Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

In the Matter of	)	Docket No. FTC-2023-0037
	)	
Health Breach Notification Rule	)	Project No. P205405
	)	
	)	
	)	

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION REGARDING HEALTH BREACH NOTIFICATION RULE, PROJECT NO. P205405

René Quashie
Vice President, Digital Health

Rachel Nemeth
Senior Director, Regulatory Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
rquashie@cta.tech
rnemeth@cta.tech

August 8, 2023

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY 1

II. THE SCOPE OF COVERED PARTIES SUBJECT TO THE RULE SHOULD BE APPROPRIATELY LIMITED, CONSISTENT WITH THE ORIGINAL INTENT OF THE HITECH ACT. 4

A. Congress Intended the Health Breach Notification Rule to Temporarily Regulate a Limited Set of Non-HIPAA Covered Entities That Deal With Information From Conventional Health Care Providers. 6

B. The Rule Should Limit the Scope of Health Care-Related Companies Whose Data Is Covered. 7

C. The NPRM's Proposed Revisions to the "Personal Health Record" Definition Should Not Cover Products That Do Not Actually Draw Information from Multiple Sources. 10

D. The FTC Should Not Classify Advertising, Analytics, or Cloud Service Providers as Third Party Service Providers Under the Rule. 11

III. THE FTC SHOULD NARROW ITS APPROACH TO "BREACH OF SECURITY." 13

A. A "Breach of Security" Should Be Limited to an Actual Acquisition of Protected Health Data. 14

B. The Commission Should Include Common Exceptions In the Rule's "Breach of Security" Definition. 17

IV. THE FTC SHOULD NOT PRESCRIBE ARBITRARY REPORTING TIMELINES FOR BREACH NOTICES AND SHOULD ADOPT A REASONABLE DETERMINATION TRIGGER. 19

V. THE FTC SHOULD SIMPLIFY THE RULE'S NOTICE PROCEDURES. 21

A. The NPRM's Email Notification Proposal Should Be Simplified. 21

B. The NPRM's Consumer Notice Requirements Should Not Include an Explanation of Potential Harms or a List of the Third Parties That Obtained a Consumer's Information. 23

VI. CONCLUSION. 25

Before the
FEDERAL TRADE COMMISSION
Washington, D.C. 20580

In the Matter of	)	Docket No. FTC-2023-0037
	)	
Health Breach Notification Rule	)	Project No. P205405
	)	
	)	
	)	

COMMENTS OF THE CONSUMER TECHNOLOGY ASSOCIATION

I. INTRODUCTION AND SUMMARY.

The Consumer Technology Association® ("CTA") respectfully submits this response to the Notice of Proposed Rulemaking ("NPRM") on the Health Breach Notification Rule ("HBNR" or "Rule") issued by the Federal Trade Commission ("FTC" or "Commission").[1] CTA is North America's largest technology trade association. Our members are the world's leading innovators – from startups to global brands – helping support more than 18 million American jobs. CTA owns and produces CES®, the world's most influential tech event. CTA and its members have operated for decades in a competitive marketplace to produce innovative products that provide enormous benefits to consumers and power the economy. In doing so, CTA's diverse membership have built out robust privacy and data security programs that strive to protect sensitive consumer data and earn consumer trust. CTA shares the FTC's overall priority of "[p]rotecting the privacy and security of personal health data."[2]

---

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

[2] Press Release, FTC, FTC Proposes Amendments to Strengthen and Modernize the Health Breach Notification Rule (May 18, 2023), https://www.ftc.gov/news-events/news/press-

However, based on CTA members' experience and review of the practical effects of the NPRM's proposals, certain of them are impractical, not helpful for consumers, and unduly burdensome. They also reach far beyond what Congress intended the Rule to cover. Congress did not give the Commission the authority to broadly regulate health data under the Rule, and the NPRM's contortions to expand the Rule will only complicate compliance efforts and detract from the core purpose of the Rule – facilitating timely notification of significant health data breaches. In particular, the NPRM proposals would expand the Rule well beyond the entities and consumer information that Congress intended for it to temporarily cover when it passed the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") in 2009. The NPRM's latest proposed changes to the Rule also diverge from the Department of Health and Human Services' ("HHS") parallel Health Insurance Portability and Accountability Act ("HIPAA") Breach Notification Rule and create more complexity by layering additional breach notification requirements on top of the existing patchwork of laws.

