U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

August 8, 2023

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Suite CC-5610 (Annex H)
Washington, DC 20580

Re: Health Breach Notification Rule, Project No. P205405

Dear Commissioners:

The U.S. Chamber of Commerce ("Chamber") appreciates the opportunity to comment on the Federal Trade Commission's ("FTC" or "Commission") proposed amendments ("NPR" or "Proposed Amendments") to the Health Breach Notification Rule ("HBNR").[1] The Chamber believes it is vital that health information be protected. However, clarifications of the HBNR in light of technological change, interoperability requirements, modernization, and adoption may be needed. The Commission should avoid amending the HBNR in such a way that would create uncertainty in the online ecosystem by including covered entities and data beyond the intent of Congress when it authorized the Rule. We encourage the Commission to work with the Department of Health and Human Services to harmonize their respective breach rules.

I. The Commission's Proposed Amendments Should Not Exceed the Agency's Statutory Authority.

Key terms under the HBNR (such as "breach of security," "personal health record," and "PHR identifiable health information") were explicitly defined by Congress in the Health Information Technology for Economic and Clinical Health Act ("HITECH Act").[2] The FTC lacks authority to redefine these terms, or to reinterpret them in ways that are inconsistent with Congress's express limited FTC authority in this space. Indeed, the FTC itself has acknowledged that the HITECH Act ***requires*** the FTC to adhere to the Act's prescribed definitions.[3] Consequently, the FTC lacks the authority to redefine and reimagine HBNR terms that are already defined within the HITECH Act.

---

[1] 88 Fed. Reg. 37819 (June 9, 2023) *available at* https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12148.pdf.

[2] *See, e.g.*, 42 U.S.C. 42 U.S.C. §§ 17921, 17937.

[3] *See* Statement of the Commission on Breaches by Health Apps and Other Connected Devices, Federal Trade Commission (Sept. 15, 2021) ("The statute directing the FTC to promulgate the Rule ***requires*** that a 'personal health record' be an electronic record that can be drawn from multiple sources.") (emphasis added); *see also* 16

II. The Health Breach Notification Rule Should Cover Entities Contemplated by Congress

A. The HITECH Act Regulated Entities Tied to Traditional Health Care

The Health Breach Notification Rule was authorized under the HITECH Act as part of the American Reinvestment and Recovery Act in 2009.[4] Congress enacted the HITECH Act primarily to promote a nationwide network of electronic health records. While Congress could not have fully anticipated the app revolution that took place in the decade after the enactment of the HITECH Act, a plain text reading of the Act indicates that the HBNR should focus on health records pertaining to data documents used in traditional medical settings, like blood pressure readings available to doctors for diagnoses. The Proposed Amendments broadly expand the types of entities and applications that would be covered by the HBNR beyond those specifically contemplated when the HITECH Act became law. In 2009, when the Commission promulgated the initial version of the HBNR, it estimated that under its Paperwork Reduction Act review, it would cover approximately 700 entities.[5] Under the Proposed Amendments, it is estimated to cover 170,000.[6] Although the number of apps and websites has grown since 2009, such an increase is indicative that the Commission's Proposed Amendments do not merely clarify its authority but are an attempt to expand it.

Currently, the HBNR covers vendors of personal health records and their third-party service providers. Under the Current Rule, a vendor of personal health records ("PHR") is an entity "…that offers or maintains a *personal health record*."[7] A PHR under the Current Rule is "an electronic record of *PHR identifiable health information* on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."[8]

The Current Rule then defines PHR identifiable health information following verbatim the HITECH Act's definition as "'*individually identifiable health information*' as defined in section 1176(6) of the Social Security Act (42 U.S.C. 1320d(6)), and, with respect to an individual, information: (1) That is provided by or on behalf of the individual; and (2) 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."[9] The Social Security Act, as amended by the Health

---

C.F.R. 318 (acknowledging that while "some commenters stated that entities should be required to provide breach notification for paper, as well as electronic, information; [and] others expressed concerns about requiring media notice," "the Commission cannot change its final rule in response to these comments" "[b]ecause these requirements come directly from the language of the Recovery Act").

