FTC Withdraws Controversial Health Breach Notification Policy Statement, But Rule's Expansive Reach Remains Through Amended Regulation

This Briefing is brought to you by AHLA's Health Information and Technology Practice Group.

September 23, 2026

Adam H. Greene, Davis Wright Tremaine LLP

On September 9, 2026, the Federal Trade Commission (FTC) rescinded its 2021 Policy Statement regarding the Health Breach Notification Rule (HBNR).[1] The FTC stated that the Policy Statement was unnecessary in light of 2024 regulatory amendments, pointing to President Trump's Executive Order 14192, titled "Unleashing Prosperity Through Deregulation," which directs agencies to eliminate obsolete guidance documents and policy statements.[2] While the Policy Statement is now withdrawn, its impact remains through the FTC's 2024 amendments to the HBNR. Specifically, the definition of "personal health record" broadly encompasses a vast range of health and wellness applications, and the definition of "breach" is so broad that the HBNR functionally serves as a very stringent privacy law, treating any uses or disclosures of personal health record (PHR) identifiable health information without the consumer's consent as a reportable breach. The biggest question, though, is whether the current administration has any interest in enforcing the 2024 amendments' broad scope.

Section 13407 of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 directed the FTC to promulgate regulations requiring vendors of PHRs and certain PHR-related entities to notify affected individuals and the FTC of a breach of PHR identifiable health information.[3] The statute also required third-party service providers to notify PHR vendors and PHR-related entities of a breach of PHR identifiable health information. At the time, big technology companies such as Google and Microsoft were offering products commonly known as PHRs that allowed consumers to securely manage and share their health information.[4] With the launch of these PHRs by technology giants, academics and news media raised questions about the privacy and security of such information due to PHRs generally falling outside the reach of the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules (because they typically are not offered on behalf of a HIPAA covered entity).[5] In response, Section 13424 of the HITECH Act also directed the Secretary of Health and Human Services (HHS), in consultation with the FTC, to conduct a study and issue a report on potential privacy and security requirements for entities that are not HIPAA covered entities or business associates, including PHR vendors.[6]

After 2009, however, PHRs never really took off among consumers. In June 2011, Google announced that it would shut down its PHR at the start of 2012, stating that there had been adoption among small pockets of consumers but "we haven't found a way to translate that limited usage into widespread adoption in the daily health routines of millions of people."[7] Microsoft ended its PHR service on November 20, 2019.[8] While these were not the only PHR services, the HBNR largely became a regulation without many regulated entities. Between the HBNR's promulgation in August 2009 and the FTC's Policy Statement in 2021, the FTC received only six breach reports from PHR vendors or PHR-related entities. The FTC did not bring any enforcement actions under the HBNR during that time.[9]

One of the first tremors of change, however, occurred in March 2021. A Senator and two Members of the House of Represenatives wrote to the FTC Acting Chair on March 4, 2021, urging the FTC to take enforcement action against menstruation-tracking mobile apps that violate the HBNR or other applicable regulations.[10] It is not clear, however, that the HBNR has ever covered such applications. The HITECH Act limits the HBNR to "PHR identifiable health information," which is defined as:

> [I]ndividually identifiable health information, as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)), and includes, with respect to an individual, information—
>
> (A) that is provided by or on behalf of the individual; and
>
> (B) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[11]

Section 1171(6) of the Social Security Act in turn defines "individually identifiable health information" as:

> Any information, including demographic information collected from an individual, that—
>
> (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
>
> (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and-
>
> (i) identifies the individual; or
>
> (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[12]

Accordingly, the HBNR does not govern information unless it was created or received by a health care provider, health plan, employer, or health care clearinghouse. If an individual tracks their menstruation on a mobile app, for example, then the information arguably has not been created or received by a health care provider, health plan, employer, or health care clearinghouse.

