Before the
Federal Trade Commission
Washington, D.C.

In re	Docket No. 2023-12148
Health Breach Notification Rule	

COMMENTS OF
THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

In response to the Notice of Proposed Rulemaking (the "NPRM") published in the Federal Register at 88 Fed. Reg. 37819 (June 9, 2023), the Computer & Communications Industry Association ("CCIA")[1] submits the following comments:

I. INTRODUCTION

CCIA is pleased to participate in the Commission's proposed rulemaking to amend the Health Breach Notification Rule ("HBNR" or "the Rule").[2] The Association appreciates the Commission's efforts to provide additional clarity around the scope of the Rule.

CCIA and its members strongly support the protection of consumer data and understand that Americans are rightfully concerned about the proper safeguarding of their sensitive health information. We provide comment herein on several of the provisions raised in the NPRM, including the proposed amendments to the Rule and the additional considerations. The comments, however, raise questions about the Commission's authority to broaden the scope and aims of the HBNR.

[1] CCIA is an international, not-for-profit association representing a broad cross-section of technology and communications firms. For over fifty years, CCIA has promoted open markets, open systems, and open networks, advocating for sound competition policy and antitrust enforcement. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. For more, visit www.ccianet.org. Legal research and summaries provided by Dalia Wrocherinsky, CCIA Law Clerk, were instrumental to these comments.

[2] All citations to the NPRM refer to the long-form document released on May 18, 2023 rather than the edition published in the Federal Register. Federal Trade Commission Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule (May 18, 2023).

II. DISCUSSION

These comments seek to aid the Commission in its efforts to clarify the Rule's applicability to health applications and other similar technologies.

A. Commission's Rulemaking Authority

The American Recovery and Reinvestment Act of 2009 ("Recovery Act") had the twin aims of advancing the use of health information technology and strengthening privacy and security protections for health information.[3] The Recovery Act directed the Department of Health and Human Services to "study, in consultation with the FTC, potential privacy, security, and breach notification requirements" with respect to those entities not subject to the requirements of the Health Insurance Portability and Accountability Act.[4] It is not clear if, or when, the report was published. Regardless, it was made evident that "[u]ntil Congress enacts new legislation implementing such recommendations, the Recovery Act *contains temporary requirements*, to be enforced by the FTC, that such entities notify individuals in the event of a security breach."[5] Given the temporary nature of the Commission's authority, the FTC's finalization of these proposed amendments to the Rule may be questionable.

Rather than resolving these uncertainties, the Commission has advanced a broader interpretation and enforcement of the HBNR which may exceed the Commission's statutory authority.

Regarding the Commission's 2021 Policy Statement, both Commissioners Noah Phillips and Christine Wilson dissented against the improper expansion of the Commission's statutory authority. Commissioner Wilson described how the HBNR was "narrowly crafted to apply in limited, highly specific circumstances" – further evidenced by the interagency cooperation and cross referenced terminology defined in the Rule and the Social Security Act.[6] Ultimately, as Commissioner Phillip noted, the HBNR was never intended to become a "broad privacy rule that

[3] The American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).
[4] 74 Fed. Reg. 42961 (Aug. 25, 2009).
[5] *Id*.
[6] *See* Dissenting Statement of Commissioner Christine S. Wilson, Policy Statement on Breaches by Health Apps and Other Connected Devices, September 15, 2021.

extends far beyond the personal health records vendors contemplated by Congress."[7] An overly broad interpretation of the Rule – one where "all applications consumers use to store and process data about anything related to health are health care providers" – diverges from the definitions used by other agencies and goes beyond what "Congress, the Commission, and sister agencies had in mind in drafting them."[8]