CTA discusses several objections to the NPRM proposals, provides feedback on questions raised in the NPRM, and urges additional changes to the Rule, as follows:

- Scope of covered parties (Part II). The scope of the entities covered by the Rule should be limited, consistent with the original intent of the HITECH Act, including by making clear that the Rule excludes merchants that may sell a variety of products that include health-related products, focusing on apps that actually gather health-related information from multiple sources, and excluding service providers such as cloud computing providers, analytics providers, and advertising providers, particularly when they do not

releases/2023/05/ftc-proposes-amendments-strengthen-modernize-health-breach-notification-rule.

target or are unaware of receiving covered health data.

- Scope of a "breach of security" (Part III). The Rule should remain focused on unauthorized "acquisition" of covered health data, not inadvertent or good-faith unauthorized access or disclosure where the information is not actually obtained by a third party. This will avoid overreporting and diverting resources to incidents with low or no risk of consumer harm. CTA agrees with the Commission's current proposal not to define "authorization," which would import a substantive consent requirement that is outside the proper scope of the Rule. CTA also recommends that the Rule explicitly incorporate exceptions to "unauthorized" acquisition that mirror those found in the HIPAA Breach Notification Rule and state privacy laws, for purposes of regulatory clarity.
- Reporting timelines and triggers (Part IV). The Commission should move away from arbitrary breach reporting timelines that are based on when a covered entity discovered a *potential* security incident, and instead require reporting under the Rule once a company has reasonably determined that a breach of security actually has occurred, and it should extend the timeline for reporting certain kinds of incidents. This will reduce overreporting, allow companies to devote maximum resources to investigating potential incidents, and increase harmonization with state data breach reporting laws.
- Notification form and content (Part V). The Commission should simplify the Rule's consumer notice form and content, including simplifying email notifications, and focusing on providing consumers with actionable information and avoiding requirements that companies speculate about the risks of a breach.

II. THE SCOPE OF COVERED PARTIES SUBJECT TO THE RULE SHOULD BE APPROPRIATELY LIMITED, CONSISTENT WITH THE ORIGINAL INTENT OF THE HITECH ACT.

The NPRM would expand the scope of covered parties in multiple problematic ways. First, it would expand the definition of "PHR identifiable health information" by adding a definition of "health care provider" along with "health care services and supplies."[3] While "PHR identifiable health information" currently includes health-related information that is "created or received by" a "health care provider,"[4] the new definition dramatically opens the door to who is a "health care provider" – including those that provide "health care services or supplies," including "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 provide[] other health-related services or tools."[5] In turn, a "personal health record" ("PHR") means an "electronic record of PHR identifiable health information,"[6] a "vendor of personal health records" includes one that "offers or maintains a personal health record,"[7] and a "PHR related entity" is one that "[a]ccesses unsecured PHR identifiable health information in a personal health record or sends unsecured PHR identifiable health information to a personal health record."[8] The upshot is that many new entities potentially would be "vendors of personal health records" or "PHR related entities"

[3] NPRM at 37,835.

[4] *Id.* at Proposed Rule § 318.2(i).

[5] *Id.* Proposed Rule § 318.2(e)-(f).

[6] *Id.* at Proposed Rule § 318.2(h).

[7] *Id.* at Proposed Rule § 318.2(n).

[8] *Id.* at Proposed Rule § 318.2(j).

subject to the breach notification requirements of the Rule.

Second, the revised Rule would define a "personal health record" as one that "has the technical capacity to draw information"[9] from multiple sources, regardless of whether that technical capability is used.

Third, while the definition of "third party service provider" would stay the same under the NPRM, the expansion of the scope of "PHR identifiable health information," "vendor of personal health records," and "PHR related entity" greatly expands the scope of third parties that may be included as well. In this case, "third party service providers" are those that provide services to a "vendor of personal health records" or "PHR related entity," and that, even more significantly, "[a]ccesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information."[10]

Overall, the proposed definitional changes would effectively expand the Rule's coverage well beyond Congress's intended scope for the Rule when it passed the HITECH Act.[11] The Commission should cabin any new definitions to avoid sweeping in entities that do not deal with – or have no intent to deal with – personal health information. Failure to limit these definitions threatens to chill innovation by causing entities that want to provide customers with new technology, services, and apps to be wary of potential regulatory burdens and avoid or limit their activity in the health space.

