epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL TRADE COMMISSION

Request for Comment on Notice of Proposed Rulemaking to Amend the Health Breach Notification Rule

88 Fed. Reg. 37,819

August 8, 2023

By notice published on June 9, 2023, the Federal Trade Commission (FTC or Commission) has requested comments on a notice of proposed rulemaking to amend the Health Breach Notification Rule.[1] The FTC's proposed rule clarifies that covered entities include mobile apps and other digital services providers to reflect how consumers interact with health services providers in the modern era and expands the definition of a "breach of security," emphasizing that an unauthorized disclosure constitutes a breach.

The Electronic Privacy Information Center (EPIC) submits these comments in support of the proposed changes and to share additional recommendations and expertise with the Commission. EPIC commends the Commission for using its authority to protect consumers' sensitive health information and is encouraged by recent enforcement actions under the long-underutilized Health Breach Notification Rule. EPIC is a public interest research center in Washington, D.C. established in 1994 to focus public attention on emerging civil liberties issues and to secure the fundamental right to privacy in the digital age. EPIC has a particular interest in

[1] Notice of Proposed Rulemaking, Health Breach Notification Rule, 88 Fed. Reg. 37,819 (June 9, 2023), https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12148.pdf [hereinafter "NPRM HBNR"].

data protection and has played a leading role in developing the authority of the FTC to address emerging privacy and cybersecurity issues and to safeguard the privacy rights of consumers.[2] EPIC has filed comments to encourage the Commission to establish a data minimization framework to best protect consumers' privacy[3] and has advocated for heightened protections for particularly sensitive information, such as health data.[4]

EPIC supports the proposed rule modifications that clarify the scope of covered entities and what constitutes a breach of security under the Rule. Section I of these comments focuses on the definitions that broaden the scope of covered entities to include platforms like mobile applications, urging the Commission to include "wellness" products more explicitly and further define the term "furnishing" within the definition of "health care provider." Section II concentrates on the meaning of a breach of security, confirming the Commission's understanding that an unauthorized disclosure is a breach of security and encouraging the Commission to further clarify that a breach includes the collection of more identifiable health information than is necessary to provide the product or service requested by the consumer. Section III notes that the revised definition of "PHR related entity" is strong but highlights the need for strict requirements concerning what qualifies as "de-identified" health information. Finally, Section IV applauds the Rule's improved notice and compliance mechanisms.

---

[2] *See, e.g.*, Consumer Reports & EPIC, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking* (Jan. 26, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf; EPIC, *What the FTC Could Be Doing (But Isn't) To Protect Privacy: The FTC's Unused Authorities* (June 2021), https://epic.org/privacy/consumer/EPIC-FTC-Unused-Authorities-Report-June2021.pdf.

[3] EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem* (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf.

[4] Suzanne Bernstein, *Data Minimization: Bolstering the FTC's Health Data Privacy Authority*, EPIC (July 13, 2023), https://epic.org/data-minimization-bolstering-the-ftcs-health-data-privacy-authority/.

I. The proposed rule appropriately broadens the scope of covered entities to include platforms like mobile apps.

Responsive to Topics 1 and 4.

EPIC supports the expanded range of entities covered under the proposed rule. Consumer health information is particularly sensitive and can be very lucrative when exploited for commercial gain. The HBNR is a critical piece authority for the Commission to address health data security and abuse issues that fall outside of HIPAA's narrow scope. As the Commission outlined in the NPRM, for HBNR enforcement authority to be most effective, the scope of covered entities and information should "reflect the current state of technology for health apps and connected devices, as well as emerging technological capabilities[.]"[5]

The new and modified definitions in the proposed rule that will determine the scope of the HBNR enable the Commission to hold entities accountable based on the nature of the entity *or* the type of information that the entity processes. The modified definition of "PHR identifiable health information" includes two new terms: "health care provider" and "health care services or supplies." The definitions of these new terms clarify the Rule's application to entities that more obviously provide health services, as well as any online service or app that happens to process or provide health related information.