[4] 42 U.S.C. §17937.

[5] 74 Fed. Reg. 42977 (Aug. 25, 2009). *Available at* https://www.govinfo.gov/content/pkg/FR-2009-08-25/pdf/E9-20142.pdf.

[6] 88 Fed. Reg. 37837.

[7] 16 C.F.R. § 318.2(j) (emphasis added).

[8] *Id*. at § 318.2(d) (emphasis added).

[9] *Id.* at § 318.2(e) (emphasis added); *See also* 42 U.S.C. § 17937(f)(2).

Insurance Portability and Accountability Act ("HIPAA"), defines individually identifiable health information as "any information…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…"[10]

A health care plan is defined by statute as "a provider of services,"[11] with a provider of services being defined by statute as "a hospital, critical care access hospital, rural emergency hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program…"[12] It is clear from a plain text reading of both the HITECH Act and HIPPA 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.

B. The Proposed Amendments Exceed the HITECH Act's Mandate

1) The Definition of "Entity Furnishing Health Care Services or Supplies"

The Commission's Proposed Amendments to the HBNR develop an entirely new category of entities covered by the Rule by redefining health care provider as "a provider of services (as defined in 42 U.S.C. 1395x(u)), a provider of medical or other health services (as defined in 42 U.S.C. 1395x(s)), *or any other entity furnishing health care services or supplies*."[13] This novel addition to the definition of health care providers broadly includes entities that provide "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."[14]

Although the Commission claims to merely expand the definition of covered entities to health apps, a plain text reading of the Proposed Amendments would indicate otherwise. The Commission notes that under their Proposed Amendments, a PHR, "would be defined as an electronic record of PHR identifiable health information on an individual that has the *technical* capacity to draw from multiple sources…"[15]For example, under the Proposed Amendments, a calendar or email app in one's phone could have the technical capacity to be synched with multiple sources online to keep track of food delivery for allergy-based menu choices and

[10] 42 U.S.C. 1320d(6).
[11] *Id* at § 1320(d)(4).
[12] 42 U.S.C. § 1395x(u).
[13] 88 Fed. Reg. 37835 (proposed 16 C.F.R. § 318.2(f)).
[14] *Id*. (defining 16 C.F.R. § 312(e)). It is important to note the Commission's supporting citations for this position is a dissent not adopted by the Commission to the proposed consent order in the *Flo Health, Inc.* case.
[15] 88 Fed. Reg. 37826 (emphasis added).

times/types of doctor appointments. Although the Commission claims it seeks to limit the types of entities it regulates with the Proposed Amendments, the plain text of the NPR would do otherwise and produce unintended consequences.

2) To be a Covered Entity, Data Must be Managed, Shared, or Controlled by the Consumer

In its Proposed Amendments and recent enforcement actions, the FTC has made clear that it intends to apply the HBNRto health-related app and website operators that collect and share browsing data with tracking technologies without affirmative consent. In so doing, the Commission ignores that theHBNR applies only to "personal health records" that are "***managed, shared, and controlled by or primarily for the individual***." But the kind of browsing data that the FTC is targeting is generally managed, shared, and controlled by the companies themselves, for those entities' own business purposes (such as to track user engagement and effectuate marketing). In fact, most users will never see most of the information collected through apps, websites, cookies, SDKs, and pixels, and thus, cannot be reasonably used for their own *health* benefit, much less manage it for *health purposes*. The FTC has previously acknowledged this critical distinction regarding the clear limitations of the HBNR.[16]

3) The FTC's position that "personal health records" include apps that have the "technical capacity to draw information from multiple sources" is also too expansive, and not legally supportable.