[9] *Id.* at Proposed Rule § 318.2(h).

[10] *Id.* at Proposed Rule § 318.2(l).

[11] Health Information Technology for Economic and Clinical Health, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified as amended in scattered sections of 42 U.S.C.) (a part of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009)).

A. Congress Intended the Health Breach Notification Rule to Temporarily Regulate a Limited Set of Non-HIPAA Covered Entities That Deal With Information From Conventional Health Care Providers.

The text of the HITECH Act and the statute's legislative history make clear that the HBNR was intended to only temporarily regulate non-HIPAA covered entities that handle personal health records or PHR identifiable health information until "Congress enacts new legislation establishing requirements for notification in the case of a breach of security, that apply to entities that are not covered entities or business associates. . . ."[12] Indeed, Congress meant the HBNR to be "temporary" while it pursued broader data breach reporting legislation.[13]

Further, while the NPRM seeks to expand the definition of a "health care provider" here, in parallel provisions, HIPAA defines a "provider of services" as "a hospital, critical access hospital, rural emergency hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program, or, . . . a fund.[14] Similarly, it defines a "provider of medical or other health services" to include various conventional health care providers, such as "physicians' services," "outpatient physical therapy services," and "qualified psychologist services."[15] The NPRM's proposed definition of a "health care provider" departs sharply from the well understood, existing definition of the term. And it is particularly inappropriate given that Congress meant the HBNR as a temporary stopgap measure, not one

---

[12] 42 U.S.C. § 17937(g)(2); *see also* H. R. Rep. 111-16, at 499 (*Confer. Rep. to accompany H.R. 1.*) (2009) ("The provisions in this section would no longer apply to breaches occurring after HHS or FTC had adopted new privacy and security standards for non-HIPAA covered entities, including requirements relating to breach notification.").

[13] In addition to the actual text of the HITECH Act and the applicable legislative history, the title of 42 U.S.C. § 17937, which governs breach notification requirements, is titled, "Temporary breach notification requirement for vendors of personal health records and other non-HIPAA covered entities."

[14] 42 U.S.C. § 1395x(u).

[15] *Id.* § 1395x(s).

that would re-write the existing understanding of what entities are covered as "health care providers."

B. The Rule Should Limit the Scope of Health Care-Related Companies Whose Data Is Covered.

The NPRM asks whether the Commission should make any modifications to the definitions of "health care provider," "health care services or supplies," or "personal health record."[16] CTA urges the Commission to limit the definition of "health care provider," as the proposed definition would impermissibly expand the FTC's authority beyond congressional intent and create practical implementation issues for entities that have little connection to actual sensitive health-related data.

The Proposed Rule defines "health care provider" to include "any . . . entity furnishing health care services or supplies."[17] It then defines "health care services or supplies," in turn, extremely broadly, as including "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."[18] If adopted, these new and capacious definitions could result in a wide array of app providers, online platforms, retailers, consumer wellness product suppliers, cloud service providers, and wearable device providers being covered under the HBNR as "PHR related entities" or "vendors of personal health records" because they deal with unsecured "PHR identifiable health information" drawn from this overly expansive definition of

[16] NPRM at 37,823-24, 37,826.

[17] *Id.* at 37,835, Proposed Rule § 318.2(f).

[18] *Id.* at Proposed Rule § 318.2(e).

a "health care provider."[19] This would mean that wellness apps, websites, retailers, and connected products would receive identical regulatory treatment under the HBNR to dedicated health care apps provided by healthcare organizations to give patients access to their health records. This result is far afield of the original intent of HITECH Act and is impractical for many entities that would be covered under this definition.

At a minimum, the Commission should clarify that the HBNR does not cover, as "health care providers," "vendors of personal health records," or "PHR related entities": (1) retailers of health-related products – for example, retailers of consumer wellness products; or (2) cloud service providers.

