KIRKLAND & ELLIS

Kirkland Alert

FTC Announces Revised Health Breach Notification Rule

30 April 2024

On April 26, 2024, pursuant to a split party-line vote, the Federal Trade Commission ("FTC") announced finalized changes to its Health Breach Notification Rule (the "HBNR" or "Rule") that will, according to the FTC, "strengthen and modernize the Rule by clarifying its applicability to health apps and similar technologies[.]" The updated Rule will go into effect on June 25, 2024.

Congress authorized the FTC to promulgate the HBNR in 2009 as part of the Health Information Technology for Economic and Clinical Health (HITECH) Act. For more than a decade thereafter, the HBNR was understood to apply narrowly to instances of theft or misappropriation of consumer medical records held by electronic medical record vendors. The FTC did not bring a single action enforcing the HBNR during that period. But, starting with the FTC's September 2021 Policy Statement, the FTC began taking the position that the HBNR was *much* broader in scope. Among other things, the FTC notably asserted that the HBNR applied to consumer health-related website browsing and app usage data shared with advertising vendors via tracking pixel without consumer consent. Although no court has ever evaluated this position, the FTC obtained several recent settlements premised on this interpretation of the Rule.

Last year, the FTC announced a Notice of Proposed Rulemaking eliciting comments on a number of proposed changes to the Rule that would conform its text to the FTC's expanded interpretation. The key proposed changes, summarized below, were largely incorporated into the finalized updated Rule:

- **Revised Definition of "PHR identifiable health information":** The finalized HBNR modifies the definition of "[Personal Health Record (PHR)] identifiable health information" and adds definitions for "covered health care provider" and "health care services or supplies." These revisions make clear that the Rule applies to health websites, apps and similar technologies that are not covered by the Health

Insurance Portability and Accountability Act ("HIPAA"). The FTC also re-affirmed its position that "PHR identifiable health information" covers information inferred from non-health-related data (e.g., location and purchases), which tracks the approach taken under other new health privacy laws, like Washington's My Health My Data Act.

- **Revised Definition of "Breach of Security":** The final Rule contains a revised definition of "breach of security." The Rule previously defined "breach of security" as the "acquisition of unsecured PHR identifiable health information of an individual in a personal health record without the authorization of the individual." The new definition makes clear that a "breach" includes disclosures unauthorized by the consumer, such as a voluntary disclosure made by the PHR vendor if a consumer did not provide affirmative express consent to such disclosure — taking a similarly expansive view as the Office for Civil Rights (OCR) regarding the use of online tracking technologies by entities covered by HIPAA.

- **Revised Scope of the Term "PHR Related Entity":** The final Rule makes clear that the HBNR covers entities that offer products and services through websites and mobile applications. The FTC also revised the definition of "PHR Related Entity" to make clear that only entities that access or send *unsecured* PHR identifiable health information to a personal health record — rather than entities that access or send any information to a personal health record — qualify as PHR Related Entities.

- **Clarification of What it Means for a Personal Health Record to Draw Information From Multiple Sources:** The Rule previously defined "personal health record" as "an electronic record of PHR identifiable health information … on an individual *that can be drawn from multiple sources* and is managed, shared, and controlled by or primarily for the individual." The final Rule amends the definition to include any electronic record of PHR identifiable health information with "the *technical capacity* to draw information from *multiple sources*," a much more sweeping concept that arguably renders the "multiple sources" language meaningless, particularly given that websites and apps typically can, as a technical matter, pull data from a broad array of sources.

- **Changes to Method and Content of Notice:** The HBNR has long required covered entities to notify consumers of a breach of security. The Rule previously required notice to occur by first-class mail, or by email "if the individual is given a clear, conspicuous, and reasonable opportunity to receive notification by first-class mail, and the individual does not exercise that choice." The amended Rule now allows notice via email so long as the affected individual has specified email as the primary contact method. The final Rule also includes new requirements for what must be

included in the notice, as well as a model notice template. In most cases, a company now must disclose the identity of any third parties that acquired the PHR identifiable health information as a result of the breach and the types of health information the breach involved.

The Commission voted 3-2 to approve the publication of the final rule in the Federal Register, with Commissioners Melissa Holyoak and Andrew Ferguson voting against the revisions. In their dissenting statement — the first dissent either has issued since their confirmations in March — Commissioners Holyoak and Ferguson assert that the majority "attempts to shoehorn its desired policy goal into a 'plain reading' of the statute," and that by doing so, the finalized Rule "exceeds the bounds Congress clearly established."

The dissenting Commissioners outline multiple "significant problems" with the final Rule, including that it contains "expansive definitions [that] are not consistent with the statute," introduces incongruities between the final Rule and corollary provisions in the Social Security Act, does not clarify the scope of regulated entities, and puts companies "at the risk of being in perpetual violation of the Final Rule, and, therefore, perpetually at the mercy of the Commission's enforcement provision." The dissenting statement offers companies accused of violating the Rule a roadmap for challenging enforcement of the final HBNR.

Authors

Olivia Adendorff, P.C.

Partner / Dallas / Washington, D.C.

Richard H. Cunningham, P.C.

Partner / Washington, D.C.

Andrea deLorimier

Associate / Austin

Robert Kantrowitz

Partner / New York

Rachael A. Rezabek

Partner / Dallas

Dennis Williams

Partner / New York

Related Services

Practices

- Cybersecurity & Data Privacy
- Healthcare & Life Sciences Regulatory

Suggested Reading

- 17 April 2024 Kirkland Alert Prospect of Comprehensive Nationwide Privacy Legislation Reemerges
- 20 July 2023 Kirkland Alert Federal Trade Commission Releases First Updates to Endorsement Guides in 14 Years
- 16 May 2023 Kirkland Alert Washington's My Health My Data Act