The modified "personal health record" definition describes the scope of covered entities based on their technical capacity for data collection. The new definition analyzes whether an app or product would be considered a personal health record based on its "technical capacity" to draw information, including PHR identifiable health information, from multiple sources. EPIC supports this definition because it rightly shifts the risks associated with personal data collection from the consumer to the entity with the "technical capacity to draw information from multiple

[5] NPRM HBNR at 37,823.

sources." If an app has the capacity to draw PHR health information from multiple sources, it can qualify as a personal health record—regardless of consumer choices or preferences.

Given the dramatic spread of health apps and other online health products that fall outside of HIPAA's narrow protections, it is valuable that the proposed definition of "health care services and supplies" provides an explicit, non-exhaustive list of examples.[6] While including terms in the definition like sleep, diet, and fitness indicate that wellness apps and services can be considered "health care services or supplies," the Commission should explicitly include the term "wellness" in the definition. The wellness industry is booming and continues to create and collect an enormous volume of health data (and other data that can be combined to become health data).[7] The Commission should make clear that a wellness product is within the scope of "health care services or supplies" by including the term in the definition. In this way, PHR identifiable health information would correctly reflect the scope and breadth of health information subject to the HBNR.

The Commission should also clarify or further define the term "furnishing" within the definition of "health care provider."[8] Under the proposed definition, an entity is a health care provider if it furnishes "health care services or supplies," a term that is separately defined. However, the meaning of "furnishing" in this context is not clear. Does an entity have to provide health care services or supplies for a particular duration or number of times in order to "furnish[]" them (and thus become a covered entity under the Rule)? What if the entity is not actively providing health care services or supplies when there is a breach or unsecured access,

[6] NPRM HBNR at 37,835.
[7] Shaun Callaghan et al., *Feeling good: The future of the $1.5 trillion wellness market*, McKinsey Insights (Apr. 8, 2021), https://www.mckinsey.com/industries/consumer-packaged-goods/our-insights/feeling-good-the-future-of-the-1-5-trillion-wellness-market.
[8] NPRM at 37,835.

even though it has provided them in the recent past? Because the term "furnishing" is central to understanding the scope of the rule, the Commission should expressly define the term, making clear the broad sweep of the "health care provider" category.

II. A 'breach of security' rightly includes unauthorized disclosures of health data but should also encompass overcollection and unauthorized retention of data.

Responsive to Topic 2.

EPIC supports the Commission's clarification that a breach of security under the rule includes unauthorized acquisition of PHR identifiable health information that occurs as a result of a data security breach or an unauthorized disclosure. The proposed clarification rightly underscores that data security incidents extend beyond malicious and unintended breaches. Indeed, it is also a breach when an unauthorized party is *intentionally* given access to PHR identifiable health information by an entity entrusted with safeguarding that data. We support the Commission in taking action to protect consumers from such exposure.

We encourage the Commission to further clarify that a breach of security under the rule also covers the scenario in which an entity that collects more identifiable health information than necessary to provide the product or service requested by the consumer. Both the Commission and Congress (through its definition of "breach of security" in the Recovery Act)[9] recognize that when an entity obtains identifiable health information about an individual without that individual's authorization, a breach of security has occurred. Because a reasonable consumer would not typically authorize a company to collect more data than is necessary to provide the product or service they are seeking, any collection in excess of that should be presumptively

[9] 42 USC 17921 § 13400(1)(A) ("The term 'breach' means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.").

treated as an unauthorized acquisition of PHI. In other words: when an entity acquires an individual's identifiable health information in excess of what the individual implicitly authorizes, a breach of security has occurred. The most effective way to ensure that sensitive health information is not breached is to disincentivize the unnecessary collection of that information the first place and to incentivize its deletion once the data is no longer needed for the original purpose of collection. As the saying goes: you don't need to protect what you don't collect.

