
**BEFORE THE FEDERAL TRADE COMMISSION**

**Office of the Secretary 600 Pennsylvania Avenue,**

**NW Suite CC-5610 (Annex H)**

**Washington, D.C. 20580**

# COMMENTS

**of**

**THE NETWORK ADVERTISING INITIATIVE**

**on the**

**Notice of Proposed Rulemaking to Amend the Commission's Health Breach Notification Rule**

**"Health Breach Notification Rule, Project No. P205405"**

**Leigh Freund**
**President & CEO**
**Network Advertising Initiative**

## I. Introduction

Pursuant to the notice published June 9, 2023, in the Federal Register, the Network Advertising Initiative ("NAI") appreciates the opportunity to comment on the Federal Trade Commission's ("FTC" or "Commission") proposed changes to 16 CFR Part 318, the Health Breach Notification Rule ("HBNR" or "Rule").

Founded in 2000, the NAI is the leading self-regulatory organization representing third-party digital advertising companies. For over 20 years, the NAI has promoted strong consumer privacy protections, a free and open internet, and a robust digital advertising industry by maintaining and enforcing the highest standards for the responsible collection and use of consumer data. Our member companies range from large multinational corporations to small startups and represent a significant portion of the digital advertising technology ecosystem, all committed to strong self-regulation and consumer trust. As a non-profit organization, the NAI promotes the health of the online ecosystem by maintaining and enforcing strong privacy standards for the collection and use of data for digital advertising across all digital media. We are encouraged by the opportunity to work with the Commission to help develop regulations that continue to ensure protections for the most sensitive types of consumer information, while balancing the legitimate interests of our industry that facilitates the open and free internet.

The NAI's leadership has predated most privacy laws in the U.S., including the HBNR. The NAI has long believed that many types of data can be sensitive, even if they do not fall under current legal and regulatory restrictions. This is why the NAI takes multiple measures to limit the collection and use of data for health-related advertising by member companies, including an outright prohibition on eligibility uses, including for healthcare, insurance, and housing.

Before required to do so by law, our members committed to obtaining opt-in consent prior to collecting or using sensitive personal information for Tailored Advertising or Ad Delivery and Reporting Purposes. This includes information now interpreted as PHR identifiable health information, such as browsing or purchase history that reveals a consumer's sensitive health condition, sensor information collected from wearable devices like heart rate monitors, and user-entered data such as information that a consumer enters manually into a website or app.

Therefore, the effect of the FTC's proposed new interpretation of the HBNR is consistent in many ways with the existing requirements of our 2020 Code of Conduct ("Code") regarding collection and use of sensitive data for advertising and marketing purposes, as well as our requirements and guidance more broadly pertaining to sensitive health data. As such, the NAI supports the Commission's efforts to update various key definitions to clarify the application and improve readability of the Rule. It is particularly important for the Commission to clarify the role of third-party service providers to eliminate potential conflicting notice requirements, and to expand methods of consumer notice in the event of a data breach to include electronic mail. However, these comments also propose the following additional modifications:

- Further revising the proposed definition of "health care services or supplies" to reasonably limit its breadth;
- Clarifying where entities performing analytics for vendors of PHR be considered third party service providers;
- Making further modifications to the Commission's proposed revisions to the definition of "personal health record" to keep it within the intended scope of the original statute;
- Striking the Commission's proposed creation of the definition of "clear and conspicuous" and instead inserting the detailed electronic notice requirements in the "methods of notice" section; and
- Striking the Commission's proposed additional requirement for notifying entities to list all potential harms associated with a particular breach when sending notification to consumers.

## II. The NAI Supports the Commission's Goals to Update and Clarify the Definition of "PHR Identifiable Health Information," but the Proposed Definition of "Health Care Services or Supplies" is Overly Broad

The Commission proposes importing language into the definition of PHR identifiable health information from the Social Security Act.[1] The NAI is supportive of Commission's proposed changes that improve the readability of the Rule – including relevant text from cross-referenced statutes makes it easier for companies, especially smaller start-ups without robust legal departments, to understand their obligations and when their activities may be in scope of the Rule. Ultimately, any changes that make the Rule easier to understand, while keeping with the intention of the underlying statute, will increase rates of compliance.