First, as currently proposed, the definition of "health care provider" would appear to sweep in both online and brick-and-mortar retailers that offer products and services "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."[20] This would, in turn, appear to impose HBNR notification obligations on retailers as "PHR related entities" that access such information about the products that consumers purchase in their point-of-sale systems.[21] The Commission should exempt retailers from the HBNR, as they should not be covered for merely selling connected fitness devices or wellness products and maintaining records from

[19] *See id.* at Proposed Rule § 318.2(j) (defining a "PHR related entity" as "an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that . . . [a]ccesses unsecured PHR identifiable health information in a personal health record or sends unsecured PHR identifiable health information to a personal health record.").

[20] *Id.* at Proposed Rule § 318.2(e)-(f).

[21] *Id.* at Proposed Rule § 318.2(n).

purchases, and it should delete the reference to "supplies" in the term "health services or supplies." This would extend the HBNR well beyond entities even remotely related to the provision of health care or the maintenance of conventional health care data, and it would potentially create breach reporting obligations that are unrelated to actual health data breaches. The proposed Rule would also be exceedingly difficult to implement and impose unreasonable burdens if it were construed to cover breaches of retail sales data that might – somewhere deep in the data – show a purchase of a health-, diet-, or wellness-related product.

Second, the Commission should clarify that cloud service providers – particularly "no-view" cloud service providers – are not covered "PHR related entities" under the Rule. This clarification would be consistent with HHS's "Guidance on HIPAA & Cloud Computing," which defines a "no-view" cloud service provider as one that maintains encrypted PHR identifiable health information on behalf of another entity without having the decryption key, and states that "the requirements of the Rules are flexible and scalable to take into account the no-view nature of the services provided by the [Cloud Service Provider]".[22] "No-look" cloud service providers are not likely to be able to determine that they even have covered health information in case of a breach, and therefore including them in scope of the rule would be an unreasonable burden. Additionally, even if a cloud provider were aware of impacted covered data, treating cloud service providers as PHR related entities "would create a problematic result for the consumer, who would receive [a breach notice] from an unfamiliar company."[23] These notices would cause confusion and would be of little use to consumers whose data may be compromised. Accordingly, the FTC should clarify that cloud service providers – and particularly "no-view"

[22] *Guidance on HIPAA & Cloud Computing*, HHS, https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology (last updated Dec. 23, 2022).

[23] NPRM at 37,825.

cloud service providers – are not covered PHR-related entities, including because by definition they do not access or send unsecured PHR identifiable health information.[24]

C. The NPRM's Proposed Revisions to the "Personal Health Record" Definition Should Not Cover Products That Do Not Actually Draw Information from Multiple Sources.

When discussing the proposed definition of "personal health record," the NPRM asks "whether an app (or other product) should be considered a personal health record even if it only draws health information from one place (in addition to non-health information drawn elsewhere); or only draws identifiable health information from one place (in addition to non-identifiable health information drawn elsewhere)."[25] And it proposes to amend the definition of a "personal health record" to be one that "has the technical capacity to draw information from multiple sources. . . ."[26] As written, Proposed Rule 318.2(h) would define any app, wearable device, or online platform that is *capable* of syncing with two or more health-related information as a "personal health record," from wearable fitness trackers to calendar apps that can be used to track daily nutrition and activities.[27] The NPRM provides an illustrative example of this:

> Diet and Fitness App Y allows users to sync their app with third-party wearable fitness trackers with the app. Diet and Fitness App Y has the technical capacity to draw identifiable health information both from the user (name, weight, height, age)

[24] *Id.* at Proposed Rule § 318.2(j). The NPRM does propose language indicating that, "While some third party service providers may access unsecured PHR identifiable health information in the course of providing services, this does not render the third party service provider a PHR related entity." *Id.* at Proposed Rule § 318.3(b). While CTA supports this language, the definition of "PHR Related Entity" should be modified to be clear that cloud service providers and other third-party service providers are not PHR Related Entities.

[25] *Id.* at 37,826.

[26] *Id.* at 37,835, Proposed Rule § 318.2(h).

[27] *See id.* at Proposed Rule § 318.2(n) ("Vendor of personal health records means an entity, other than a HIPAA- covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that offers or maintains a personal health record.").

