August 8, 2023

Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

Submitted via regulations.gov

Re: Health Breach Notification Rule, Project No. P205405

On behalf of the Software & Information Industry Association (SIIA), the principal trade association for those in the business of information, we write to provide feedback regarding the proposed revisions to the Health Breach Notification Rule (HBNR) request for public comment. SIIA represents over 450 companies in academic publishing, education technology, financial information, software, platforms used by millions worldwide, and data analytics and information services. Our mission is to protect the three prongs of a healthy information environment essential to that business: creation, dissemination and productive use.

The Commission's request for public comment frames the proposed revisions as designed to "ensure that the Rule remains relevant in the face of changing business practices and technological developments."[1] We agree that certain changes to the text of the current notification regime are helpful for clarifying the scope of the Rule. Unfortunately, the amended definition of "health care provider" would expand its meaning to many new entities whose inclusion makes little sense under the Rule. The revised data breach definition would similarly require endless notifications and needlessly confuse and concern consumers. Further, we believe it is important to resolve any lack of clarity regarding the definitions surrounding third party service providers and how they are distinct from digital and advertising platforms. Finally, we caution against prescribing inflexible requirements such as affirmative express consent to qualify for consumer authorization of data disclosure.

1. Changes Reflected in the Proposed Rule

A. Comments on *Clarification of Entities Covered*: The definition of "health care provider" should not be expanded to cover entities beyond those traditionally focused on providing health care products or services.

Under the HBNR proposal, the Commission would expand the definition of "health care provider" to cover a broad range of "health apps and similar technologies not covered by HIPAA."[2] A fair reading of the underlying statutes, including 42 U.S.C. 1395x(u) and 42 U.S.C. 1395x(s), makes clear that the proposed definition would go well beyond how the term "health care provider" is understood under U.S. law and how consumers and businesses are likely to understand the term. For example, while HIPAA

[1] Federal Trade Commission, "Health Breach Notification Rule" (June 9, 2023), 88 FR 37819 (https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12148.pdf) ("HBNR"), at 37822.
[2] *Id.*

is limited to "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 [title 42], a fund,"[3] the proposed Rule would cover any "entity furnishing health care services or supplies" to include "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."[4]

Expanding the definition of health care provider in this way would render a wide swath of entities whose business models are well outside those covered by the Rule subject to the Rule's requirements. The expansive definition of "supplies" would capture any website offering wellness products as a "health care provider." Thus, a store that sells third party fitness products would be required to notify consumers in case of a breach under the proposed Rule. We do not believe this is the intended or proper scope of the Rule. Instead, we recommend at the very least that "or supplies" be struck from the proposed definition to avoid this result.[5] While technological advancements in the health and wellness market raise important questions for consumers within the FTC's authority, the proposed expansion of the HBNR in this manner would also go well beyond statutory parameters.[6]

We are lastly concerned that the proposed changes would not align with consumer expectations around data privacy for entities covered by HIPAA and non-HIPAA entities such as third-party online apps. For example, HIPAA does not cover data collected by fitness apps. Treating online apps not associated with medical providers the same as hospitals for purposes of consumer notification would create a conflict in data protection frameworks under U.S. law. Accordingly, we recommend the Commission follow the approach in HIPAA and maintain the separation between HIPAA-regulated entities and non-HIPAA regulated entities.

B. Comments on *Clarification Regarding Types of Breaches Subject to the Rule*: Relevant security breaches should be limited to those that cause or pose a significant risk of harm to consumers.

The proposed Rule would expand the scope of what constitutes a security breach to cover any unauthorized disclosure or access regardless of harm. While we recognize the importance of striking the right balance between over- and under-notification, the expanded scope would cover instances in which

[3] 42 U.S.C. § 1395x(u).
[4] HBNR at 37823.
[5] While HIPAA does define "health care services or supplies" broadly in 42 U.S.C. 1320d(3), the intent of that definition is to set standards within the medical community with regard to determining "individually identifiable health information." Standard setting in the medical community is a fundamentally different policy aim than disclosure of data breaches. Moreover, HIPAA does not contemplate extending its requirements to the types of third parties contemplated by the Commission's proposed definitional change.
[6] We recognize that the American Recovery and Reinvestment Act of 2009 directed the FTC to establish a "temporary breach notification requirement for vendors of personal health records and other non-HIPAA covered entities." 42 U.S.C. § 17937. The statute directed the FTC to "promulgate interim final regulations by not later than the date that is 180 days after February 17, 2009" with a sunset provision if "Congress enacts new legislation establishing requirements for notification in the case of a breach of security." *Id.* That has not occurred, and we believe the Commission does not have the authority to extend the breach notification rule to entities as contemplated by the proposal.

there is no reasonable likelihood that any personal data could be used improperly or cause harm to individual consumers. Requiring notice in all instances of breach under this broad definition would create "notice fatigue" and create significant additional compliance challenges for companies.

