FTC Proposes Amendments to Health Breach Notification Rule, Affirming its Commitment to Privacy of Consumer Health Information

Insights 05.22.23

PROFESSIONAL

ANDREA FREY
Partner
San Francisco
San Diego

KERRY K. SAKIMOTO
Associate
Los Angeles

The Federal Trade Commission (the "FTC") released proposed changes to the Health Breach Notification Rule (the "HBN Rule") on May 18, almost three years exactly following the agency's request for public comment on the rule issued May 20, 2020.

Promulgated in September 2009 by the FTC, the HBN Rule requires vendors of personal health records ("PHRs") and PHR related entities that are not regulated by the Health Insurance Portability and Accountability Act ("HIPAA") to notify individuals, the FTC, and, in some cases, the media, of a breach of unsecured personally identifiable health data contained in a PHR (i.e., an electronic record of PHR identifiable health information drawn from multiple sources and managed, shared, and controlled by or primarily for an individual). 16 CFR Part 318. The HBN Rule also requires that any "third party service providers" notify the vendor of PHR or the PHR related entity in the event of a discovery of such a breach.

Since the rule's passage, the digital health and wellness market has grown tremendously in recent years, with a proliferation of apps and other direct-to-consumer health technologies, such as fitness trackers and fertility monitors, increasingly available. The FTC (among other federal agencies) took note as the amount of health data collected from consumers, and the incentive for companies to use or disclose that sensitive data for marketing and other purposes, proliferated – in some cases without proper notice, consent, or authorization from the consumer. In September 2021, the agency issued a policy statement emphasizing that it considers many of these health and wellness apps to be PHR vendors, and therefore subject to the HBN Rule. The policy statement also sought to clarify that a "breach of security" by a PHR vendor is not just a cybersecurity attack, but *any* impermissible disclosure of user's sensitive health information – including instances where a wellness app discloses unsecured PHR identifiable information to a third party without the consumer's consent. Finally, the FTC warned the industry that it intended "to bring actions to enforce" the HBN Rule consistent with the policy statement.

In February 2023, the FTC made good on this warning in a first-of-its-kind enforcement action under the HBN Rule taken against a PHR vendor, alleging that a virtual prescription drug discount platform violated the HBN Rule by disclosing over 500 consumers' sensitive health information to third party advertising platforms like Facebook and Google, without the authorization of those consumers. Then, on May 17 – just a day before the proposed rule was released – the FTC announced the second-ever

enforcement action under the HBN Rule, this time against a fertility tracking company that allegedly disclosed users' sensitive sexual and reproductive health information to various third parties like AppsFlyer without consumer consent.

The FTC's proposed rule and recent enforcement actions signal that the agency very much seeks to keeps pace with emerging technological capabilities and developments in the digital health and wellness arena, in part through modifying the HBN Rule to clarify a more expansive applicability to the activities of such apps and similar technologies. Below, we provide a summary of the key takeaways regarding the proposed modifications to the HBN Rule for digital health and wellness businesses.

Summary of the Proposed Modifications to the HBN Rule

Most significantly, the proposed rule seeks to clarify the HBN Rule's scope, including its applicability to PHR vendors and PHR related entities that deal with PHR identifiable health information created or received by a "health care provider" not covered by HIPAA, which would include traditional providers of medical and other health services (*e.g.*, physicians), as well as any other entity furnishing "health care services or supplies." The FTC proposes to define the "health care services or supplies" broadly to refer to online services, such as a website, mobile application, or Internet-connected device, that "provides mechanisms to track diseases, health conditions, diagnosis or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet, or that provides other health-related services or tools." By doing so, the agency sweeps in app vendors that offer not just health but also wellness services to consumers.

This proposed rule makes other additional changes to the HBN Rule, including but not limited to:

- Revising the definition of "breach of security" to explicitly include unauthorized acquisition of PHR identifiable health information in a PHR that occur as a result of a data security breach or an unauthorized disclosure (such as when a wellness app discloses unsecured PHR identifiable information to another company without authorization or consent from the consumer);
- Revising the definition of "PHR related entity" to include entities that access or send unsecured PHR identifiable health information to a PHR vendor, rather than entities that access or send *any* information to a PHR vendor;
- Clarifying what it means for a PHR vendor to draw PHR identifiable health information from multiple sources;
- Authorizing a "clear and conspicuous" electronic notice be made by PHR vendors to report a breach to affected consumers; and
- Expanding the required content of the notice to consumers affected by a breach, including regarding the potential harm resulting from the breach and protective measures that the notifying entity is making available to affected consumers (the agency also provide a template notice to consumers).

The proposed rule would also make clear that the FTC considers any violation of the HBN Rule as an unfair or deceptive conduct under Section 5 of the FTC Act, subject to civil penalties of up to $50,120 *per day per violation* (increased annually for inflation).

More Enforcement Scrutiny on the Horizon

This proposed rule appears to be part of continued scrutiny by the FTC regarding consumer protection in healthcare – with respect to privacy and security and beyond. For example, on the same date as the release of the proposed rule, the FTC issued a policy statement on biometric information, warning that the increasing surveillance and use of biometric information (e.g., facial features, iris or retina, fingerprints, to name a few), including powered by machine learning, "raises significant consumer privacy and data security concerns and the potential for bias and discrimination." In the policy statement, the FTC identifies examples of practices it will scrutinize to determine whether such collection activities would be unfair or deceptive conduct under Section 5 of the FTC Act. In addition, in April 2023, the FTC sent notices of penalty offenses to 670 companies involved in marketing of drugs, homeopathic products, dietary supplements, and functional foods, that allegedly made deceptive and unsubstantiated product claims in advertisements, in conflict with the agency's Health Products Compliance Guidance issued late 2022.

Next Steps

The FTC is accepting comments on the proposed rule for 60 days after publication in the Federal Register. In addition to comments on the proposed regulations, the FTC is seeking comment on certain changes considered but not proposed. This includes comments sought regarding defining "authorization" or "affirmative express consent" of an individual to disclosure of their information, including seeking comments regarding acceptability of consent via clicking to "agree" or "accept" in connection with a pre-checked box or agreeing to terms and conditions without being required to review such terms and conditions. The FTC ultimately did not propose a definition at this time, as it believes its prior commentary and enforcement actions make clear what would not be authorized disclosures and what would not satisfy the standard of "meaningful choice," but seeks public comment whether its current guidance is sufficient.

In light of the proposed rule and other recent actions taken by the FTC and other regulatory bodies, digital health and wellness companies would be well-advised to review how they handle consumers' health information and ensure they employ reasonable privacy and data security measures with regard to such data.

RELATED CAPABILITIES

Digital Health

Health Information Privacy and Security