The Commission had not enforced the HBNR for over a decade, despite it becoming fully effective in 2010. Instead of providing guidance on how the Rule applies to newer technologies, such as by referencing its legislative history and statute, the Commission seeks to formalize its broad interpretation of the Rule in the enforcement actions against GoodRx and PreMom. These enforcement actions reflect many of the topics outlined in its 2021 Policy Statement.[9] As observers have described, "this is the second time the FTC has charged an [entity] with a violation of the HBNR, despite the lack of statutory authority (or even a final rule) that would bring app developers under the scope of the HBNR."[10] Although the Commission's new interpretations of the Rule were aimed at filling the gap in the protections of non-Health Insurance Portability and Accountability Act (HIPAA) regulated digital health information, it would essentially "retroactively codify" many aspects of the Policy Statement.[11] This codification would, amongst other things, include a drastic departure from the common understanding of what constitutes a breach of security.

Rather than pursuing an expansion of its authority, the Association urges the Commission to use this proceeding to provide much-needed clarity for businesses and consumers alike.

---

[7] *See* Dissenting Statement of Commissioner Noah Joshua Phillips, Policy Statement on Breaches by Health Apps and Other Connected Devices, September 15, 2021.
[8] *Id*.
[9] FTC Policy Statement on Breaches by Health Apps and Other Connected Devices (Sept. 15, 2021), https://www.ftc.gov/news-events/events-calendar/open-commission-meeting-september-15-2021 ("2021 Policy Statement").
[10] *See* Maneesha Mithal, et al., *FTC Announces Proposed Settlement with Premom Fertility Tracking App for Privacy Practices*, Wilson Sonsini (May 24, 2023), https://www.wsgr.com/en/insights/ftc-announces-proposed-settlement-with-premom-fertility-tracking-app-for-privacy-practices.html.
[11] *See* Maneesha Mithal, et al., *FTC Announces Proposed Amendments to the Health Breach Notification Rule*, Wilson Sonsini (May 22, 2023), https://www.wsgrdataadvisor.com/2023/05/ftc-announces-proposed-amendments-to-the-health-breach-notification-rule/.

B. Proposed Amendments to the Definition of "PHR Identifiable Health Information"

The Commission describes that the addition of the new terms "health care provider" and "health care services or supplies" are to provide needed clarity about the types of data and entities covered by the Rule.[12] However, CCIA is concerned that their additions go beyond clarification to encompass nearly all health and wellness apps and connected health devices not subject to HIPAA. For example, despite HIPAA adopting far more limited definitions of what constitutes "health care", the proposed definitions import broader language.[13] Specifically, the inclusion of an extensive list of what qualifies as "health care services or supplies" would not only incorporate purveyors of health apps but also any online store offering health products such as lotion and vitamins.

Consumers have different expectations for applications like MyChart and one to help track their fitness goals. It is unclear that imposing broad requirements that fail to acknowledge the disparity between these applications helps achieve the Commission's intended goal to "level the competitive playing field" for HIPAA and non-HIPAA covered entities. This approach is misplaced, especially in terms of the disparity between these apps. The Commission could mitigate the consequences of an overly broad definition by potentially mandating that only certain types of apps can hold themselves out to be "health apps."

C. Proposed Amendments to the Definition of "Breach of Security"

The Commission's proposed definition unnecessarily conflates two key concepts, a security incident and disclosure of data, that risks undermining the purpose of each notice.

Notifications in the event of a security incident allow a consumer to take some action to protect themselves, such as when a bad actor breaches a vendor of PHRs. In the past, the Commission has utilized notice requirements to empower consumers and prevent ongoing harm

[12] NPRM at 15.

