UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Joint Statement of Chair Lina M. Khan,
Commissioner Rebecca Kelly Slaughter, and Commissioner Alvaro M. Bedoya
Health Breach Notification Final Rule
Commission File No. P205405

April 26, 2024

Today, the FTC finalizes an update to the Health Breach Notification Rule ("the Final Rule") that ensures its protections keep pace with the rapid proliferation of digital health records. We do so to fulfill a clear statutory directive given to us by Congress.

In 2009, as part of the American Recovery and Reinvestment Act ("ARRA"), Congress passed the Health Information Technology for Economic and Clinical Health Act ("HITECH Act").[1] Among other things, the HITECH Act sought to fill the gaps left by the privacy and security protections created under the Health Insurance Portability and Accountability Act ("HIPAA"), which was passed more than a decade earlier.[2] Specifically, it expanded the kinds of entities subject to the privacy and security provisions of HIPAA,[3] gave state attorneys general enforcement powers,[4] and—most relevant here—directed the Commission to issue a rule requiring entities not covered by HIPAA to provide notification of any breach of unsecured health records.[5] The Commission issued the original rule in 2009.[6] In 2020, the Commission initiated its regular decennial rule review and, in 2021, the Commission issued a policy statement clarifying how the rule applies to health apps and other connected devices.[7] In the years since, the Commission has brought enforcement actions against health apps alleging violations of the Health Breach Notification Rule.[8] Today's issuance of the Final Rule codifies this approach, honoring the statutory directive that people must be notified when their health records are breached.

[1] Am. Recovery and Reinvestment Act of 2009, Pub. L. 111-5, 123 Stat. 115 (2009) at Sec. 13400 et seq.
[2] Health Insurance Portability and Accountability Act, Pub. L. 104-191, 110 Stat. 1936, 2022 (1996) at Sec. 1171, codified at 42 U.S.C. § 1320d.
[3] Health Information Technology for Economic and Clinical Health Act, Pub. L. 111–5, Div. A, Title XIII, Subtitle D, § 13401 & 13404 (codified at 42 U.S.C. § 17937(a))
[4] *Id*. § 13410(e).
[5] *Id*. § 13407(g)(1).
[6] 74 Fed. Reg. 42962 (Aug. 25, 2009).
[7] Statement of the Commission on Breaches by Health Apps and Other Connected Devices (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.
[8] *See, e.g.*, Fed. Trade Comm'n, FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-

The dissent argues that the Commission's action "exceeds the Commission's statutory authority."[9] But its analysis contravenes a plain reading of the statute.

In the HITECH Act, Congress directed the FTC to issue rules requiring vendors of personal health records ("PHR") to notify consumers and the FTC following "a breach of security of unsecured PHR identifiable health information."[10] The statute defines the term "PHR identifiable health information" as "individually identifiable health information, as defined in section 1320d(6) of this title."[11] Section 1320d(6), a portion of the Social Security Act created by HIPAA, defines "individually identifiable health information" as "any information . . . that is created or received by a health care provider, health plan, employer, or health care clearinghouse."[12] Section 1320d(3), another section of the Social Security Act created by HIPAA, defines "health care provider" as, first, "a provider of services" as defined in § 1395x(u);[13] second, "a provider of medical or other health services" as defined in § 1395x(s);[14] and, third, "any other person furnishing health care services or sup (a)4 (Td(,R)Tjw 1)3 (sin)w [(th)3h sei 128.

services.”[19]

Notably, in its 1999 Notice of Proposed Rulemaking for the HIPAA Privacy Rule, HHS originally had proposed to define the term "health care" as constituting "the *provision* of care, services, or supplies…."[29] But, in its final rule, HHS eliminated the concept of "provision" in order to distinguish the broader term of "health care" from the narrower term "treatment."[30] HHS explained: "We delete the term 'providing' from the definition [of health care] to delineate more clearly the relationship between 'treatment,' as the term is defined in § 164.501, and 'health care.'"[31] HHS defined "treatment," in contrast to "health care," as "the provision, coordination, or management of health care and related services."[32] In short, HHS defines "health care" broadly, covering all aspects related to the health of an individual, and defines "treatment" more narrowly, referring to the provision of medical care to an individual. The dissent's proposal to narrow the third category of "health care provider" to "traditional forms of health care providers" closely mirrors the approach that HHS *rejected* when it defined this term.[33]

The dissent also claims that changing the phrase "can be drawn" to "has the technical capacity to draw" violates the surplusage canon because it renders the limitation meaningless as to health apps, because "virtually every app has the technical capacity to draw some information from more than one source."[34] This argument fails for two reasons. First, as the Statement of Basis and Purpose ("SBP") explains, there are products and services that do not satisfy this requirement.[35] Second, even if the definition did reach every health app, that would not itself suggest that the Final Rule's definition was wrongly crafted. Rather, it would reflect the rapid growth in digital applications and services related to consumers' health.[36]

The practical ramifications of the dissent's legal shortcomings are significant.

---

omitted). It is not clear how this qualifies as a mischaracterization. Indeed, this is precisely the stated purpose of the Health Breach Notification Rule: To cover entities that HIPAA does not. The dissent also notes that we fail to recognize that HHS provides two examples of "health care." But, HHS expressly states that the definition "includes, but is not limited to" these categories.

GoodRx marked the first time the Commission had ever enforced the Health Breach Notification Rule. A top