

FTC's Health Privacy Efforts Raise Specter Of Litigation

By **Allison Grande**

Law360 (June 8, 2023, 6:07 PM EDT) -- The Federal Trade Commission is moving to step up its already aggressive policing of how health apps use and share sensitive personal information, but unresolved questions over the scope of the agency's authority is likely to spark challenges that could sharply curtail these efforts.

At its latest open commission meeting last month, the FTC proposed changes to its Health Breach Notification Rule that include clarifying that the rule applies to health apps and other similar technologies that collect or use consumers' health information. While the commission issued a policy statement in 2021 affirming these services are covered by the rule and has taken enforcement action against two such platforms, the rule change would formalize this stance and give the agency firmer footing moving forward.

"The proposed rulemaking leaves absolutely no room for confusion for entities that are trying to grapple with whether they are subject to the rule and would give more teeth to the 2021 policy statement," said Melissa Crespo, a partner at Morrison Foerster LLP. "For those that didn't necessarily pay attention to the FTC's signals that it's going to start using the health breach notification rule, this is obviously the biggest flag the commission could have waved to say, 'You better have your practices in order.'"

While the rule has been on the books since 2009, the FTC hadn't used it in an enforcement action until the commission in February accused digital health care platform GoodRx Holdings Inc. of "repeatedly" violating its promise to not share personal health information with Facebook, Google and other advertisers.

Then, the day before its May 18 open meeting, the commission announced that it would be wielding the rule for a second time in an enforcement action against fertility app Premom. The commission claimed that Premom shared users' sensitive personal information with third parties and failed to notify consumers of these unauthorized disclosures in violation of the Health Breach Notification Rule.

"It took a while for the FTC to take enforcement action under the rule, but now that they've dipped their toe in the pool, they're jumping in," said Roger Cohen, a partner in the health care practice at Goodwin Procter LLP.

This more aggressive stance, however, is unlikely to go unchecked.

The public has 60 days to comment on the FTC's proposed changes to the Health Breach Notification

Rule, and attorneys say they wouldn't be surprised to see at least some of this feedback focus on the commission's authority to sweep health apps, fitness trackers and similar direct-to-consumer health technologies into the universe of services that fall outside the federal Health Insurance Portability and Accountability Act but are covered by the revised notification rule.

"The FTC is acting very aggressively in the actions it's taken under this rule, but it's far from clear that a service like GoodRx is a covered vendor of personal health records," Cohen said.

The proposed amendments to the Health Breach Notification Rule include revising what qualifies as "[personal health record] identifiable information," "health care provider" and "health care services or supplies" to make clear that the explosion of new mobile health apps and connected devices that collect vast amounts of sensitive consumer health information fall under the rule's umbrella.

The revisions would also solidify that a "breach of security" that triggers notification under the rule includes both the type of data theft incidents most commonly associated with the term — that is, when personal information is stolen from or lost by the organization — but also instances where the company has intentionally disclosed users' information to third parties without permission.

Unauthorized data-sharing allegations were the basis of the two enforcement actions the FTC has taken to date under the rule, with the commission accusing GoodRx of illegally divulging personal health information to Facebook, Google and other advertisers and Premom of unlawfully disclosing users' private information to Chinese data collectors and other third parties.

"Up until recently, most people thought of a breach as intruder coming in and taking personal information," said Reed Freeman, partner and co-chair of the privacy and data security practice group at ArentFox Schiff LLP. "But under the Health Breach Notification Rule, what's a breach is much broader and will require companies to ensure that what they're saying about in their publicly facing privacy policies align precisely with their data disclosure practices."

While the FTC has long taken the view under Section 5 of the FTC Act that privacy policies must be accurate and not misleading, the commission has lacked the authority to impose fines for these violations the first time they occur. But now, with the Health Breach Notification Rule, the FTC has "civil penalties to back that up," Freeman noted.


"The clear message to industry is that they really have to know what data is leaving their company and for what reason," he added.

The recent proposed changes are also important because they would solidify the agency's position that the rule sweeps broadly to encompass "a much broader swath of digital health companies" than previously believed, rather than forcing the agency to attempt to establish these standards through their enforcement actions, Goodwin Procter's Cohen noted.

"This area has been a big focus for digital health companies, and I'd anticipate that the FTC will get comments on whether the commission's proposed changes are consistent with the statute and whether it has the authority to revise definitions to extend to these digital health companies," Cohen said.

In pushing back on the proposal, companies are likely to argue that the statute was meant to apply to a narrow subset of vendors of personal health records and that only Congress — and not the FTC — has the authority to expand that definition beyond what the Legislature intended, according to Cohen.

If the rule is finalized as currently drafted, which the commission is widely expected to do, there's also the chance that the changes could be challenged under the Administrative Procedure Act as being inconsistent with the statute, Cohen added.

There's also little doubt that the FTC will continue to bring actions that focus on the sharing of sensitive health information, particularly given **increased concerns** about third-party access to personal data such as medical records and location history in the wake of the U.S. Supreme Court's Dobbs  decision last year overturning the constitutional right to abortion.

"As the ecosystem has gotten far more complex, and it's becoming much easier to share large amounts of sensitive information, the FTC is putting a clear emphasis on health privacy," said Daniel Kaufman, a BakerHostetler partner and former acting director of the FTC's Bureau of Consumer Protection.

As this activity continues to build, attorneys say they'll be watching closely to see if more companies move to challenge rather than settle these actions.