[13] HIPAA adopts far more narrow language, limiting "health care" to actual care, services, and supplies related to physical or mental conditions, or functional status, of an individual or that affects the function or structure of the body, and prescription drugs and devices. The Health Insurance Portability and Accountability Act, 45 C.F.R § 160.103

in situations where consumers' health or safety is at risk,[14] have a financial or legal interest that needs to be protected, or it is necessary to prevent the ongoing dissemination of deceptive information.[15]

However, notification for the disclosure of data could cause consumer concern or worry even when there is no real harm, especially in scenarios where it is typical to disclose some of this information. When required, notice can be an important mechanism to help consumers take action to protect themselves and this approach is reflected in many state data breach notification laws. The Commission should not try to re-purpose this powerful equitable tool into a penalty, nor as Commissioner Phillips cautioned against, "take[] the position of requiring consumer notice for the mere sake of the notice itself."[16]

Given that they are distinct concepts, there should be separate notification timelines to reflect different levels of risk. The Commission should take a risk-based approach here, adopting a shorter timeline for an actual breach of security – enabling consumers to take some action. In developing this requirement, the Commission could look to the language used in state data breach notification laws[17] and other federal statutes[18] to ensure they are accurate and provide necessary exceptions. CCIA recommends that any final should include some "discovered in fact" or "reasonably should have known" language to make clear that a breach does not occur if the third-party service provider had no knowledge of it.

CCIA also recommends the Commission look at various potential exceptions to a breach of security, including to:

- Prevent and detect security incidents, identity theft, fraud, harassment, or malicious, deceptive, or illegal activity; preserve the security or integrity of systems; or prosecute responsible individuals for such actions.
- Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by authorities.
- Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may be illegal.

---

[14] *See Daniel Chapter One*, No. 9329 (Jan. 25, 2010), https://www.ftc.gov/enforcement/casesproceedings/082-3085/daniel-chapter-one,
[15] *FTC v. Applied Food Sciences, Inc.*, No. 1:14-cv-00851 at 12, 21 (W.D. Tex. Sept. 10, 2014).
[16] *See* Separate Statement of Commissioner Noah Joshua Phillips, *In the Matter of Flo Health, Inc.*, FTC File No. 1923133 (Jan. 13, 2021).
[17] *See* Summary, *Security Breach Notification Laws*, National Conference of State Legislatures (Jan. 17, 2022), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws.
[18] The HIPAA breach notification rule could serve as a good example. 45 C.F.R. § 164.404.

- Perform internal operations consistent with the consumer's expectations.
- Provide a product or service a consumer requested or perform a contract with the consumer.
- Protect the vital interests of consumers.
- Process personal data for reasons of public interest in the area of public health, subject to certain conditions.

D. Proposed Amendments to the Definition of "PHR Related Entity"

CCIA appreciates the Commission's efforts to provide clarity but issues still remain concerning its overall scope. Specifically, the proposed definition should be further amended to clarify that it does not extend to non-health-related apps that solely contribute data. The Rule should not apply to technology developers and cloud service providers that simply provide technical capabilities for data exchange. CCIA urges the Commission to clearly indicate such providers are not included within the scope of this definition, especially given that they are not in the position to know what data is in their services at a given time.

E. Clarifying "What it Means for a Personal Health Record To Draw Information From Multiple Sources"

The proposed changes fail to provide any additional clarity and if adopted, would significantly broaden the Rule's scope to include a wide range of online services such as email apps. With the change, an app would qualify as a PHR if it was simply possible to draw such information from multiple sources like a wearable device. This rigid definition does not account for actual consumer use of a feature or any unforeseen uses. For example, even if the settings enabled an individual to limit the information sent to the app to only a single source, it would still be considered a PHR given its technical capacity to do so. CCIA strongly recommends the Commission revise this proposed language to account for actual consumer use and align with its own previous interpretation of what "multiple sources" refer to.[19]

[19] "... the FTC previously viewed the phrase "multiple sources" as referring to actual entities, not other data sources on the consumer's mobile or connected device, such as calendar dates." Dissenting Statement of Commissioner Christine S. Wilson, 1-2.

F. Proposed Amendments to Method of Notice

The proposed changes are welcomed but the Commission should further specify that organizations are not required to use the model method of notification. Any mandate to use a model notice would force organizations to collect or retain more data than required and undermine their efforts to adhere to the data minimization principle.