The Commission also proposes adding the term "health care services or supplies" to the text of the Rule to further clarify its applicability to apps and other modern online health services. The NAI agrees that additional clarification is appropriate to identify that in some cases, developers of apps and consumer technology services may be considered health care providers to the extent they provide mechanisms to track health conditions and bodily functions, and that the individually identifiable health information they collect or use may be considered PHR identifiable health information. However, as currently proposed, the definition of health care services or supplies serves to expand the scope of PHR identifiable health information beyond that which is reasonable. Specifically, the NAI cautions against the breadth the Commission proposes, particularly the use of the language "...or that provides other health-related services or tools."[2]

The Commission's interpretation of PHR identifiable health information as illustrated in the 2021 Policy Statement[3] and recent enforcement actions[4] modernizes the Rule to more clearly apply to non-HIPAA health records managed through commonly used applications and websites.

---

[1] Notice of Proposed Rulemaking on the Health Breach Notification Rule, 88 Fed. Reg. 37819 at 37822 (proposed Jun., 9, 2023) (hereinafter "NPRM").
[2] NPRM at 37823.
[3] FTC's Policy Statement on Health Breach Notification Rule, Sept. 2021.
[4] See *U.S. v. GoodRx Holdings, Inc.*, Complaint (Feb. 1, 2023); *U.S. v. Easy Healthcare Corp.*, Complaint (May, 17, 2023).

However, the definition of health care services or supplies[5] as proposed in this rulemaking goes beyond the Commission's previous interpretations, and beyond the scope of Congress' original intent.[6] While services such as online menstrual cycle trackers and diet applications that collect and manage information such as calories, weight, and age seem to be clearly in scope of the Rule and reflect a modern interpretation of the term, the language proposed threatens to sweep entities such as purely informational health-related websites into the category of "health care provider." An overly-broad definition would diminish the Rule's protections of genuinely sensitive information, such as that collected and stored in health-tracking applications. To remedy this, we urge the Commission to strike the vague language "...or that provides other health-related services or tools" from the definition of health care services or supplies.

## III. The NAI Supports the Commission's Objectives to Revise the Definition of PHR Related Entity, Particularly Clarifying Where Entities Performing Analytics for Vendors of PHR Be Considered Third Party Service Providers

The Commission proposes revising the definition of "PHR related entity" to clarify that it includes entities offering products or services through *any* online service, and to provide that only entities that send or access *unsecured* PHR identifiable health information are considered PHR related entities[7] – The NAI is supportive of this goal. The NAI is also supportive of the Commission's attempt to distinguish between related entities and third parties, and we support the position that entities providing analytics services to vendors should in most cases be considered third parties and not PHR related entities.

There are currently thousands of health-related apps available for download, many of which focus on treating and managing specific diseases, and allow users to automatically upload sensor information to the apps from devices such as remote blood pressure cuffs and heart rate monitors. The NAI has long considered sensor information such as heartbeat collected from a wearable monitor to be sensitive, and our 2020 Code requires opt-in consent before its use in Tailored Advertising or Ad Delivery and Reporting, regardless of whether it was collected through a website or a mobile application.[8] This proposed change to the rule will ensure that information intended to be in scope of the Rule will always be protected, regardless of the medium. This is consistent with the original intent of the Rule – to protect the most sensitive types of non-HIPAA covered health data.

Revising the third prong of the definition of PHR related entity to only include entities that send or access *unsecured* PHR identifiable health information to a personal health record is a valuable clarification. Particularly in light of the Commission's proposed expansion to the definition of PHR identifiable health information and breach of security, the Commission's suggestion reasonably narrows the scope of the Rule and prevents unintended information or practices from

[5] NPRM at 37835. ("Health care services or supplies includes 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.").
[6] 42 U.S.C. § 17937; American Recovery and Reinvestment Act of 2009, Public Law 111–5, 123 Stat. 115 (2009).
[7] NPRM at 37824.
[8] NAI Code, § II.C.1.h.

