GUNDERSON DETTMER

Spotlight on Recent FTC Enforcement Actions: Is Your Users' Health Data Being Leaked Through Your Adtech?

Insights
March 29, 2023

In the past two months, the Federal Trade Commission ("FTC") has brought two enforcement actions against companies that collect health data stemming from such companies' use of sensitive health data for retargeted advertising purposes. In February, the FTC announced a first-of-its-kind enforcement action against GoodRx Holdings Inc. ("GoodRx") for allegedly sharing health-related information with Facebook, Google, and other advertisers without the knowledge or consent of GoodRx's users. Then, in March, the FTC announced that it had issued a proposed order banning BetterHelp, Inc. ("BetterHelp"), an online counseling service, from sharing consumers' health data for advertising purposes.

These enforcement actions highlight the aggressive approach that the FTC is taking towards policing the use of health data for advertising purposes. Companies that collect health data—especially those that participate in the online ads ecosystem—should take note of several key takeaways from these actions.

GoodRx Enforcement Action

On February 1, 2023, the FTC announced the first-ever enforcement action under the Health Breach Notification Rule (the "Rule"), which it brought against GoodRx, a telehealth and prescription drug discount provider. According to the complaint, GoodRx made promises to its users that it would only share their personal data with limited third parties and for limited purposes, that it would restrict third parties' use of such data, and that it would never share health data with advertisers or other third

parties. Instead, the complaint goes on, GoodRx repeatedly violated these promises by sharing sensitive user information—such as users' prescription medications and health conditions—with third party advertisers without providing notice of the sharing or obtaining user consent or authorization. Moreover, GoodRx permitted third parties that received users' health data to use and profit from the information for their own independent business purposes.

As a result, the FTC concluded that GoodRx:

1. **Violated the Rule by failing to notify relevant parties when it shared users' health data with third parties through tracking technologies hosted on its website and mobile app.** The Rule imposes breach notification requirements on companies that process consumer health data, but that are not subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), including health apps and connected devices that draw information from consumers and APIs. The Rule is deemed triggered when such entities experience a "breach of security." In a 2021 Policy Statement issued by the FTC, the agency adopted a broad view of the term, warning that disclosure of "sensitive health information without users' authorization, [] is a 'breach of security' under the Rule." In other words, a "breach" is not limited to cybersecurity incidents. According to the FTC, "[i]ncidents of unauthorized access, including sharing of covered information without an individual's authorization, triggers notification obligations under the Rule." This is the first time that the FTC has employed this expansive reading of the Rule to charge a company with a violation of the rule.

2. **Violated the FTC Act by engaging in several deceptive practices, including making false promises about the sharing of personal information**. The FTC noted that GoodRx displayed a HIPAA seal, falsely suggesting compliance with HIPAA, despite engaging in practices that were not compliant.

3. **Violated the FTC Act by engaging in unfair practices, including by failing to implement measures to prevent the unauthorized disclosure of health data.** Notably, the FTC determined that GoodRx engaged in an "unfair practice" by failing to provide notice and obtain consent before using and disclosing the health data of GoodRx's users for advertising purposes.

Under a proposed order, GoodRx would pay a $1.5 million penalty for violating the Rule and would be permanently prohibited from sharing health data for advertising purposes.

BetterHelp Enforcement Action

On March 2, 2023, the FTC announced a proposed order banning BetterHelp, an online counseling service, from sharing the health data of website visitors and users for advertising purposes. The order also requires BetterHelp to pay $7.8 million to provide partial refunds to users in settlement of charges that it disclosed users' sensitive information to third parties despite promising to keep the data private. According to the complaint, BetterHelp encouraged users to provide sensitive information, including information about their mental health and whether they were on any medications, by telling website visitors and users that it would not use or disclose their personal health data except for limited purposes, such as providing counseling services. However, BetterHelp subsequently provided email addresses, IP addresses and health questionnaire information of its users and website visitors to third parties, such as Facebook and Snapchat, for advertising purposes.

As a result, the FTC concluded that BetterHelp:

1. **Violated the FTC Act by making deceptive statements about its privacy practices, including representations that it would not disclose health data to third parties**. Similar to GoodRx, BetterHelp also made representations regarding HIPAA compliance, including by displaying a HIPAA seal, despite never having engaged a third party to review its HIPAA compliance.

2. **Violated the FTC Act by engaging in unfair business practices, including by failing to obtain website visitors' and users' affirmative express consent to collect, use, and disclose their health data for advertising purposes and failing to contractually limit third parties' ability to leverage health data for their own purposes.** This is a particularly notable departure from common practice as the general market standard in the US is to give users the possibility to opt out of such sharing, if any choice is offered at all. New state laws that come into effect in 2023 give consumers the right to opt-out of retargeted advertising and the processing of their sensitive information, subject to exceptions.

Key Takeaways

Any company that collects or otherwise handles health data should:

- Determine whether the Rule, HIPAA, state breach notification laws, or other state comprehensive privacy laws apply. Health data sits at the intersection of several regulatory regimes, and several new state privacy laws impose additional requirements with respect to the use and disclosure of health data. Also conduct a gap assessment of the company's existing privacy program and take steps towards compliance.

- Identify all online advertising tools and third-party tracking technologies (like cookies and pixels) employed on the company's website or mobile application. This includes understanding what information is disclosed and to whom. The FTC's enforcement actions signal that it is taking an expansive view of what constitutes "heath data," and that it expects companies to obtain consent before using or disclosing that data for retargeted advertising purposes.
- Ensure that agreements with service providers, including advertisers, that receive health data contain restrictions on how those third parties may use such data. Failure to have appropriate contractual language in place with service providers may result in a disclosure of personal information constituting a "sale" under U.S. state privacy laws.
- Consider whether it needs to obtain user consent or authorization before processing or disclosing health data.
- Avoid making representations that it is HIPAA compliant if it is not, in fact, compliant or if it has not engaged a third party to review its HIPAA compliance.
- Ensure that its public-facing policies are accurate and conspicuously posted. Any public representations regarding data collection, use, and sharing should be reviewed to ensure that they accurately reflect the company's practices.

How can GD help?

If you have any questions regarding this alert or need assistance with evaluating your obligations, please reach out to your Gunderson Dettmer attorney or contact a member of our data privacy team:

Anna Westfelt
Cecilia Jeong
Frida Alim
James Gately
Brian Hall

Related Services

Data Privacy

Featured Insights

FIRM NEWS

Gunderson Dettmer Commemorates 2025 Asian American and Pacific Islander Heritage (AAPI) Month

CLIENT NEWS

Brazilian Carbon Capture Company Mombak Announces $30M Financing

CLIENT NEWS

Africa B2B OmniRetail Announces $20M Financing

CLIENT NEWS

Glacier Announces Series A Financing to Expand Robot Recycling Fleet

CLIENT NEWS

Dataminr Announces $100M Investment Led by Fortress Investment Group

CLIENT NEWS

Omnidian Announces $87M Series C for Renewable Energy Performance

INSIGHTS

Splitting the Pie: How Savvy Founders Divide Ownership and Navigate Other Founder Equity Decisions

CLIENT NEWS

Chainguard Announces $356 Million Series D Led by Kleiner Perkins and IVP

INSIGHTS

Client Insight: California AI Transparency Act

INSIGHTS

Client Insight: Prepare for BE-10 Benchmark Survey of US Direct Investment Abroad

INSIGHTS

Tech Brew Interviews Aaron Rubin in “Where the legal battle stands around copyright and AI training”

CLIENT NEWS

Latin America Fintech Belvo Announces $15M Funding