G. Proposed Amendments to Notice Content

CCIA is concerned about the proposed modifications to the substance of the notice, especially given the Commission's broad interpretation of what constitutes PHR identifiable health information. First, requiring two contact methods is a higher requirement than HIPAA. Second, requiring a description of potential harm offers little to no benefit to individuals. Notifying consumers about potential harm, even if there is no proof that there has been harm, could cause unnecessary confusion and panic from individuals, along with diluting the impact of notices. Lastly, it should be made clear that if a third party did not intend to retain the information, this should be noted in any disclosure.

III. ADDITIONAL CONSIDERATIONS

A. Proposed Definitions for "Authorization" and "Affirmative Express Consent"

As the Commission considers defining these two terms, the Association recommends reviewing the language adopted in other states to promote interoperability. Specifically, the Virginia Consumer Data Protection Act provides a strong and well-understood definition of "consent" that helps ensure such an obtained consent is not nominal nor a result of confusing language or user interfaces.[20]

B. Proposed Changes to the Definition of "Third Party Service Provider"

The Commission should not consider expanding the definition of a third party service provider to include advertising and analytics providers. Any proposed changes should avoid a

[20] Virginia Consumer Data Protection Act, S.B. 1392 § 59.1-575. ("a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. Consent may include a written statement, including a statement written by electronic means, or any other unambiguous affirmative action.").

broad reading that would create a confusing reporting obligation and additional uncertainty, especially given the lack of clarity created by the other proposed modifications.

An expansive definition would place onerous notice obligations on companies that do not provide products and services aimed at personal health records and, in fact, do not want to receive any personal health records. The definition would sweep in advertising and analytics providers that are sent any personal health records – for example, URLs that simply reference specific health conditions – whether or not the advertising or analytics providers' products and services have any connection to the purported personal health records, and whether or not the advertising and analytics providers prohibit the sending of such data. Advertising and analytics providers provide technologies that many businesses – including smaller businesses – depend on, as they provide tools to help businesses understand and measure their products and services, and better reach and serve people who may be interested in their services and products. To provide effective service, these providers often receive data from millions of third parties and may not have the practical ability to actively monitor and audit the granular data they receive.

Requiring advertising and analytics providers to inform a vendor of personal health records every time they receive a supposed personal health record would be unworkable as a practical matter. CCIA recommends the Commission to not make this change or at least to be limited to providers actually using data for actual health related purposes.

C. Proposed Changes to Timing Requirements

CCIA appreciates the Commission's inquiry into whether to extend the Rule's timing requirement. Entities suffering and recovering from a breach face a wide-range of pressures that are further compounded by a short 10-day timing requirement. The Commission could help alleviate these pressures and ensure consumers receive meaningful notification by extending the requirement to 30 days and further allowing an additional extension if the entity has a reasonable basis.

D. Paperwork Reduction Act

The Commission is also inviting comments on the Paperwork Reduction Act. The NRM estimates that the proposed changes to the informational collection requirements would cover an

additional 170,000 entities, in the event of a breach, because there are 170,000 apps in the Apple Store under "Health and Fitness."[21] Given that proposed amendments would go vastly beyond these aforementioned apps in the apps store, it seems clear that there has been insufficient impact analysis. Additionally, to assume these proposed changes would only lead to 71 breaches per year based on the breach incident rate for HIPAA-covered entities seems problematic, given that the proposed definition of a "breach" goes far and beyond HIPAA's definition. CCIA recommends the Commission review these estimates in light of these concerns.

IV. CONCLUSION

The Commission should (1) review the NPRM to ensure it comports with the bounds of its statutory authority, and (2) consider issuing an amended NPRM with more accurate and balanced language that reflects the twin aims of advancing the responsible use of health information technology and strengthening privacy and security protections for health information.

Respectfully submitted,

Alvaro Marañon
Policy Counsel
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001
amaranon@ccianet.org

Aug 8, 2023

[21] NPRM at 47.