being swept in, while assuring truly sensitive information remains subject to disclosure requirements. Additionally, as noted in the Commission's proposal, limiting the definition of PHR related entities in this way also serves to encourage entities to take steps to properly de-identify information in accordance with the American Recovery and Reinvestment Act, and to choose partners based on their good data stewardship.[9]

In light of the proposed change to the definition of PHR related entity, the NAI shares the concern that this may ultimately lead to conflicting disclosure requirements for companies that could be considered both PHR related entities and third parties. Our members include third party digital advertising and analytics companies, and are most likely to be subject to the Rule's disclosure requirements as either related entities or third parties. For this reason, this distinction is extremely important for purposes of understanding compliance obligations. To this end, we are supportive of the Commission's proposed addition to 16 C.F.R. § 318.2(b) that clarifies firms that perform services such as attribution and analytics for apps and technologies providing health care services or supplies are third party service providers, not related entities. In situations where an entity could be dually considered a PHR related entity and a third party service provider, their relationship with the consumer and the nature of the service they offer should be considered.

In addition, to avoid creating undue burden on third parties that do not target PHR related entities and that have in place contractual restrictions against their clients sharing PHR identifiable health information, the Rule should exclude such entities. This exclusion would align with the objectives of the proposed Rule by incentivizing PHR related entities to limit the sharing of health information with third parties without creating extremely challenging or impossible compliance requirements on third parties that have elected not to work with PHR data.

Additionally, in response to the Commission's request for comment on the hypothetical[10] scenario posed in the Notice regarding notification to individuals after a breach, the NAI believes vendors of PHR are best suited to notify affected parties. As noted in the proposed rule, third party service providers have little to no contact or relationship with a consumer. These entities typically operate "business to business" and do not have a direct relationship with consumers. Consequently, affected individuals may be confused by, or completely ignore communications from these companies all together, directly contradicting the purpose of the Rule's disclosure requirements, and the intent behind the changes proposed in this rulemaking to facilitate clear and effective notice to consumers.[11]Additionally, these entities often lack the information needed to contact the individuals in accordance with the Rule's notice requirements. Attempting to

[9] NPRM at 37825.
[10] NPRM at 37825 ("The Commission also requests comment on the following scenario: a third party service provider, such as an analytics firm, receives PHR identifiable health info (e.g., device identifier and geolocation data from which health information about an individual can be inferred) and then sells it to another entity without the consumer's authorization. The Commission considers this to be a reportable breach, even if the consumer consented to the original collection. In such a scenario, the third party service provider would be required to notify the vendor of personal health records or PHR related entity, who in turn would notify affected individuals. The Commission requests comment on this approach, including whether as a policy matter it is advisable under the Rule to require a vendor of personal health records or PHR related entity to notify its customers about such onward disclosures.").
[11] NPRM at 37825.

acquire the proper information to do so would likely result in the collection of *more* information, rejecting basic principles of data minimization.

## IV. The NAI Opposes the Commission's Proposal to Revise the Definition of "Personal Health Record" to be an Electronic Record of PHR Identifiable Health Information on an Individual That Has the Technical Capacity to Draw Information from Multiple Sources and That Is Managed, Shared, and Controlled by or Primarily for the Individual

The Commission proposes modifying the definition of "personal health record" to read "an electronic record of PHR identifiable health information on an individual that has the technical capacity to draw information from multiple sources and that is managed, shared, and controlled by or primarily for the individual" – expanding both the type of information that can be included, and the purpose for which that information is collected and held.[12] The NAI is concerned that this proposed change could lead to an interpretation of the Rule beyond the intent of the original statute for the following two reasons.

First, pursuant to the current Rule, a personal health record must be able to draw *PHR identifiable health information* from multiple sources. However, as currently proposed, a service would qualify as a personal health record if it is able to draw *any information* from multiple sources.[13] This proposed expansion would serve to rewrite the original intent of the HBNR, and potentially sweep in new types of commonly exchanged, non-sensitive information. Particularly in light of the Commission's proposed expansion to the definition of PHR identifiable health information, discussed above, amending the definition of personal health record in a way that includes *any* information drawn from multiple sources, regardless of whether that information is identifiable health information, could have unforeseen consequences, is likely to apply too broadly, and could decrease the availability of innovative products and services.

