

FTC brings enforcement action under Health Breach Notification Rule against fertility app

May 25, 2023 | Client Update | 5-minute read

In its second enforcement action under the Health Breach Notification Rule, the Federal Trade Commission (FTC) reinforces the administration's focus on protecting reproductive health data post-*Dobbs*.

Background

On May 17, 2023, the Department of Justice filed an eight-count [complaint](#) on behalf of the FTC against Illinois-based Easy Healthcare Corporation (Easy Healthcare), an online provider of home healthcare products, for sharing its customers' health data with third parties without the customers' knowledge or consent. In addition to Section 5(a) of the FTC Act, the complaint alleges violations of the Health Breach Notification Rule (HBNR) promulgated in 2009, which requires any "vendor of personal health records" to make various disclosures when the security of its individually identifiable health records has been breached. The FTC's application of the HBNR's "breach of security" provisions to intentional sharing of information mirrors the approach in the February 2023 enforcement [action](#) against GoodRx. The [proposed order](#) resolving the enforcement action against Easy Healthcare imposes a \$100,000 civil penalty and a ban on sharing health data with third parties for advertising purposes. The FTC voted 3-0 in support of the action. State Attorneys General in Connecticut, Oregon, and the District of Columbia announced a parallel settlement the same day.

In July 2022, two weeks after the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*, President Biden signed an [Executive Order](#) directing the FTC Chair to consider taking steps to protect consumers' privacy when seeking information about, and the provision of, reproductive healthcare services. The *Easy Healthcare* enforcement action, along with the FTC's prior [suit](#) against the data broker Kochava Inc. for selling geolocation data that could be used to track individuals' movements to and from sensitive healthcare locations,¹ reinforces the administration's focus on protecting reproductive health data in the post-*Dobbs* landscape.

Easy Healthcare's alleged practices

Easy Healthcare enables women to log information about their periods and fertility onto a free mobile app — the Premom Ovulation Tracker (Premom). According to the FTC, Easy Healthcare violated Section 5(a) of the FTC Act by sharing identifiable health data with third parties, including two China-based mobile analytics companies, despite representations to the contrary. Among other things, the FTC also alleges that Easy Healthcare (i) failed to restrict third-party use of customer data in accordance with its own policy; (ii) failed to implement reasonable privacy and data security measures, such as encrypting certain data shared with third-party developers or auditing the data collection and privacy practices of those developers; and (iii) failed to notify its customers that identifiable health data had been shared with third parties in violation of the HBNR. Under the terms of the proposed order, Easy Healthcare neither admits nor denies the allegations in the complaint.

Injunctive relief

The proposed order, which remains subject to court approval, requires Easy Healthcare to pay a \$100,000 civil penalty and places various limitations on Easy Healthcare's ability to share customer information. As noted above, the order permanently bans Easy Healthcare from sharing health information with third parties for advertising purposes. The order also prohibits sharing of health information with third parties for any purpose without the affirmative, express consent of the customer. The requisite consent is defined as "any freely given, specific, informed, and unambiguous indication of an individual's wishes demonstrating agreement by the individual, such as by a clear affirmative action" following clear and conspicuous disclosure (defined separately).

The proposed order, which has a 20-year term, also imposes a series of compliance obligations and accountability mechanisms, including:

- **Mandated privacy and security program.** Easy Healthcare must implement a comprehensive privacy and security program, including written safeguards that control for the internal and external risks to the security and privacy of customer information, within 60 days of entry of the order. Easy Healthcare must also designate a qualified employee to be responsible for the program and to report directly to the CEO.
- **Independent assessments.** Easy Healthcare must obtain periodic evaluations of the privacy and security program from an independent, third-party assessor with a mandate to identify any gaps or weaknesses or material noncompliance with program requirements.
- **Executive certifications.** Easy Healthcare must provide the FTC with annual statements from a senior corporate manager regarding the company's implementation of and compliance with all terms in the order.

Key takeaways

The *Easy Healthcare* enforcement action offers several key takeaways for companies that collect sensitive information, particularly information related to reproductive healthcare.

- In the last four months, the FTC has twice invoked the previously dormant HBNR against healthcare apps — consistent with a [September 2021 FTC policy statement](#) warning various categories of companies to comply with the HBNR.
- Any remaining doubt about whether the HBNR would become a meaningful enforcement tool evaporated on May 18, when the FTC [announced proposed changes](#) to the HBNR that would "clarify" that the Rule applies to healthcare app developers. The proposed changes would also clarify that the term "breach of security," as used in the HBNR, covers unauthorized disclosures, in addition to more traditional data security breaches.
- As in the [proposed order against GoodRx](#), the proposed restrictions here — including the permanent ban on sharing health information with third parties for advertising purposes — further underscore the FTC's heightened expectations for companies operating in the health space, particularly companies that are not subject to HIPAA. Moreover, the action targets reproductive health data — a top priority for the Biden administration post-*Dobbs* and similar to the 2021 [action](#) against Flo Health, Inc., for sharing health information collected via another fertility app.
- Finally, the action illustrates increased coordination among federal and state enforcement authorities. The same day the FTC announced its enforcement action, the Attorneys General of Connecticut, Oregon, and the District of Columbia [announced](#) a separate \$100,000 resolution with Easy Healthcare, which was negotiated and finalized in coordination with the FTC.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres

+1 212 450 4724
greg.andres@davispolk.com

Martine M. Beamon

+1 212 450 4262
martine.beamon@davispolk.com

Angela T. Burgess

+1 212 450 4885
angela.burgess@davispolk.com

Robert A. Cohen

+1 202 962 7047
robert.cohen@davispolk.com

James W. Haldin

+1 212 450 4059
james.haldin@davispolk.com

Paul J. Nathanson

+1 202 962 7055
+1 212 450 3133
paul.nathanson@davispolk.com

James P. Rouhandeh

+1 212 450 4835
rouhandeh@davispolk.com

Michael Scheinkman

+1 212 450 4754
michael.scheinkman@davispolk.com

Howard Shelanski

+1 202 962 7060
howard.shelanski@davispolk.com

This communication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's privacy notice for further details.

¹ The FTC's suit against Kochava was dismissed with leave to amend on May 4, 2023. See *FTC v. Kochava Inc.*, No. 22-CV-377, 2023 WL 3249809 (D. Idaho May 4, 2023).