> and the fitness tracker (user's name, miles run, heart rate), even if some users elect not to connect the fitness tracker.[28]

CTA encourages the Commission to ensure that the Rule only covers apps, connected devices, and other connected platforms that *actually obtain* PHR identifiable health information on an individual from multiple sources. That is, the Rule should not cover apps that either obtain PHR identifiable health information from a single source or that merely have the "technical capacity to draw information from multiple sources. . . ."[29] Otherwise, the Rule would technically cover apps that have built-in functionalities that are never used or used only in beta form, and where the actual health data collected is indistinguishable from that collected by an app that has only one data source.[30] That result would be arbitrary and capricious. It is also potentially confusing for app developers that must assess whether their app is "capable" of a functionality, rather than applying a bright-line rule of whether the app actually draws health information from multiple sources.

D. The FTC Should Not Classify Advertising, Analytics, or Cloud Service Providers as Third Party Service Providers Under the Rule.

The NPRM asks whether advertising and analytics providers should be considered third party service providers under the HBNR "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. . . ."[31] This threatens to substantially expand and confuse regulatory burdens for a variety of third

---

[28] *Id.* at 37,826.

[29] *Id.* at 37,835, Proposed Rule § 318.2(h).

[30] *See id.* at 37,826 ("For example, an app might have the technical capacity to draw information from multiple sources, but its API is entirely or mostly unused, either because it remains a Beta feature, has not been publicized, or is not popular.").

[31] *Id.* at 37,831.

parties, with a variety of unintended consequences. As a result, CTA encourages the Commission to not expand the Rule to encompass advertising, analytics, *or* cloud service providers. At a minimum, to the extent the Rule is expanded, the Commission should exclude service providers that contractually prohibit their vendors or PHR related entities from sharing PHR identifiable health information.

Expanding the definition of third party service provider to include advertising, analytics, and cloud service providers and platforms would place onerous, if not practically impossible, investigation and notification obligations on varied companies that do not knowingly seek out, deal with, or exercise any measure of control over, conventional health care data.[32] For one, the Rule could be interpreted as requiring third party service providers to investigate on an ongoing and exhaustive basis whether "PHR identifiable health information" – which the Rule defines extremely broadly – had been received. That level of information examination would impose exorbitant operational costs and potentially infeasible technical challenges, while potentially creating new privacy risks or incompatible contractual obligations between business partners. Advertising, analytics, and cloud service providers and platforms often receive data from thousands or millions of third parties, and they may not have the resources – or technical capability – to actively monitor, audit, and analyze the granular data that they receive to determine whether PHR identifiable health information has been received. The Rule would also place the burden on the advertising, analytics, and cloud providers and platforms to determine whether, assuming PHR identifiable health information had been received, that receipt was

[32] *Id.* at 37,835, Proposed Rule § 318.2(l). The FTC has interpreted the term "PHR identifiable health information" exceptionally broadly to include, for example, URLs that simply reference specific health conditions. *Id.* at 37,835, Proposed Rule § 318.2(l); *see also* Complaint for Permanent Injunction, Civil Penalties, and Other Civil Relief ¶ 111, *United States v. GoodRx Holdings, Inc.*, No. 4:23-cv-460 (N.D. Cal. Feb. 1, 2023), ECF No. 1.

without authorization, such that it constitutes a breach of security – and addressing such risks could require businesses to collect even more information from consumers. But in most instances, it will be the vendor or the PHR related entity—not the third party service provider—that will know whether authorization exists. Together, these infeasible obligations would substantially impair the abilities of advertising, analytics, and cloud service providers and platforms to provide their services to small and large businesses alike.[33]

In the event the Commission nonetheless extends the definition of third party service providers to include advertising, analytics, and cloud service providers and platforms, it should at a minimum establish a safe harbor for providers that contractually limit their customers, vendors or business partners from sharing PHR identifiable health information with them. This safe harbor would incentivize contractual accountability mechanisms addressing the parties that collect and share such information and are best positioned for compliance.

III. THE FTC SHOULD NARROW ITS APPROACH TO "BREACH OF SECURITY."

The NPRM also seeks comment on the scope of its proposed "breach of security" definition.[34] The NPRM specifically proposes to amend "breach of security" to add the following sentence at the end of the definition: "A breach of security includes an unauthorized acquisition of unsecured PHR identifiable health information in a personal health record that

[33] *See id.* at 37,834-35, Proposed Rule § 318.2(a).