We believe the approach taken in the current Rule, which includes a rebuttable presumption that unauthorized access equates to unauthorized acquisition unless there is clear evidence that acquisition did not occur, is sufficient to address the risk to consumers. We recommend the Commission maintain its risk-based approach to data breach notification, which reflects an assessment of harm associated with data that has been accessed inappropriately. In addition, we would caution against relying on the text of the Recovery Act or the Commission's actions in *GoodRx* and *EasyHealthcare* as necessitating expansion of the breach threshold in the manner contemplated by the proposed Rule.

2. <u>Changes Considered but Not Proposed</u>

A. Comments on *Modifying Definition of Third Party Service Provider*: Third party service providers should not include advertising and analytics providers and platforms.

We recommend that the definition of third party service providers not include "advertising and analytics providers and platforms."[7] We do not believe that the concerns identified in the *GoodRx* matter support a material change to the approach taken under the current regulations. Instead, we suggest that the burden remain on PHR related entities and vendors—rather than on advertising and analytics providers and platforms, including no-view cloud storage providers—to ensure that any PHR identifiable health information is protected wherever such data is used or shared.

To provide effective service and tools that many businesses, including small businesses, depend on, such providers and platforms may receive data from massive numbers of third parties. It would be technically impractical—if not impossible—for them to individually inspect and determine whether the data received is potential PHR identifiable health information. This challenge is exacerbated by both the HBNR proposal's expansive conception of PHR identifiable health information and the requirement to determine whether information was shared without authorization – knowledge likely possessed by a vendor or PHR related entity, not the receiving advertising or analytics provider or platform.

The challenges of this sort of compliance regime would be compounded by a proposed rule the Commission considered and rejected, which would designate providers and platforms as third party service providers "anytime they access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured PHR identifiable health information when providing services to vendors of personal health records and PHR related entities."[8] This would create significant uncertainty about which entities are within the definition and even when they are subject to the Rule's requirements. For example, it is possible on one hand that a Fortune 500 company becomes a service provider in perpetuity the minute any branch of such a company accesses unsecured PHR identifiable health information. On the other hand, a company that discloses PHR identifiable health information to a PHR related entity, but then ceases this aspect of its business, may now not fit the definition even though they are the originator of the data. Given the requirements imposed on third party service providers under the Rule, this ambiguity within the definition itself would create significant regulatory uncertainty.

[7] HBNR at 37831.
[8] *Id.*

B. Comments on *Defining Authorization and Affirmative Express Consent*: Requiring overly prescriptive requirements for consumer authorization would render compliance impractical and frustrate consumers.

The Commission correctly opted not to define "authorization" as "affirmative express consent" for any disclosure of data subject to the Rule. We believe doing so would be imprudent. Requiring affirmative consent for all data covered by the Rule would force consumers attempting to use these devices to read—or for voice-activated devices, even listen to—a potentially lengthy privacy policy more likely to annoy and fatigue these consumers than meaningfully educate them regarding disclosures.

Similarly, we do not believe the prohibition on "dark patterns" requires affirmative consent by default. It is dangerous to assume that consent regimes necessarily equate to either express consent or "interfaces designed with the substantial effect of subverting or impairing user autonomy and decision-making" – this would create significant regulatory uncertainty.[9] Instead, we believe transparency through appropriate disclosures via a privacy notice or user interface calibrated to consumers' reasonable expectations would strike a better balance for both consumers and service providers.

As the Commission considers additional feedback on these items, we caution against prescribing overly specific requirements for consumer authorizations. Inflexible requirements that assume contemporary consumer interfaces would inevitably render engagement with increasingly complex technologies, such as voice-activated or other convenience-enhancing devices, impractical in the future. Even if such rules incorporate the gamut of technologies available on the market today, the nuances of consumer notices and their practicalities will inevitably evolve.

* * *

Thank you for considering our views. We look forward to continued engagement with the Commission and would be happy to discuss any of these issues further with you.

Respectfully submitted,

Paul N. Lekas
Senior Vice President, Global Public Policy & Government Affairs

Anton J. van Seventer
Counsel, Privacy and Data Policy

[9] *Id.* at 37830.