The FTC's attempt to redefine "personal health records" to include any application that has the "technical means" to draw information from multiple sources is far too expansive and would sweep in virtually every app in existence – which, again, is contrary to Congress's intended limited scope of the Rule. Further, the FTC's longstanding guidance has been that an entity is a vendor of "personal health records" if it has "an online service that allows consumers to store and organize ***medical*** information from ***many*** sources in one online location."[17] The FTC's new position – that an app can be a "personal health record" even if it only pulls health information from one source and pulls something akin to calendar invites from another – contradicts its longstanding guidance and further illustrates that the Commission's attempted re-imagining of critical HBNR terms is legally unsupportable.[18]

The Proposed Amendments would create confusion as to whether entities are in fact covered by the HBNR which could lead to extensive litigation to determine the Proposed Rule's

---

[16] *See* 74 Fed. Reg. 42962, 42967, fn. 61 (August 25, 2009) (noting that "personal health records" "do not include the kinds of records managed by or primarily for commercial enterprises.").

[17] *Complying with the FTC's Health Breach Notification Rule*, FTC.gov: Guidance (Feb. 16, 2015), https://web.archive.org/web/20150216060636/https://www.ftc.gov/tips-advice/businesscenter/guidance/complying-ftcs-health-breach-notification-rule (emphases added).

[18] *See generally Facebook v. Duguid*, 141 S. Ct. 1163 (2021) (in the TCPA context, rejecting the argument that Facebook's platform qualified as an "automatic telephone dialing system" simply because it had the technical capacity to automatically dial numbers).

scope. The Commission should not seek to redefine vendors of personal health records in a way that exceeds what was contemplated by Congress at a time before the app economy was in full swing.

III. The FTC's Proposed Interpretation of "Individually Identifiable Health Information" is Overly Broad and Outside the Scope of Its Authority

Under the HBNR, covered entities would be required to provide notice of a breach upon discovery of a breach of secured of unprotected PHR Identifiable health information. Under the HITECH Act, PHR Identifiable Health Information is "Individually Identifiable Health Information" as defined by HIPAA. Although the Commission does not formally change the definition of individually identifiable health information, the Commission declares that it interprets the definition to mean "traditional health information (such as diagnoses or medications), *health information derived from consumers' interactions with apps and other online services* (such as health information generated from *tracking technologies* employed on websites or mobile applications or from customized records of *website or mobile application interactions), as well as emergent health data (such as health information inferred from non-health-related data points, such as location and recent purchases)*."[19]

In its Proposed Amendments, the FTC asserts that PHR identifiable *health information* includes, among other things, *non-health information* such as consumers' location data, browsing data, and "emergent health data." This interpretation is nonsensical and broad. For instance, the FTC seems to suggest that the fact that an IP address associated with a person's viewing of a health-related website could, on its own, be considered PHR identifiable health information. The practical effect of such a reading would require industry participants to treat nearly all categories of consumer data as potentially including health data. Congress clearly did not intend for the Rule to sweep so broadly. In fact, while Congress instructed the National Alliance for Health Information Technology ("NAHIT") to assist in defining key terms in the HITECH Act, it rejected NAHIT's proposal to define PHR identifiable health information as including "health-related information on an individual," and opted instead for the far narrower construction reflected in the Act, which was clearly intended to cover only traditional paper medical records that were being digitized during the digital transition occurring in the economy around the time of the HITECH Act.[20] The FTC is bound by Congress's more limited definition and intended purpose of the Act.

Such an Interpretation could massively expand the types of data covered by the HBNR beyond the bounds of what Congress established in the HITECH Act. The usage of terms such as "inferred," and non-health information would create uncertainty as to which data is covered by the Rule. The FTC's Interpretation exceeds Its statutory authority.

---

[19] 88 Fed. Reg. at 37823 (emphasis added).

[20] *Compare* Nat'l All. for Health Info. Tech., Report to the Office of the National Coordinator for Health Information Technology on Defining Key Health Information Technology Terms, at 19 (2008), https://www.nachc.org/wp-content/uploads/2016/03/Key-HIT-Terms-Definitions- Final_April_2008.pdf *with* 42 U.S.C. § 17937(f)(2).