[34] *Id.* at 37,824, 37,834-35, Proposed Rule § 318.2(a); 16 C.F.R. § 318.2(a) ("Breach of security means, 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. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.") (emphasis removed).

occurs as a result of a data breach or an unauthorized disclosure."[35] That greatly expands the definition of a breach in connection with the provision that "[u]nauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information." In doing so, the NPRM's "breach of security" proposal threatens to sweep in *any* unauthorized access, including accidental access by employees that does not result in the exfiltration of unsecured health data or any potential consumer harm. If adopted, this definition will result in compliance confusion, overreporting, and consumer notice fatigue. These risks are all exacerbated given the many other regulatory initiatives across the federal government on cybersecurity reporting and harmonization, which is a priority for this Administration and Congress.[36] The Commission should therefore cabin the NPRM's "breach of security" definition.

A. A "Breach of Security" Should Be Limited to an Actual Acquisition of Protected Health Data.

The definition of "breach of security" in the HITECH Act is far more targeted than the NPRM's proposal, defining the term as "with respect to unsecured PHR identifiable health information of an individual in a personal health record, ***acquisition*** of such information without

[35] NPRM at 37,824, 37,834-35, Proposed Rule § 318.2(a).

[36] *See e.g.*, Request For Information On Cybersecurity Regulatory Harmonization, Office of the National Cyber Director, Executive Office of the President (July 19, 2023), https://www.whitehouse.gov/wp-content/uploads/2023/07/ONCD-Reg-Harm-RFI-Final-July-19.2023.pdf; *Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022*, Request of Information , 87 Fed. Reg. 55,833 (Sept. 12, 2022); Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, Div. Y, 136 Stat. 1038, 1038-1059 (2022) (codified at 6 U.S.C. 681f) (creating the Cyber Incident Reporting Council to harmonize reporting requirements).

the authorization of the individual."[37] That is, the HITECH Act limits a "breach of security" to actual ***acquisition***, not access to or disclosure of covered data without actual acquisition by a third party. Indeed, a separate provision of the HITECH Act, outside of the HBNR provisions, defines a different kind of "breach" as "unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information. . . ."[38]

Not only would a broad "breach of security" definition that covers "access" be inconsistent with the HITECH Act, it would result in overreporting of security incidents with no marginal benefit to consumers. Companies may believe that covered data was potentially accessed but not acquired, but overreport out of abundance of caution. This will cause consumer confusion, because there are no actionable steps for consumers if their data was not actually acquired by a third party without authorization. It also will inundate the FTC with reports of more routine events without clear consumer injury, such as employees inadvertently exceeding their authorization and potentially being able to access covered data, but without evidence that they viewed, used, or acquired the data in any way. Such a broad definition will divert companies' data security personnel and resources.

---

[37] 42 U.S.C. § 17937(f)(1) (emphasis added).

[38] *Id.* § 17921(1)(A) (emphasis added); *see also* Dissenting Statement of Commissioner Noah Joshua Phillips, Regarding the Policy Statement on Breaches by Health Apps and Other Connected Devices, FTC, at 3 (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596328/hbnr_dissent_final_formatted.pdf ("But the 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 for 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.") (emphasis removed).

A broad "breach of security" definition would also go beyond the HIPAA Breach Notification Rule requirements. The HIPAA Breach Notification Rule excludes from its definition of "breach" any "inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, . . . and the information received as a result of such disclosure is not further used or disclosed. . . ."[39] It also excludes "[a]ny unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure. . . ."[40] In this way, the HIPAA Breach Notification appropriately recognizes that low-risk access events should not rise to the level of being reportable events.

The NPRM separately asks whether the Commission should define the term "authorization" within the definition to mean "affirmative express consent," consistent with the California Consumer Privacy Rights Act ("CPRA").[41] CTA urges the agency to refrain from defining "authorization" as requiring affirmative express consent, as doing so would dramatically expand the scope of "unauthorized" acquisition to encompass data sharing that does not meet CPRA requirements – which is not required by law in most jurisdictions. Doing so would effectively require covered entities to obtain a specific kind consent from an individual when dealing with covered health data. This is well beyond the purview of the HBNR, which is meant

[39] 45 C.F.R. § 164.402(1)(ii).

