

Blog Post

FTC Cracks Down on BetterHelp's Sharing of Health Information for Advertising

March 27, 2023

By [Jordan T. Cohen](#) and [Elizabeth F. Hodge](#)

Following its [February settlement with GoodRx](#), the Federal Trade Commission (FTC) has fired another shot across the bow in its ongoing campaign to protect consumers' digital health information. Earlier this month the FTC [announced a consent order with BetterHelp, Inc.](#), an online mental health counseling service, to resolve alleged violations of the Federal Trade Commission Act (FTC Act) related to the company's collection, use, and sharing of customers' health information.

This case is notable for several reasons, which we discuss below, but a key takeaway for health app developers is that the mere disclosure of a customer's email address or IP address to a third party, including advertisers, can be deemed a disclosure of health information when it is readily apparent to the recipient that the information relates to specific services, such as mental health counseling. The consent order is also notable for banning BetterHelp from sharing health data for advertising purposes, and, if finalized, would appear to be the first order requiring a company to pay partial refunds, totaling \$7.8 million, to consumers whose health information was disclosed.

The FTC's [complaint](#) against BetterHelp set forth the following allegations: (1) disclosure of health

Related People

[Jordan T. Cohen](#)
[Elizabeth F. Hodge](#)

Related Work

[Data Privacy and Security](#)
[Healthcare](#)
[Pharmacy, Drugs, and Medical Devices](#)

Related Offices

[New York](#)
[Tampa](#)
[West Palm Beach](#)

Health Law Rx

[Akerman Perspectives on the Latest Developments in Healthcare Law](#)

[Read blog posts](#)

information for advertising purposes; (2) deceptive privacy misrepresentations; and (3) failing to employ reasonable measures to safeguard health information.

Disclosure of Health Information for Advertising Purposes

To sign up for BetterHelp's services, consumers must create an account and fill out an intake questionnaire. Through this questionnaire, BetterHelp gathers information including the consumer's email address, IP address, and information about health status and history, such as the reason for seeking therapy services.

BetterHelp allegedly disclosed this intake information to numerous third party advertising platforms, including Facebook, Snapchat, Pinterest, and Criteo, and used it to market their services from 2013–2020. For example, between 2017 and 2018, BetterHelp allegedly provided Facebook with lists of over 7 million consumers' email addresses, and Facebook then matched over 4 million of these consumers with their Facebook accounts, targeting these individuals and similar users with advertisements. According to the FTC, consumers' email addresses are inherently health information because they indicate that their owners were seeking mental health services. BetterHelp also allegedly disclosed other intake responses such as whether the consumer had previously participated in therapy for targeted advertising purposes.

Like GoodRx, BetterHelp used various tracking technologies to obtain and subsequently disclose information, including through the use of tracking pixels. Understanding and addressing consumer tracking has become a priority for the FTC, which recently published a summary of the practice entitled *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*.

Deceptive Privacy Misrepresentations

The FTC further alleged that BetterHelp engaged in deceptive business practices by falsely promising that health information would stay private between the consumer and the counselor. Meanwhile, BetterHelp was allegedly providing information gleaned from the intake questionnaires to third parties for advertising purposes.

The intake questionnaire was displayed in the center of the homepage on the BetterHelp website, urging consumers to provide health information, while the privacy policy was in small, low-contrast writing at the bottom of the homepage. Throughout the intake questionnaire there were statements assuring users that their information was private, such as “Rest assured—any information provided in this questionnaire will stay private between you and your counselor.” The privacy policy was also deceptive because it did not mention that health information may be provided to third parties for advertising purposes. Further, the website featured a deceptive Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance seal, falsely representing compliance with privacy and security requirements.

The FTC claimed these deceptive privacy assurances were material to consumers since consumers would want this highly sensitive information to remain private, but had no reasonable way to avoid the harms due to BetterHelp’s repeated misrepresentations. The FTC also alleged that the weekly fees consumers paid for BetterHelp’s services included a “price premium” based on the company’s claimed privacy practices; i.e., the company was able to charge more for its services because customers believed that their data would be protected.

Failing to Employ Reasonable Measures to Safeguard Health Information

Finally, the FTC alleged that BetterHelp engaged in unfair business practices by failing to employ

reasonable measures to safeguard health information. For example, BetterHelp allegedly failed to train employees on how to protect information when using it for advertising and did not implement policies or provide notice to consumers on collection, use, and disclosure of health information. Further, BetterHelp did not contractually limit how third parties could use and disclose health information and merely agreed to third parties' general terms of service, which provided little to no restrictions on their use of the health information.

Notably, despite finding that BetterHelp impermissibly shared consumer health information with third parties, the FTC did not allege that the company violated the Health Breach Notification Rule (HBNR). In her concurring statement supporting the decision to forego alleging a violation of the HBNR, FTC Commissioner Christine S. Wilson explained that the information BetterHelp collects from its clients and provides to therapists on its platform is not a personal health record of identifiable information because it does not include records that can be drawn from multiple sources. The consumer provides their information to BetterHelp, but the company does not pull additional health information from other sources or vendors.

Proposed Consent Order

To resolve these allegations, BetterHelp agreed to a consent decree under which it must pay \$7.8 million for partial refunds to consumers who purchased counseling services from the company. This is the first time the FTC has required a company to pay partial refunds to consumers whose health information was disclosed. BetterHelp will also have to pay all costs and expenses associated with the independent redress monitor who will oversee disbursement of the refunds.

The consent decree also requires BetterHelp to:

- not disclose consumers' health information to third parties for advertising purposes;
- obtain consumers' affirmative, express consent before sharing their health information with third parties;
- properly represent the use of covered information;
- notify third parties who improperly received access to covered information and instruct them to delete it;
- provide notice to all affected users;
- establish and implement a privacy program that protects the privacy, security, availability, confidentiality, and integrity of covered information with privacy assessments by a third party professional; and
- submit certification and reports of proper compliance.

As is FTC practice, the settlement has a twenty-year term.

Takeaways

In addition to this action highlighting the FTC's enforcement priorities, there are a number of takeaways for health app developers, who should consider taking the following steps:

- Reconcile policies and practices. Developers should consider reconciling their privacy policies and privacy-related statements with their actual use and disclosure of customer data. A mismatch between policies and practices could create exposure under the FTC Act and, depending on the app, the HBNR and/or HIPAA.
- Review HIPAA "seals" and "certifications." Think twice before placing HIPAA "seals" or other indicators of HIPAA compliance on documents, websites, and apps, especially if you are not directly regulated by HIPAA.

- Evaluate your compliance staffing needs. The case also highlights the importance of appropriately staffing an organization with employees who have experience in data protection and data governance. According to the complaint, BetterHelp had delegated decision-making authority over its use of Facebook advertising to a junior analyst who had recently graduated college, had no relevant experience in safeguarding consumer health information, and had not received training.
- Analyze third party terms. Developers should review and, when appropriate, revise the terms of service and privacy policies of third parties that will be receiving sensitive data. In this case, BetterHelp simply accepted Facebook and other third parties' terms, thereby providing those third parties with near unfettered use of such information.

The FTC's focus on healthcare data privacy is likely to continue as consumer reliance on these platforms increases. We will continue to keep a close eye on developments in this space.

This information is intended to inform firm clients and friends about legal developments, including recent decisions of various courts and administrative bodies. Nothing in this Practice Update should be construed as legal advice or a legal opinion, and readers should not act upon the information contained in this Practice Update without seeking the advice of legal counsel. Prior results do not guarantee a similar outcome.