Second, the Commission also suggests that a service need only have the *technical capacity* to draw this information from multiple sources. In today's interconnected world, it is difficult to identify any app or online service that does not have the *technical capacity* to draw some kind of information from multiple sources – whether that be personal information, such as location or the contents of a personal calendar, or simply non-identifiable information the app or service requires in order to function properly. The Commission's proposal establishing that a personal health record needs only have the "technical capacity to draw from multiple sources," although a minor change in the wording, makes no such differentiation between those records that actually do collect information from multiple sources, and instead functions to include a seemingly limitless amount of scenarios based on technical capability, rather than on design and function.

Therefore, in order to remain true to the original intent of the HBNR, we urge the Commission to make clear that a personal health record not only has the technical capacity to draw PHR identifiable health information from multiple sources, but that it also has the functionality and actually does incorporate data from multiple sources.

[12] NPRM at 37826.
[13] 16 C.F.R. § 318.2 (2022).

## V. The NAI is Supportive of the Commission's Proposal to Provide for Electronic Notice but Does Not Believe a New Definition of "Clear and Conspicuous" Is Necessary

The Commission proposes expanding the methods of consumer notice in the event of a breach to include email and one or more other electronic means as an alternative to providing written notice via first class mail, and adding a definition of "clear and conspicuous" to guide companies in effectuating this notice.[14] The NAI appreciates the Commission's effort to make compliance more accessible and efficient, and we support this proposed change to broaden the methods available for vendors and related entities to provide consumer notice. However, we believe adding a new term for "clear and conspicuous" is unnecessary and likely confusing, and instead urge the Commission to insert this language directly into §318.5 of the Rule.

### *A. The NAI Supports the Commission's Proposal to Provide for Electronic Notice in the Event of a Breach*

As the Commission notes, a major goal of this rulemaking is to make the HBNR more understandable, and ensure that victims of breaches of security are provided complete and accurate information about the exposure of their sensitive information.[15] Because interactions between consumers and vendors of PHR/PHR related entities overwhelmingly occur online, through either a mobile app or website, it logically makes the most sense to provide consumers notice of a breach in a medium that reflects their relationship with a company in order to reduce potential confusion and increase the likelihood that they receive and understand the notification. Additionally, providing for notice via electronic mail will be more affordable and efficient for regulated entities, likely increasing rates of compliance, as well as the rate with which consumers are successfully notified. These changes modernize the Rule, ultimately benefiting affected consumers and businesses alike by making notice unavoidable and consistent with the consumer's relationship with the product.

Further, the NAI emphasizes that providing for electronic notice in the manner proposed by the Commission does not run afoul of traditional principles of data minimization. Given the increasingly "online" relationship between vendors of PHR/ PHR related entities and the proposed prerequisites for use of the alternative electronic notice mechanism, an entity likely already has the consumer's email address and consent to contact the consumer electronically when they registered on the app or through the online service's webpage. If anything, requiring written notice via first-class mail to the consumer's physical address may prove to be more difficult and less aligned with data minimization principles if the notifying entity did not require a consumer to provide a physical mailing address upon signing up for the online service.

The NAI also supports the Commission's proposal to provide a model notice for use by notifying entities, and believes it will be helpful in increasing rates of compliance and understanding of the Commission's expectations.[16] However, we urge the Commission to make use of the model notice *voluntary*, and allow notifying entities to provide alternative notices aligned with the

[14] NPRM at 37827.
[15] NPRM at 37827.
[16] NPRM at 37827.

Commission's established requirements. A helpful analogy can be found in data protection assessment (DPA) requirements across state privacy laws. For example, in its implementing regulations, the Colorado Privacy Act (CPA) provides covered businesses the ability to use the same data protection assessment used for another jurisdiction's law or regulation, provided it is compatible with Colorado's specific requirements.[17] By allowing companies to use the same DPA across multiple state laws, the CPA promotes flexibility, and allows companies to preserve resources while still maintaining compliance. Thus, the Commission should similarly provide a model notice as a voluntary resource, and permit notifying entities to provide alternative forms of notice that comply with the Rule's substantive requirements.