IV. The Proposed Amendments Are Back Door Privacy—Not Breach—Requirements

The HITECH Act mandates notification requirements on the part of vendors and third-party service providers upon a breach of security.[21] The Act further defines a breach of security as "with respect to unsecured PHR identifiable health information of an individual in a personal health record, *acquisition* of such information without the authorization of the individual."[22]

The Proposed Amendments make a subtle but significant change to the definition to expand the definition of a breach to include "an authorized acquisition of unsecured PHR identifiable health information in a personal health record that occurs as a result of a data breach or an authorized *disclosure*." [23] The use of the term "disclosure" required notification would effectively operate as an opt-in notice and consent privacy regime. The Chamber expresses the same concerns that former Commissioner Noah Phillips outlined in his dissent to the 2021 Health Breach Policy Statement in which he noted[24]:

> [T]he law limits HBNR to "breach of *security"* defined only as "*acquisition* of such information without the authorization of the individual." That difference matters. The statutory definition of breach of the HBNR differs from the definition of breach for protected health information in other parts of the same statute, which covers "unauthorized *acquisition, access*¸ use or disclosure of protected health information which compromises the *security or privacy* of such information." To arrive at its desired outcome, the Statement ignores the distinction drawn by the law itself.

Although then-Commissioner Phillips referenced the Commission wrongly defining breach based on unauthorized access, the same logic also applies to stating that unauthorized *disclosure* should be considered a breach.

Additionally, the Commission cites the *GoodRx and Easy Healthcare* cases as examples justifying the Proposed Amendments. For example, the NPR states that "the Commission's recent settlement with GoodRx, alleging violations of the Rule, highlights that *disclosures* of PHR identifiable information inconsistent with a company's *privacy* promises constitute an unauthorized disclosure."[25] The Commission's own record indicates it seeks to promulgate opt-in privacy notice and consent—not merely breach—requirements. Such a determination is better suited for Congress, not the Commission.[26]

If the Commission has found consumer harm inflicted by covered entities in violation of Section 5 of the FTC Act appropriate to justify new privacy requirements on covered entities, it

---

[21] 42 U.S.C. § 17937(a).
[22] *Id*. at § 17937(f)(1).
[23] 88 Fed. Reg. 37834 to 37835 (defining 16 C.F.R. § 318.2(a)).
[24] https://www.ftc.gov/system/files/documents/public_statements/1596328/hbnr_dissent_final_formatted.pdf.
[25] 88 Fed. Reg. 37830.
[26] The commission cannot site its own consents as proof of what the law means.

should conduct a rulemaking under its legally-required Magnuson-Moss Rulemaking requirements. The FTC should not cloak a data privacy rule as a breach rule to avail itself of more streamlined Administrative Procedure Act processes.

In addition to process concerns, the Chamber asserts that the proposed change to the definition of "breach" would add to a growing patchwork of state health privacy laws in states like Washington that also do not clearly define covered entities and impose opt-in privacy requirements. Given the potential for state patchwork and conflict problems, and that Congress did not contemplate the HBNR to be an opt-in privacy regime, Congress—not the Commission—is the appropriate source of clarity.

V. Clarifications The Commission Should Make

A. De-identification

The Commission's NPR states that "de-identification would render the data no longer PHR identifiable health information subject to the Rule."[27] The Commission should issue an amended NPR to receive comment on clarifying the definition of "de-identification."

B. Exceptions

The Chamber reiterates that the definition of "breach" proposed by the Commission acts to change the Rule into a *de facto* opt-in privacy rule. While the Chamber does not concede the Commission has the authority under the HITECH Act, if the Commission proceeds with such an approach, it should provide exceptions for legitimate and societally beneficial uses of data that other privacy laws have for failure to honor opt-in including but not limited to network security, prevention and detection of fraud, protection of health, network maintenance, and service/product improvement.

We stand ready to discuss these issues, our suggested changes, and our concerns in greater detail. If you have any questions, please reach out at jcrenshaw@uschamber.com.

Sincerely,

Jordan Crenshaw
Senior Vice President
Chamber Technology Engagement Center
U.S. Chamber of Commerce

[27] *Id*. at 37825.