ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy / Consumer Protection/FTC / Health Care ADVISORY ■

JULY 11, 2023

FTC Continues Its Focus on Health Privacy

By **Kathleen Benway**, **Sarah Beach**, **Sara Guercio**, *and* **Hyun Jai Oh**

Since the Federal Trade Commission (FTC) announced its first action involving the Health Breach Notification Rule (HBNR or "Rule") against GoodRx Holdings Inc. earlier this year, it has continued to focus on consumer privacy in the digital health care space, including by announcing its second action alleging violation of the HBNR and by proposing amendments to it.

Like its action against GoodRx, where the FTC alleged that the company violated the HBNR by sharing health data with third-party digital advertising and analytics providers in a manner that was inconsistent with its own privacy policy, in this most recent case, the FTC alleged that fertility tracking app Premom's sharing of health-related information with third-party advertisers amounted to a "breach" under the HBNR.

In its proposal to amend the Rule, the FTC states that the scope of "breach" under the Rule is not limited to cybersecurity breaches but also covers any unauthorized disclosure of personal health record (PHR) identifiable health information. Businesses dealing with health information that is not covered by the Health Insurance Portability and Accountability Act (HIPAA) should pay particular attention to the proposed amendments because the FTC's statement that the Notice of Proposed Rulemaking (NPRM) offers a clarification of the existing HBNR, including its broad definition of PHR, means that the FTC considers these "clarifications" to be in effect now. The FTC is accepting written comments on the NPRM through August 2, 2023.

Enforcement Action Against Easy Healthcare

On May 17, 2023, the FTC announced an enforcement action against Easy Healthcare Corporation, the developer of Premom, which is marketed as a fertility tracking app. In its complaint, the FTC alleged that Easy Healthcare violated (1) Section 5 of the FTC Act by failing to adhere to promises it made to Premom users in its privacy policy regarding its practices for sharing sensitive health information with third parties; and (2) the HBNR by failing to report such unauthorized disclosures as a security breach.

Specifically, the FTC alleged Easy Healthcare stated in its privacy policy that it would not share Premom users' health information with third parties without users' consent, Easy Healthcare would only share non-identifiable data when it did share data with third parties, and identifiable data was only used by Easy Healthcare for its own analytics and advertising purposes.

The FTC alleged that Easy Healthcare shared hundreds of thousands of Premom users' sensitive and identifiable health information, including information about their sexual and reproductive health, parental and pregnancy status, and pregnancy-related symptoms, with third parties for advertising purposes, including Google and two Chinese analytics providers.

Specifically, Easy Healthcare allegedly shared health information by allowing third-party software development kits (SDKs) to capture Premom users' interaction with the app that conveyed information about users' fertility and pregnancy. For instance, when a user recorded information related to her period through Premom, Easy Healthcare logged that information as "Log period-save" and shared it via third-party SDKs.

According to the complaint, the information captured by SDKs could also be used by other advertisers to track users across the internet and other apps. This means third parties could infer sensitive health information from what appears to be non-health information collected across multiple platforms, such as device identifiers, geolocation, and media access control addresses.

Finally, the FTC alleged that Easy Healthcare did not implement reasonable privacy and data security measures, including by failing to properly encrypt the data it collected, including users' health information. The FTC further argued that Easy Healthcare failed to conduct adequate assessment of third-party SDKs before deployment and to continuously monitor SDK publishers' terms and conditions and privacy policies.

The FTC issued a proposed order that, in addition to requiring a civil monetary penalty of $100,000, permanently bans Easy Healthcare from sharing user health information with third parties for advertising purposes and requires Easy Healthcare to submit annual compliance certifications for the next 20 years. The FTC voted 3–0 to refer the complaint and proposed order to the Department of Justice for filing.

Proposed Changes to the Health Breach Notification Rule

On June 9, 2023, the FTC published an NPRM seeking comment on the proposed changes to the HBNR that are drawn from the FTC's September 2021 statement on Breaches by Health Apps and Other Connected Devices. The FTC stated that the amendments would change or expand the HBNR in some cases and clarify the FTC's current interpretation of the Rule in other cases.

