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-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising; Fed. Trade Comm'n, Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order (May 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc.

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 supplies."[15]

The term "health care services or supplies," undefined in the statute, is defined in the Final Rule as follows:

> Health care services or supplies means any online service such as a website, mobile application, or internet-connected device that provides mechanisms to track diseases, health conditions, diagnoses 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.[16]

The dissent argues that this definition violates certain canons of statutory construction.[17] But its effort to cabin the third category of HIPAA's "health care provider" reads it out of existence, violating the canon that holds interpretations giving effect to every clause of a statute are superior to those that render distinct clauses superfluous.[18] Specifically, the second category of "health care provider" already comprises a vast array of "provider[s] of medical and other

---

[9] Dissenting Statement of Comm'r Melissa Holyoak at 1 (Apr. 25, 2024) (hereinafter "Dissent").
[10] Health Information Technology for Economic and Clinical Health Act, Pub. L. 111–5, Div. A, Title XIII, Subtitle D, § 13407 (codified at 42 U.S.C. § 17937(a)).
[11] 42 U.S.C. § 17937(f)(2).
[12] 42 U.S.C. § 1320d(6).
[13] *See* 42 U.S.C. § 1395x(u) ("The term "provider of services" means a hospital, critical access hospital, rural emergency hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program, or, for purposes of section 1395f(g) and section 1395n(e) of this title, a fund.").
[14] 42 U.S.C. § 1395x(s) (listing a vast array of services, tests, supplies, and measurements, comprising over 2000 words and 15 categories, one of which has over 30 subcategories).
[15] 42 U.S.C. 1320d(3) (emphasis added).
[16] HBNR Final Rule § 318.2(e).
[17] Dissent at 2 ("When a statute contains a list, "each word in that list presumptively has a 'similar' meaning" under the canon of *noscitur a sociis*. And when a general term follows a list of specific terms, the *ejusdem generis* canon teaches that the general term "should usually be read in light of those specific words to mean something 'similar.'" Together, these canons instruct that the final category of health care provider that includes the general term "*other* person" must be similar to the more specific terms that precede it." (citations omitted)).
[18] *Marx v. Gen. Revenue Corp.*, 568 U.S. 371, 386 (2013) (Thomas, J.) ("Finally, the canon against surplusage is strongest when an interpretation would render superfluous another part of the same statutory scheme.").

services."[19] If the Commission were to interpret the third category as comprising, as the dissent recommends, only "traditional forms of health care providers," this distinct provision would be entirely redundant.

The dissent's approach also fails to give meaning to other textual differences between the second and third category. The second category in the definition of "health care provider" discusses a "provider" and "medical" services.[20] The third category, by contrast, drops the terms "provider" in favor of "person furnishing" and drops "medical" in favor of "health care."[21] Honoring the materially different words of the statute requires us to read these two categories as covering distinct, not entirely overlapping, entities.[22] The Final Rule faithfully follows these textual markers and identifies specific services and tools that comprise "health care services or supplies."[23] Contrary to this plain reading of the text, the dissent claims that Congress must have meant for this provision to apply only to "traditional forms of health care providers."[24] But we cannot subordinate the text of the statute to speculative accounts of what Congress intended.

The dissent also notes that the Department of Health and Human Services ("HHS") "has never interpreted the term 'health care provider' to reach the expansive, creative conclusion that the Commission does today."[25] HHS *has*, however, interpreted "health care provider," and its interpretation of this term is consistent with the Commission's definition.[26] In the HIPAA Privacy Rule, HHS defines first two categories of "health care provider" using the same language as the statute, but the third category is changed from "any other person furnishing health care services or supplies" to "any other person or organization who furnishes, bills, or is paid for health care in the normal course of business."[27] HHS also defines "health care" broadly, as any "care, services, or supplies *related to the health of an individual*."[28]