Take for example a dentist who tells her patient that she needs to floss more. The dentist encourages the patient to download an app that will reminder her to floss daily, but the app collects information related to the patient's height, weight, fitness level, and location that are unrelated to the service the patient is seeking (i.e., flossing reminders). The app also syncs with the patient's general health app on her phone, from which it acquires information relating to her heart rate, sleep information, and menstrual cycle. Because the app's acquisition of that information is not authorized by the patient (insofar as it not necessary to the provision of flossing reminders), a breach has occurred. The Commission should thus clarify that the Rule's definition of "breach of security" also extends to this type of overcollection of PHR identifiable health information.

Similarly, EPIC urges the Commission to clarify that an entity which retains identifiable health information for longer than necessary to serve the purpose for which it was collected has triggered a "breach of security." An entity that retains PHR identifiable health information for any significant length of time is highly likely to retrieve (i.e., acquire) such information from the database in which it is stored—for example, to periodically back such data up or to transfer it to a different storage device. If the entity carries out such processes beyond the period of time implicitly authorized by a consumer, it has accordingly breached the security of that data.

Excessive retention of PHR identifiable health information, therefore, can also constitute an unauthorized acquisition under the HBNR.

In response to Question 1 (Topic 2), the Commission's revised definition of "breach of security" is helpful because it provides entities with more clarification and information with respect to their obligations, which will promote compliance. Entities that take adequate measures to prevent unauthorized access to identifiable health information will not need to make significant changes to their business practices. This clarification will help guide businesses that need to improve their data security practices, which will benefit consumers.

In response to Question 2 (Topic 2), the HBNR should make clear that overcollection of PHR identifiable health information is itself is a form of unauthorized disclosure, as an entity acquiring PHR identifiable health information from an individual in excess of that individual's implied authorization has triggered a breach of security.

III. The revised definition of 'PHR related entity' is strong but highlights the need for strict 'de-identification' requirements.

Responsive to Topic 3.

We strongly support the Commission's revised definition of "PHR related entity" to include a non-HIPAA-covered entity that (1) offers products or services through the website of a vendor of personal health records; (2) offers products or services through the websites of HIPAA-covered entities that offer individuals personal health records; or (3) accesses information in a personal health record or sends information to a personal health record.

As explained in Section I, EPIC supports extending the scope of "PHR related entity" to cover online services, including mobile applications. First, extending the rule to include vendors of personal health records through any online service, including mobile applications, is appropriate and consistent with the way consumers access health information today.

Second, the Commission should limit the data that falls outside of the scope of the HBNR to the greatest extent possible in order to protect consumers' personal health information. To that end, the Commission should encourage the Department of Health and Human Services to update its section 13402 guidance ("Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals")[10] to specify that data minimization is a *required* methodology for entities to make personal health information "unusable" to unauthorized individuals. The current HHS guidance states that PHI is rendered unusable, unreadable, or indecipherable if the electronic PHI is encrypted as specified in the HIPAA Security Rule consistent with NIST encryption standards or when the media on which PHI is stored is destroyed and cannot be reconstructed or destroyed consisted with NIST standards.[11] But the Commission should encourage HHS to add a third, mandatory methodology to this list: a data minimization framework requiring that the collection, use, sharing, and retention of PHI be limited to that which is reasonably necessary to fulfill the authorized purpose for which the PHI is collected (plus narrow additional purposes that HHS may specify). Such a methodology would render extraneous PHI unusable, unreadable, and indecipherable to unauthorized individuals *because that data would be unavailable to begin with*.

The Commission's definition of "PHR related entity" also highlights the importance of ensuring that "de-identified" data not fall out of the HBNR's coverage unless it is truly anonymized. As proposed, PHR vendors that "de-identify" identifiable health information before

[10] 45 CFR § 164.402 ("*Unsecured protected health information* means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5.").
[11] Dep't of Health & Human Servs., *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (2020), https://www.hhs.gov/guidance/document/guidance-render-unsecured-protected-health-information-unusable-unreadable-or.