[40] *Id.* § 164.402(1)(i).

[41] NPRM at 37,824, 37,830; Cal. Civ. Code 1798.140(h).

as a breach notification rule, not one that allows the FTC to impose substantive consent requirements. It also would be extremely burdensome, and likely not administrable for many companies. Instead, the FTC should find "authorization" for sharing to be satisfied if done consistent with a company's privacy policy or terms and conditions, or when a consumer agrees to opt-in to certain data sharing, such as by clicking a box proximate to a disclosure of material terms.

B. The Commission Should Include Common Exceptions In the Rule's "Breach of Security" Definition.

CTA encourages the Commission to incorporate explicit exceptions into the NPRM's proposed "breach of security" definition, to ensure that its implementation is practical, and promote harmonization with the HIPAA Breach Notification Rule and applicable state privacy laws. These exceptions would make clear that certain activities are not reportable "breaches of security." Each of these is well recognized as a permissible purpose for data sharing and making them explicit will assist with compliance. The FTC should specifically include exceptions for access to PHR identifiable health information –

- Involving an inadvertent disclosure by a person authorized to access unsecured PHR identifiable health information to another person authorized to access the unsecured PHR identifiable health information, and no further disclosure occurs;[42]
- Involving unintentional acquisition or access by an employee in good faith and within the scope of their authority and additional disclosure does not occur;[43]
- To permit sharing between personnel within a company for a business purpose;

[42] 42 U.S.C. § 17921(1)(B)(ii).

[43] *Id.* § 17921(1)(B)(i).

- To detect and prevent security incidents, identity theft, fraud, harassment, or malicious, deceptive, or illegal activity; preserve the security or integrity of systems or to prosecute responsible individuals for such actions;[44]

- To comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by authorities;[45]

- To cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and good faith believes may be illegal;[46]

- To perform internal operations consistent with the consumer's expectations;[47]

- To provide a product or service a consumer requested or perform a contract with the consumer;[48]

- To protect the vital interests of consumers;[49] and

- To process personal data for reasons of public interest in the area of public health, subject to certain conditions.[50]

Incorporating these exceptions will enhance regulatory certainty for companies covered by both the Rule and state privacy laws and provide safe harbors for disclosures that are unlikely to result in consumer harm.

[44] Cal. Code Regs. Tit. 11, § 7027(m)(2)-(3); Va. Code Ann. § 59.1-582(A)(7); Colo. Rev. Stat. § 6-1-1304(3)(a)(X).

[45] Va. Code Ann. § 59.1-582(A)(2); Colo. Rev. Stat. § 6-1-1304(3)(a)(II).

[46] Va. Code Ann. § 59.1-582(A)(3); Colo. Rev. Stat. § 6-1-1304(3)(a)(III).

[47] Cal. Code Regs. Tit. 11, § 7027(m)(6); Colo. Rev. Stat. § 6-1-1304(3)(a)(VII).

[48] Va. Code Ann. § 59.1-582(A)(5); Cal. Code Regs. Tit. 11, § 7027(m)(1); Colo. Rev. Stat. § 6-1-1304(3)(a)(VIII).

[49] Cal. Code Regs. Tit. 11, § 7027(m)(4); Va. Code Ann. § 59.1-582(A)6; Colo. Rev. Stat. § 6-1-1304(3)(a)(IX).

[50] Va. Code Ann. § 59.1-582(A)(8); Colo. Rev. Stat. § 6-1-1304(3)(a)(XI).

IV. THE FTC SHOULD NOT PRESCRIBE ARBITRARY REPORTING TIMELINES FOR BREACH NOTICES AND SHOULD ADOPT A REASONABLE DETERMINATION TRIGGER.

CTA encourages the FTC to adopt a "reasonable determination" HBNR notification trigger to give entities time to ascertain the scope and gravity of a data security incident. In any event, given the Commission's generally broad view of a "breach of security," the NPRM's ten business-day breach of security notification timeline to the FTC (for incidents impacting 500 or more consumers) is exceedingly short, and threatens to divert critical resources from company efforts to investigate new incidents. The FTC should instead take a risk-based approach that distinguishes between, for example, incidents perpetrated by criminal hackers with malicious intent, and incidents involving inadvertent activities by employees that are ultimately contained.