Potentially in response to the March 2021 letter from Congress, in September 2021 the FTC released the Policy Statement clarifying the scope of the HBNR.[13] Stating that the Statement was a response to "the explosion in health apps and connected devices," the FTC clarified that a PHR includes any app capable of drawing information from multiple sources if at least one source includes health information. For example, the Policy Statement clarified that a PHR includes a blood sugar monitoring app that

draws health information from a consumer's inputted blood sugar levels and also takes non-health information from another source (e.g., dates from the phone's calendar). As for the requirement that PHR identifiable health information is created or received by a health care provider, health plan, employer, or health care clearinghouse, the Policy Statement stated that the developer of a health app or connected device is a "health care provider." This meant that information may qualify as PHR identifiable health information simply because it is received by an app developer, regardless of whether the information was ever created or received by a clinician. The Policy Statement also clarified that a "breach of security" is not limited to cybersecurity intrusions or nefarious behavior, but rather encompasses any access or sharing of PHR identifiable health information without the consumer's authorization. Through its Policy Statement, the FTC clarified that it now interpreted the HBNR to encompass a wide range of health and fitness apps, without regard to whether they maintain information created by a clinician, and essentially turned a traditional breach notification rule into an extremely stringent privacy rule (requiring a consumer's authorization for any access or disclosure of their PHR data).

Not everyone within the FTC was on board with this direction, however. The FTC's two Republican-appointed commissioners both dissented from the Policy Statement. Then-Commissioner Christine Wilson dissented on the basis that: (1) the FTC was engaged in rulemaking to update the HBNR at the time and the Policy Statement short-circuited such rulemaking; and (2) the Policy Statement improperly expanded the FTC's statutory authority through overly-broad interpretations of "health care provider" and "drawn from multiple sources."[14] Similarly, then-Commissioner Noah Joshua Phillips dissented on the basis of the Policy Statement serving as an "end run" around FTC and HHS rulemaking efforts, its broad interpretation of app developers qualifying as "health care providers," and the use of the HBNR to police misrepresentations related to privacy (rather than solely more traditional "breaches of security").[15]

In 2024, the FTC amended the HBNR.[16] The 2024 amendments essentially codified the broad reach of the Policy Statement. They revised the definition of "breach of security" to clarify that a breach of security includes an unauthorized acquisition of unsecured PHR identifiable health information that occurs as a result of a data breach *or an unauthorized disclosure*.[17] They defined a "covered health care provider" to include a provider of "health care services or supplies," defining the latter as explicitly including "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."[18] The Republican-appointed FTC commissioners issued a dissent to the amendments, arguing that the amendments exceed the FTC's statutory authority. In particular, the dissent questioned the amendments' "astonishingly broad definition of 'health care services or supplies.'"[19]

The 2025 change of administration also brought a corresponding change in FTC commissioners. The FTC currently only has two commissioners, both Republican appointed. Chairman Andrew Ferguson, then a commissioner, joined the dissent to the 2024 amendments. This leaves the FTC's interest in enforcing the 2024 amendments in question.

The FTC's 2026 withdrawal refers to the Policy Statement as "controversial" and indicates that the 2024 amendments rendered the Policy Statement unnecessary. Accordingly, the Policy Statement is now null and void.

The more significant question is whether the current FTC will enforce the HBNR based on the 2024 amendments or based on the prior regulatory text. The FTC's Chairman is on record supporting the claim that the 2024 amendments exceed the FTC's statutory authority. Accordingly, the FTC could seek to initiate notice-and-comment rulemaking to revert the HBNR to its pre-2024 text (at least with respect to the scope of what constitutes a breach of security and who is a "health care provider" for purposes of PHR identifiable health information). But doing so requires time and resources. It's not clear that the HBNR is a sufficient priority to merit such attention. Instead, the FTC could simply use its enforcement discretion to not enforce the HBNR with respect to health and wellness apps that do not meet the older interpretation of what constitutes a PHR.