---

[19] 42 U.S.C. § 1320(d)(3) (citing 42 U.S.C. § 1395x(u)).
[20] 42 U.S.C. § 1320(d)(3).
[21] *Id*.
[22] *See Southwest Airlines Co. v. Saxon*, 596 U.S. 450, 458 (2022) (Thomas, J.) ("Where a document has used one term in one place, and a materially different term in another, the presumption is that the different term denotes a different idea" (cleaned up)).
[23] In addition to defining this term by identifying specific services, the Final Rule actually also *narrowed* the definition originally proposed in the NPRM, by eliminating "includes" from the definition. SBP at 27 ("[T]he Commission has substituted the word 'means' for 'includes' to avoid implying greater breadth than the Commission intends.").
[24] Dissent at 3. This rejection of the text of the statute, in favor of vague speculation about what Congress intended, mirrors the argument advanced by the Chamber of Commerce ("the Chamber"). The Chamber purports to rely on a "plain text reading" of the statute but immediately switches—in the very same sentence—to vague notions of Congressional intent: "It is clear from a plain text reading of both the HITECH Act and HIPPA [*sic*] that *Congress intended* for the HBNR to cover health records *more aligned* with the provision of health services provided by traditional health providers at a time when it was attempting to digitize traditional health records." Comment submitted by U.S. Chamber of Com., Health Breach Notification Rule, *Regulations.gov* (Aug. 8, 2023) at 3, https://www.regulations.gov/comment/FTC-2023-0037-0108 (emphasis added).
[24] Dissent at 3.
[25] Dissent at 3.
[26] That the HIPAA Privacy rule has a narrower overall scope does not change this fact.
[27] 45 C.F.R. § 160.103.
[28] *Id.* (emphasis added). The dissent asserts that we "mischaracterize[] the HIPAA Privacy Rule, which only applies to HIPAA 'covered entities' and their 'business associates,'—i.e., to traditional health care providers, that do not include the broad swath of app developers the Final Rule will encompass." Dissent at 4 n.24 (internal citations

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. 45 C.F.R. § 160.103. In any case, the breadth of these categories further underscores the expansive scope of HHS's definition of health care. *Id*.

[28] Dissent at 2.

[29] Proposed Rule, Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918, 60049 (Nov. 3, 1999) (emphasis added).

[30] 65 Fed. Reg. 82462, 82477.

[31] *Id.*

[32] 45 C.F.R. § 164.501.

[33] Dissent at 2.

[34] Dissent at 4.

[35] SBP at 29-30.

[36] The dissent's argument anachronistically assumes that Congress intended for the Rule to cover some health apps, but not other health apps. But, in fact, the Apple and Google app stores were in their infancy when Congress drafted this legislation in 2009, and so there is no indication that Congress was thinking about specific health apps at all. To the extent the dissent's argument is that Congress simply did not anticipate the vast number of products that would end up covered by the broad category of "supplies and services," it is not within the Commission's authority to re-write the statute based on the Commission's belief of what Congress would have wanted. *MCI Telecomms. Corp. v. Am. Telephone & Telegraph Co.*, 512 U.S. 218, 229 (1994) (holding that FCC's authority to "modify" does not extend to eliminating altogether a statutory requirement).

Just last year, the Commission brought an action against Easy Healthcare Corporation, alleging privacy violations by its fertility tracking application Premom.[37] As laid out in the complaint, Premom—which encourages users to provide information about their menstrual cycles, fertility, and pregnancy, as well as to import their data from other services, such as Apple Health—shared information with advertisers and China-based companies through software development kits ("SDKs") embedded in the application. The Commission's eight-count complaint against Easy Healthcare reflected the seriousness of this misconduct, charging the business with deceptive and unfair practices, as well as a violation of the Health Breach Notification Rule, which triggered civil penalties.

Under the dissent's analysis of health care services or supplies, the developer of the Premom application—Easy Healthcare—would not be covered by the Health Breach Notification Rule. This reading would mean that when companies like Easy Healthcare suffer a breach that may divulge health information to companies located in China, the Health Breach Notification Rule would not require them to disclose the breach to its users. It would also mean that when Easy Healthcare broadcasts women's sensitive health data across the vast commercial surveillance network propped up by SDKs and ad networks, the Health Breach Notification Rule would not require Easy Healthcare to alert women. Today's Final Rule rejects this atextual and cramped reading of the law, ensuring that businesses that hold themselves out as health care services companies—like Easy Healthcare—are considered "health care services" companies under the law.

Lastly, the dissent claims that the Final Rule introduces ambiguity where previous there was none. But *GoodRx* suggests otherwise. In a unanimous action, the Commission charged GoodRx with making unauthorized disclosures of people's health data to Facebook and Google, among others.[38] GoodRx, meanwhile, disputed the applicability of the HBNR to its practices, calling it a "novel" application.[39] By codifying how HBNR applies to online platforms and applications, today's Final Rule provides market participants with *more* clarity about what entities are covered—thereby providing greater certainty and notice.[40]

---

[37] Press Release, Fed. Trade Comm'n, Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order (May 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc.