### *B. The NAI Urges the Commision to Include Detailed Electronic Notice Requirements Directly into Section 318.5 of the Rule and Refrain from Creating a New Definition of "Clear and Conspicuous"*

In expanding the Rule to provide for breach notification by electronic mail, the Commission also proposes a new definition of "clear and conspicuous" to describe how said notice should be displayed to consumers.[18] While the NAI appreciates the Commission's guidance here, and recognizes the importance of clear, straightforward breach notifications to consumers, we are concerned that describing these criteria within a new definition of "clear and conspicuous" is unnecessary and confusing in light of other common applications of the term. Instead, we urge the Commission to insert the notice requirements for electronic mail directly into §318.5 of the Rule.

The "clear and conspicuous" standard is widely used across varying privacy laws and regulations, and generally requires that disclosures be in a reasonably understandable form. Since the meaning of "clear and conspicuous" depends on the specific application of the term, of which there are many beyond the scope of this Rule, it is unnecessary and would be impractical to adopt a prescriptive definition for this term within the Rule. Flexibility in this standard is important, as there are multiple different ways for companies to provide notification to consumers that is "clear and conspicuous" based on the type of notice, their relationship with consumers, where they sit in the larger online ecosystem, and the consumer's reasonable expectations. For this reason, it is helpful to think of "clear and conspicuous" as used across the various privacy laws as a high-level guiding principle that works to effectuate meaningful consumer notice, analyzed on a case by case basis. In an effort to contribute to the guiding principles for drafting effective notices to consumers about the collection and use of their data, the NAI published our Best Practices for User Choice and Transparency in 2022, which identifies practical suggestions based on a wide range of legal requirements to guide companies in maximizing effective and efficient notice and choice mechanisms.[19]

---

[17] 4 C.C.R § 904-3-8.02(B) ("If a Controller conducts a data protection assessment for the purpose of complying with another jurisdiction's law or regulation, the assessment shall satisfy the requirements established in this section if such data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.").

[18] NPRM at 37827.

[19] Best Practices for User Choice and Transparency, The NAI (2022), https://thenai.org/press/nai-best-practices-for-user-choice-and-transparency-help-companies-avoid-dark-patterns-in-tailored-advertising/.

The NAI therefore recommends that the Commission include the requirements for "clear and conspicuous" notice by electronic mail directly into the "methods of notice" section of the Rule, as opposed to creating a new definition that could create confusion with respect to the overarching meaning of the term in other contexts.

## VI. The NAI Opposes the Commission's Proposal to Require Notifying Entities to Include Description of Potential Harms

The Commission's proposed additions to the Rule's notice requirement – such as detailed contact information and a thorough list of the types of PHR identifiable health information exposed – are reasonable additions that adequately provide affected individuals with relevant information about a breach of their sensitive health data. However, the Commission also proposes expanding the content of the required notice to individuals to include a brief description of potential harm that could result from the breach.[20] The NAI opposes the addition of this requirement and urges the Commission to exclude it from the final version of the Rule.

Harm in the context of data breaches is often difficult to predict, and doing so often involves speculating about potential future events. While traditional breach notifications typically relate to well established harms such as identity theft and financial injury, it is substantially more difficult to predict potential harms regarding consumers' health data.

The NAI agrees that it is important to equip affected individuals with relevant information about the nature of a breach, including through a detailed inventory of the information compromised and a mechanism by which to ask questions and obtain more information about the incident. However, requiring notifying entities to speculate in a consumer notification about potential, often unknown or unlikely harms that could be associated with a breach, is unreasonable. What is more, being confronted with a list of unfounded harms, particularly where there is neither significant evidence nor likelihood of such harms, would be confusing and overwhelming to affected individuals reading the notices without significant context of the likelihood of those harms.

Consequently, requiring notifying entities to speculate about the potential harms one could experience as a result of the breach is unnecessary and inefficient, and we urge the Commission to excise it from the final Rule.

## VII. Conclusion

The NAI thanks the Commission for the opportunity to provide comments on its proposed rule, and appreciates the Commission's efforts to collaborate with industry on these important topics. We look forward to being a resource to the Commission, and working collectively to advance consumer privacy while supporting and uplifting innovation and competition in the digital advertising industry.

[20] NPRM at 37828.