This leaves the health and wellness industry in a period of uncertainty. If a health and wellness app suffers a breach, does it choose to comply with the current HBNR regulatory text? Or does it agree with Chairman Ferguson's position, interpret that it is not truly a PHR under the statute, and rely on the FTC to not enforce the 2024 amendments? Even if the FTC chooses to not currently enforce the 2024 amendments, the regulatory text remains in place and a future administration may once again seek to apply the HBNR to virtually all health and wellness apps. A particularly interesting twist would be if an app developer came forward and challenged the 2024 amendments, with the current FTC potentially choosing to support rather than defend the challenge.

In short, the Policy Statement may be withdrawn, but the practical question of whether the HBNR applies to virtually all health and wellness apps very much remains in flux.

[1] *FTC Withdraws Obsolete Policy Statement*, FTC (Sept. 9, 2026), https://www.ftc.gov/news-events/news/press-releases/2026/09/ftc-withdraws-obsolete-policy-statement.

[2] Exec. Order No. 14192, 90 Fed. Reg. 9065 (Feb. 6, 2025).

[3] 42 U.S.C. § 17937.

[4] *Google Health, a First Look*, Google (Feb. 28, 2008), https://googleblog.blogspot.com/2008/02/google-health-first-look.html; *Peter Neupert: Microsoft HealthVault Launch*, Microsoft (Oct. 4, 2007), https://news.microsoft.com/speeches/peter-neupert-microsoft-healthvault-launch/.

[5] R. Steinbrook, *Personally Controlled Online Health Data—The Next Big Thing in Medical Care*, New Eng. J. of Med. (Apr. 17, 2008); S. Lohr, *Warning on Storage of Health Records*, N.Y. Times (Apr. 17, 2008).

[6] HITECH Act, Pub. L. No. 111-5, § 13424(b), 123 Stat. 115, 277 (2009).

[7] *An update on Google Health and Google PowerMeter*, Google (June 24, 2011), https://googleblog.blogspot.com/2011/06/update-on-google-health-and-google.html.

[8] M. Jo Foley, *Microsoft is closing its HealthVault patient-records service on November 20*, ZDNET (Apr. 5, 2019), https://www.zdnet.com/article/microsoft-is-closing-its-healthvault-patient-records-service-on-november-20/.

[9] *Notices Received by the FTC Pursuant to the Health Breach Notification Rule*, FTC, https://www.ftc.gov/system/files/ftc_gov/pdf/Health%20Breach%20Notices%20Received%20by%20the%2 (last accessed Sept. 11, 2026).

[10] Letter from Sen. Robert Menendez, Rep. Bonnie Watson Coleman, and Rep. Mikie Sherrill to Rebecca Kelly Slaughter, Acting Chairwoman, FTC (Mar. 4, 2021), https://web.archive.org/web/20210311053501/https://www.menendez.senate.gov/imo/media/doc/Congr

[11] 42 U.S.C. § 17937(f).

[12] 42 U.S.C. § 1320d(6).

[13] *Statement of the Commission on Breaches by Health Apps and Other Connected Devices*, FTC (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/rules/health-breach-notification-rule/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

[14] C. Wilson, *Dissenting Statement of Commissioner Christine S. Wilson*, FTC (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596356/wilson_health_apps_policy_stat

[15] *Dissenting Statement of Commissioner Noah Joshua Phillips Regarding the Policy Statement on Breaches by Health Apps and Other Connected Devices*, FTC (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596328/hbnr_dissent_final_formatted.pd

[16] HBNR, 89 Fed. Reg. 47028 (May 30, 2024).

[17] 16 C.F.R. § 318.2.

[18] *Id.*

[19] *Statement of Commissioner Melissa Holyoak, Joined by Commissioner Andrew Ferguson*, FTC (Apr. 26, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/p205405_hbnr_mhstmt_0.pdf.

ARTICLE TAGS

Health Information and Technology Practice Group Health Information