"It's always hard to fight the government, especially with the risk it entails," Cohen said. "But if the FTC continues to pursue aggressive enforcement in this area, there's likely to be more pushback."

Aside from challenging how the FTC wields the Health Breach Notification Rule, companies facing regulatory action are also likely to fight the commission on how it regulates health data using its Section 5 authority.

In its actions against both GoodRx and Premom, the FTC accused the companies of engaging in unfair and deceptive practices in violation of Section 5 by misrepresenting their policies on sharing personal data with third parties and failing to implement sufficient safeguards to prevent these unauthorized disclosures.

Both companies denied any wrongdoing, noting that they disputed the claims that they unlawfully shared personal data with unauthorized third parties but had elected to settle the claims to avoid the "time and expense" of litigation.

However, the FTC has come under fire in the past for characterizing certain uses of personal data as an "unfair" practice likely to cause "substantial injury" to consumers, and the agency's health privacy actions present a fertile ground for future challenges, especially given the potential for the commission's stance on the proper handling of health data to be extended to other categories of potentially sensitive information.

"The big question in these cases is whether they mean the same type of rules the FTC is trying to enforce in regard to obtaining consent before sharing health applies to all categories of sensitive data, including biometrics, TV viewing habits and web surfing data," said ArentFox's Freeman. "There doesn't really seem to be a limiting principle to the FTC's enforcement regime, and it will be interesting to see if someone litigates this."

A potential challenger may have a stronger leg to stand on following an Idaho federal judge's **decision last month** in the FTC's location data privacy suit against mobile app analytics provider Kochava.

In a rare challenge to an FTC action, Kochava had argued that the commission lacked support for its

claim that the company violated the unfairness prong of Section 5 by selling geolocation data that could enable third parties to track mobile device users to and from sensitive locations.

In granting Kochava's bid to dismiss the suit, U.S. District Judge B. Lynn Winmill ruled that the FTC had failed to adequately allege that Kochava's data sales "cause or are likely to cause" secondary harms such as stigma or discrimination, although he granted leave for the agency to file an amended complaint, giving the commission a chance to beef up its consumer harm assertions.

"The Kochava ruling makes it very clear that the FTC's unfairness authority is a challenging tool for the FTC to use in privacy cases," said Kaufman, the BakerHostetler partner and former acting bureau chair.

The FTC is currently leaning on its Section 5 authority to support an array of actions to regulate the use and disclosure of sensitive information. This includes a policy statement on biometric privacy that the FTC issued at the same May 18 open meeting where it unveiled its proposed health rule expansion.

In its policy statement, the FTC warned that the increasing use of consumers' biometric information and related technologies, including those powered by machine learning, raises "significant consumer privacy and data security concerns and the potential for bias and discrimination," while making clear that the agency stood committed to policing unfair or deceptive acts and practices related to the collection and use of consumers' biometric information.

However, given that the policy statement is "primarily premised on unfairness" and practices they can target based on this authority, questions are likely to swirl about the legality and longevity of this move as well, Kaufman noted.

"The FTC has great expectations of what it wants to achieve in this area, but the Kochava decision signals it's not going to be easy," Kaufman said.

Still, the FTC's enforcement work involving sensitive data continues to chug on and reach beyond health and biometrics to additional hot-button areas, including artificial intelligence and the collection of children's data.

FTC Commissioner Alvaro Bedoya has stressed that the agency has authority under existing tools, including Section 5, to tackle privacy and discrimination risks raised by the growing use of generative AI. And the FTC has leaned on its statutory authority under the Children's Online Privacy Protection Act, which gives the agency specific rulemaking authority and fining powers, to secure multimillion-dollar penalties against Microsoft and Amazon in recent weeks for their allegedly unlawful handling of data from children under 13.

"The enforcement with respect to sensitive information ... seems to be continuous and picking up the pace through a combination of enforcement action, litigation, proposed rulemaking and guidance blogs which set to clarify the agency's position about the concepts of 'unfair and deceptive' in the context of data protection," said Odia Kagan, partner and chair of the General Data Protection Regulation compliance and international privacy practice at Fox Rothschild LLP.

While lawmakers at the state and federal levels are rushing to enact laws to specifically address topics such as the gaps in coverage for health apps not covered by HIPAA and the emergence of AI, "the FTC is confirming that in Section 5 of the FTC Act, plus its enforcement and guidance to date, it has the legislative framework it needs for enforcement and is set to do so, right now," Kagan added.

In the health privacy arena, Washington state took a major step forward in April when it **put in place** a novel law requiring companies that collect wellness, nutrition, fitness, location and other health-related data to obtain users' consent before collecting, sharing or selling this information, and empowers consumers to file private lawsuits for alleged violations.

While other states and Congress are expected to try to replicate or build on these efforts by instituting broader privacy protections for both health information and a wide range of other personal data, the FTC's latest enforcement actions show that companies shouldn't wait until these laws are in place to ensure that the sensitive information they hold is secure, experts say.

"In the absence of congressional action, the FTC is going to continue to use old rules to address perceived privacy gaps and areas that are viewed as not being as heavily regulated," said David Kessler, head of the U.S. privacy practice at Norton Rose Fulbright.

"With so much more of this information out there available to collect and monetize, and with the FTC seeing so much more risk for consumers, the commission likely feels there's an opportunity to instill better practices in app developers and others collecting, processing and transferring sensitive information," Kessler added. "The best way to comply is to be more transparent with consumers about what information is being collected and what it's being used for, which will require businesses to stay on top of changing their notices as their business models change over time."

--Editing by Alanna Weissman and Emily Kokoll.