Arnold & Porter

March 15, 2023

FTC Announces $7.8 Million Fine as Part of Settlement With BetterHelp Regarding Health Information Privacy Practices

Enforcement Edge: Shining Light on Government Enforcement

By Emily A. Dorner, Nancy L. Perkins, Jami Vibbert, Jason T. Raylesberg

The FTC is not pausing its pursuit of charges concerning the allegedly unfair and deceptive sharing of patient data for advertising purposes. Just one month after the FTC's settlement with, and $1.5 million fine imposed on, GoodRx for violations of the Health Breach Notification Rule (HBNR) and Section 5 of the FTC Act, on March 2, the FTC announced a $7.8 million fine and proposed consent order with BetterHelp, Inc. for alleged violations of Section 5 of the FTC Act.

Specifically, the FTC alleged that, among other things, BetterHelp shared customers' sensitive health data with third parties such as Facebook and Snapchat for advertising purposes, contrary to online representations the company made to customers. In its complaint, the FTC asserted that these alleged misrepresentations amounted to violations of Section 5 of the FTC Act, which broadly prohibits unfair and deceptive practices harmful to consumers. Although the FTC did not allege that BetterHelp shared customers' medical records *per se*, the FTC alleged that BetterHelp uploaded personal health information in the form of the email addresses of all of its current and former clients to Facebook, so that Facebook could identify similarly situated consumers and target them with advertisements for BetterHelp's mental health services — which allegedly brought tens of thousands of new customers and millions of dollars of revenue to the company. Although the email addresses shared with Facebook were hashed (i.e., represented cryptographically with a sequence of letters and numbers that masked the underlying data), according to the FTC's complaint, BetterHelp knew Facebook would be able to undo the hashing to uncover the email addresses of individuals who visited the BetterHelp site for mental health counseling. In its press release, the FTC underscored that hashing "won't protect the privacy of consumers' information if third parties can un-hash the data," and stated that "personal information" may be "health information" simply due to the nature of the product or service (e.g., an email address is considered health information when the source of that email is an online health service).

Under the proposed consent order, BetterHelp must, among other things, (1) pay a fine of $7.8 million to be used to provide partial refunds to allegedly harmed customers (making this case the first FTC action to return funds to consumers whose health data was allegedly compromised); (2) cease sharing (a) identifiable information relating to the mental health of a consumer with any party for advertising purposes and (b) personal information with any party for the purpose of targeting the consumer to which the disclosed information pertains; (3) obtain affirmative, express consent before sharing any consumer's personal information with a third party; (4) direct third parties to delete the consumer health and other personal information that BetterHelp revealed to them; (5) limit how long the company retains personal and health information; and (6) put in place a comprehensive privacy program that includes strong safeguards to protect consumer data. The FTC warned in its press release, "[l]et this proposed order be a stout reminder that the FTC will prioritize defending Americans' sensitive data from illegal exploitation."

The FTC's back-to-back enforcement actions against GoodRx and BetterHelp underscore the FTC's commitment to protecting consumer health information and filling in perceived gaps to protect patient privacy when HIPAA doesn't apply. Organizations that deal with identifiable health information outside the scope of HIPAA therefore can expect that their privacy notices, as well as the manner in which they handle and share consumer health information, increasingly will be subject to FTC scrutiny. The FTC will be seeking to determine, among other things, if companies handling personal health information have sufficient policies and procedures to protect the information, including but not limited to technical, administrative, and physical safeguards to secure the information; restrictions on sharing of the information; and mechanisms to timely provide consumers with appropriate access to and control over their personal information. These compliance responsibilities call for companies' vigilance in evaluating and improving their privacy and data security practices and programs, as well as their records retention and information governance policies and procedures to ensure that their practices are reasonable, sufficiently protective, transparent, and consistent with any statements made to consumers or the public generally.

For questions about compliance with Section 5 of the FTC Act or other data privacy and protection issues, contact the authors or any of their colleagues in Arnold & Porter's Privacy, Cybersecurity & Data Strategy practice group.