[38] Press Release, 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-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising; *See also*, Concurring Statement of Comm'r Christine S. Wilson, GoodRx Holdings, Inc. (Feb. 1, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/2023090_goodrx_final_concurring_statement_wilson.pdf ("Today's settlement marks the first enforcement matter in which the FTC has invoked the HBNR. I congratulate staff on this important step — the agency rightly is focused on protecting the privacy of sensitive health data and empowering consumers to make informed choices about the goods and services they use."); *see also id*. at 5 (describing the GoodRx case as "an important milestone in the Commission's privacy work."). The dissent suggests that Commissioners Holyoak and Ferguson would have supported the application of HBNR to GoodRx.

[39] *See* GoodRx, GoodRx Response to FTC Settlement (Feb. 1, 2023) ("We believe this is a novel application of the Health Breach Notification Rule by the FTC. . . . We do not agree with the assertion that this was a violation of the HBNR.").

[40] The dissent implies, without saying so explicitly, that GoodRx is properly covered by HBNR. Dissent at 7-8. The dissent also states that it "would support finalizing a rule that *extends* and *clarifies* the scope of the Commission's

GoodRx marked the first time the Commission had ever enforced the Health Breach Notification Rule. A top priority for us at the Commission is ensuring we are faithfully discharging our statutory duties, rather than letting the authorities that Congress has granted us sit dormant, and we are proud of the work the Commission and the staff are doing to take care that the full set of laws assigned to the FTC are being faithfully executed.[41] We agree with the dissent that we must look out for the institutional integrity of the Commission. Failing to use the full scope of our statutory tools to protect Americans—and failing to update our application of these tools even as technologies change—would undermine the agency's integrity and credibility alike.

We are deeply grateful to the Division of Privacy and Identity Protection for leading the Commission's work to activate the Health Breach Notification Rule and for finalizing this Rule update. In an environment rife with new and evolving threats to Americans' health data, ensuring we are faithfully harnessing all of our statutory tools to protect people from data breaches is paramount.

***

enforcement in this important area of consumer protection if that rule were consistent with our grant of authority from Congress." Dissent at 1 (emphasis added). Today's Final Rule does precisely that. Previously, the rule did not define "health care services or supplies," and today's Final Rule does. Previously, health apps like GoodRx stated that it was unclear whether the rule applies to them, and today's Final Rule makes clear that it does. This from the dissent suggests a more modest disagreement with the contours of how the Rule defines "health care services or supplies," though—notably—the dissent does not provide an alternative definition.

[41] *See, e.g.*, Press Release, Fed. Trade Comm'n, FTC Hits R360 and its Owner With $3.8 Million Civil Penalty Judgment for Preying on People Seeking Treatment for Addiction (May 17, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-hits-r360-its-owner-38-million-civil-penalty-judgment-preying-people-seeking-treatment-addiction (the Commission's first action brought under the Opioid Addiction Recovery Fraud Prevention Act); Harris Jewelry, Press Release, Fed. Trade Comm'n, FTC and 18 States Sue to Stop Harris Jewelry from Cheating Military Families with Illegal Financing and Sales Tactics (Jul. 20, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/07/ftc-18-states-sue-stop-harris-jewelry-cheating-military-families-illegal-financing-sales-tactics (the Commission's first action brought under the Military Lending Act); Press Release, Fed. Trade Comm'n, Smart Home Monitoring Company Vivint Will Pay $20 Million to Settle FTC Charges That It Misused Consumer Credit Reports (Apr. 29, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/04/smart-home-monitoring-company-vivint-will-pay-20-million-settle-ftc-charges-it-misused-consumer (the Commission's first action brought under the Red Flags Rule, brought under Acting Chair Slaughter); Press Release, Fed. Trade Comm'n, FTC Sues Burger Franchise Company That Targets Veterans and Others With False Promises and Misleading Documents (Feb. 8, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/02/ftc-sues-burger-franchise-company-targets-veterans-others-false-promises-misleading-documents (the Commission's first action under the Franchise Rule since 2007); Press Release, Fed. Trade Comm'n, FTC Issues Rule to Deter Rampant Made in USA Fraud (Jul. 1, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-issues-rule-deter-rampant-made-usa-fraud (issuance of the Made in the USA Rule, more than 25 years after Congress authorized the Commission to promulgate a rule).