sharing it with third party service providers have rendered the data not PHR identifiable health information subject to the HBNR. But so-called "de-identification" techniques are often inadequate, leaving protect consumers' highly sensitive health information susceptible to re-identification.[12] Accordingly, the Commission should narrowly tailor what information is "de-identified" to data that is truly anonymized—for example, datasets that are rendered differentially private through noise injection. The Commission should set threshold requirements for effective de-identification to ensure that vendors and third parties are taking adequate steps to prevent reidentification of an individual's health information. EPIC would recommend a de-identification standard that is consistent with the one laid out in the proposed the American Data Privacy and Protection Act ("ADPPA").[13] This standard requires, among other things, that covered entities "take[] reasonable technical measures to ensure that the information cannot, *at any point*, be used to re-identify any individual or device[.]"[14]

IV. The proposed rule's improved notice and compliance mechanisms will benefit consumers.

Responsive to Topics 5, 6, 7.

EPIC supports the proposed rule's improved notice requirements. The modified requirements for the content, timing and type of notice will benefit consumers and promote compliance. In addition to the requirement for notice to be communicated in a clear and conspicuous way, EPIC applauds the addition of the term "electronic mail" to ensure that notice is effectively delivered to consumers.[15] In the event of a breach, the two-pronged definition

[12] Natasha Lomas, *Researchers spotlight the lie of 'anonymous' data*, Tech Crunch (July 24, 2019), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/; *Re-identification of "Anonymous" Data is Scarily Simple*, Anonyome Labs (Dec. 17, 2020), https://anonyome.com/2020/12/re-identification-of-anonymous-data-is-scarily-simple/.
[13] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).
[14] *Id.* at § 2(12) (emphasis added).
[15] *Id*.

requires notification through the combination of email with either a text message, in-app message or an electronic banner on the website or app. This modification acknowledges that email may not be the most reliable way to effectuate notice while allowing an entity to use communication pathways that already exist on their app or website. By requiring email *and* an in-app or website notice option, the expanded definition enables entities to have the best chance at notifying consumers regardless of whether they reliably check their email or continue to use the entity's app or website. We also note that the "electronic mail" definition is consistent with the principles of data minimization because it does not require the entity to collect information beyond what is likely already gathered (consumer email address) to effectuate notice.

Based on the sensitivity of the information involved in the event of a breach and the high risk of consumer injury from a breach, it is important that the Rule requires certain content to be apparent in the notice. In addition to providing model notice, EPIC supports the Commission's five proposed changes to expand the required content of the notice.[16] It will be particularly helpful for consumers to receive both a description of the type of information involved in the breach as well as the potential harm that could result from the breach. By contextualizing the potential harms from a breach, consumers will be better equipped to address injuries from a breach. Further, if consumers have been affected by and notified of a breach, they should have the ability to contact the breaching entity for further information. The proposed rule rightly requires entities to include contact procedures and information for consumers to contact notifying entities in the content of the notice. Finally, the proposed rule also acknowledges the potential downstream effects from third parties acquiring unsecure PHR identifiable health information. The notice requirements include information about any third party that acquired

[16] *Id.*

unsecured PHR identifiable health data as the result of a breach. Therefore, not only does the proposed rule provide consumers with necessary information, but it also requires breaching entities to acknowledge and describe downstream effects of the breach.

EPIC also supports the Commission's general effort to expand the Rule's readability and promote compliance. The consolidated notice and timing requirement makes clear when how and when notice must be effectuated. Certain notice and timing processes are both required by the rule and reinforced by the penalty for daily non-compliance.

V. Conclusion

The Commission should adopt the proposed changes to the Health Breach Notification Rule subject to the recommendations above. EPIC applauds the Commission for its willingness to use all of its available tools to protect consumers' personal health information. If you have any additional questions, please contact EPIC Counsel Sara Geoghegan at geoghegan@epic.org.

Sincerely,

/s/ John Davisson
EPIC Director of Litigation
& Senior Counsel

/s/ Sara Geoghegan
EPIC Counsel

/s/ Suzanne Bernstein
EPIC Law Fellow

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire Ave. NW
Washington, DC 20036
202-483-1140 (tel)
202-483-1248 (fax)