legal consequences.

Liability for Omissions: Recent FTC actions also indicate that companies can face consequences not only for what they

say, but also for what they *fail* to say. For instance, the FTC's complaints against BetterHelp, Practice Fusion, and PaymentsMD, reference each party's "Failure to Disclose" how the company intended to share consumers' sensitive health information.

The Broadened Scope of Health Information

Examining the FTC recent guidance reveals a dramatic expansion in the definition of what can constitute protected health information. Traditionally, health data was thought of as information directly related to medical history, such as the content typically found on medical forms. However, with the advent of new technologies, the agency has spotlighted several critical areas:

Geolocation Data: Based on the FTC's guidance regarding health and location, even seemingly innocuous location data can unintentionally expose private health details. For example, regular visits to a cancer treatment center, family planning clinic, o addiction facility can be seized upon by data aggregators. These intermediaries, often operating without direct user interactior or app usage insight, can still deduce sensitive health information from precise location data and sell this data to third parties.

Health-App Interaction: The FTC's actions against companies like Easy Healthcare Corp. (the company behind the Premom ovulation tracker), BetterHelp, and Flo Health emphasize that interactions with health-related apps can also constitute health information. For instance, simply toggling a setting like "pregnancy mode" or selecting "Expectant Parent" within an app can convey critical insights into a user's health status. This has become increasingly important in the context of reproductive health privacy following the overturning of Roe v Wade's abortion protections.

Biometric Information: The FTC, in multiple policy statements, has consistently flagged the surging use — and potential abuse — of biometric data and associated technologies. As the realm of biometric technologies expands, details like an individual's facial features, iris patterns, palm veins, and fingerprints can be effortlessly captured. Highlighting this trend, Whole Foods (an Amazon subsidiary) has recently deployed palm vein scanning, a method reminiscent of fingerprinting, for their checkout process across hundreds of stores.

Moreover, some advanced systems purport to derive behaviors, traits, or even aptitudes from this biometric data. The FTC hasn't hesitated to act, taking on companies misappropriating voice data (Amazon/Alexa), video footage (Ring), and genetic information (Vitagene). In a similar vein, the Commission has expressed apprehension about the sprawling databases generated from genetic test kit sales, noting their allure for both malicious intruders and inadvertent breaches.

As technology evolves and the concept of health information and sensitive personal information expands, businesses need to think about their data practices. They must be mindful of the data they collect, how they collect, share and use it, what representations are made regarding the data, and the measures put in place to safeguard and store it. This recognition is essential in aligning with FTC regulations, ensuring user privacy and security, and mitigating legal risks.

Authored By:

Harry Nelson, Managing Partner, Nelson Hardiman

Tara A. Davidoff, Attorney, Nelson Hardiman

Yehuda Hausman, Law Clerk, Nelson Hardiman

Nelson Hardiman LLP

Healthcare Law for Tomorrow

Nelson Hardiman regularly advises clients on new healthcare law and compliance. We offer legal services to businesses at every point in the commercial stream of medicine, healthcare, and the life sciences. For more information, please contact nelsonhardiman.com