Notably, the FTC referenced the Department of Health and Human Services (HHS) guidance for "securing" electronic health information as the standard for encryption and also disclosed that it "sought informal input from staff at federal agencies … including staff at HHS." This NPRM therefore suggests a strong cross-agency coordination in the health care space and sheds further light on what the FTC considers to be unsecured PHR identifiable health information subject to the HBNR.

The NPRM clarifies the HBNR's applicability to health apps and other direct-to-consumer devices and technologies, such as fitness trackers, which, since the Rule's issuance in 2009, "have become commonplace." The FTC makes this clarification through the addition of two new terms, "health care provider" and "health care services or supplies," that include online services that provide health-related services or tools, such as mechanisms to track disease and health conditions, medications, sexual health, diets, and other health-related information.

Other notable changes and clarifications include:

- **Revising the definition of "breach of security" to clarify that it includes not just data breaches, but *any* disclosure of PHR identifiable health information not authorized by a consumer.** A breach of security therefore may include an app provider's voluntary disclosure of PHR identifiable health information that was not authorized by users.
- **Clarifying that a "personal health record" is "drawn from multiple sources" when it "has the technical capacity to draw information from multiple sources."** This clarification indicates that, when analyzing the scope of PHR, the FTC focuses on a product's technical ability rather than an individual consumer's use of the product.
- **Modernizing methods of notice by permitting email notification of consumers, expanding the contents of such notice, and providing examples of permissible notices.** The amendments would require applicable notice to include additional content, such as a brief description of the potential harm, description of third-party acquirers of information, description of information involved, and mitigating measures taken.

Businesses should note that the FTC posed some of these changes, such as the expanded definitions of "breach of security" and "personal health record," as "clarifications," meaning the FTC considers them to be currently effective. Other changes, including the modernization of the notice method and expansion of required contents of notice, would become effective 60 days after the publication of the final rule.

The FTC has also requested public comment in several areas, including whether the changes "sufficiently clarify the Rule's application to purveyors of health apps and similar technologies that are not covered by HIPAA," or whether the definition of "electronic mail" may lead to over-notification or might result in collecting more data than necessary. Public comments are due August 8, 2023.

Takeaways

Health privacy remains a priority focus for regulators. The FTC continues to take the position that a business's voluntary disclosure of health information to its service providers may constitute a breach under the HBNR. Therefore, businesses that collect and use health information should assess whether their sharing of health information can trigger liabilities under the HBNR.

Use of tracking technologies requires careful review and vendor due diligence. Failure to implement reasonable privacy and data security measures can expose businesses to liabilities under Section 5 of the

FTC Act. When implementing third-party tracking technologies, such as cookies, pixels, or SDKs, the FTC expects businesses to conduct ongoing vendor due diligence. Businesses should carefully review the terms and conditions and privacy policies of the vendors of tracking technologies to understand what rights those vendors have over the information exchanged through tracking technologies. Moreover, businesses should ensure there are adequate oversight mechanisms in place, for instance through contractual rights to conduct periodic privacy and data security audits.

The FTC considers some of the proposed changes to the HBNR to already be in effect. Notable clarifications include the HBNR's applicability to health apps and other health-related services or tools, expansion of the scope of breach of security, and expansion of the scope of PHR. Therefore, businesses should immediately assess the impact of these amendments, even though the FTC has not published the final rule.

You can subscribe to future ***Privacy, Cyber & Data Strategy***, ***Consumer Protection/FTC*** , and ***Health Care*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

ALSTON & BIRD

WWW.ALSTON.COM

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ +1 404 881 7000 ■ Fax: +1 404 881 7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
CHARLOTTE: One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ +1 704 444 1000 ■ Fax: +1 704 444 1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ +1 214.922.3400 ■ Fax: +1 214.922.3899
FORT WORTH: Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ +1 214 922 3400 ■ Fax: +1 214 922 3899
LONDON: 4th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44 0 20 3823 2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ +1 213 576 1000 ■ Fax: +1 213 576 1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ +1 212 210 9400 ■ Fax: +1 212 210 9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ +1 919 862 2200 ■ Fax: +1 919 862 2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ +1 415 243 1000 ■ Fax: +1 415 243 1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ +1 650 838 2000 ■ Fax: +1 650 838 2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ +1 202 239 3300 ■ Fax: +1 202 239 3333