The NPRM does not propose any revisions to the HBNR notification timing requirements, but asks "whether it should extend the timeline to give entities more time to investigate breaches and better ascertain the number of affected individuals. . . ."[51] CTA encourages the Commission to give entities time to fully investigate breaches to ascertain their scope before making notifications, abandon prescriptive and arbitrary reporting timelines, and reject the HBNR's strict "discovery" notification trigger in favor of a trigger based on when a company makes a "reasonable determination" of a breach. This would give covered entities the needed time to evaluate security incidents that are often complex, fluid, and ongoing. This is especially true given the NPRM's rigid proposal requiring notification to media; a prescriptive reporting timeline based on the discovery of a potential incident risks spreading misinformation and alarm.[52] A "reasonable determination" trigger will instead increase harmonization with state

[51] NPRM at 37,831.

[52] *Id.* at 37,836, Proposed Rule § 318.3(a)(3).

breach reporting laws, and allow companies to investigate the gravity and extent of a potential security incident before notifying consumers.[53]

The NPRM also proposes far stricter breach of security reporting deadlines for notifications to the FTC than are currently required under the HIPAA Breach Reporting Rule, which requires covered entities to notify HHS within 60 calendar days of the discovery of the breach if it impacts 500 or more individuals.[54] Proposed Rule 318.4(b) in the NPRM, however, would require that all breaches of security involving the unsecured PHR identifiable health information of 500 or more individuals "be provided as soon as possible and in no case later than ten business days following the date of discovery of the breach."[55] This ten-business day timeline is far too short, and would divert important company resources from investigating potential incidents.[56] While the Federal Communications Commission ("FCC") similarly has a seven-business day reporting timeline for notifications to the Federal Bureau of Investigation ("FBI") and U.S. Secret Service ("USSS") for breaches impacting customer proprietary network

[53] See e.g., Ala. Code § 8-38-5(b) ("[T]he covered entity shall provide notice within 45 days of the covered entity's receipt of notice from a third-party agent that a breach has occurred or upon the covered entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates."); Ariz. Rev. Stat. § 18-552(B) ("If the investigation results in a determination that there has been a security system breach, the person that owns or licenses the computerized data . . . shall" notify the necessary individuals, agencies, and authorities.); Colo. Rev. Stat. Ann. § 6-1-716(2)(a) ("Notice must be made . . . not later than thirty days after the date of determination that a security breach occurred. . . ."); R.I. Gen. Laws § 11-49.3-4(a)(2) ("The notification shall be made in the most expedient time possible, but no later than forty-five (45) calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements. . . .").

[54] 16 C.F.R. § 318.5(c); 45 C.F.R. § 164.408(c).

[55] NPRM at 37,836, Proposed Rule § 318.4(b).

[56] *Id.* at 37,831.

information, that timeline is still based on when the telecommunications carrier has made a "reasonable determination" that a breach has occurred.[57]

In any case, the Commission should take a risk-based approach when setting reporting periods, focusing on the scope of the incident and the level of likely consumer financial and/or identity theft harms. In connection with a reasonable determination trigger, the agency may create relatively shorter notification timelines for higher-risk incidents – for example, those that involve the exfiltration of PHR identifiable health information by a criminal actor. For incidents involving accidental disclosures or rogue employees whose unauthorized efforts are thwarted before data is exfiltrated from a company, however, longer timelines for notification – or even no notifications – may be appropriate, as this information would be of little to no use to consumers, and would be less useful to the FTC than notices about ongoing threats to consumer personal information.

V. THE FTC SHOULD SIMPLIFY THE RULE'S NOTICE PROCEDURES.

The FTC should further simplify the NPRM's rule regarding notifications, and only require one form of notice to consumers. The Commission should also simplify its proposed notice content requirements, which will unnecessarily create consumer confusion if adopted. In doing so, the FTC should either remove or revise the exemplar notices provided in Appendix A of the NPRM to delete descriptions of potential consumer harm and contact information for third parties that acquired unsecured PHR identifiable health information.

A. The NPRM's Email Notification Proposal Should Be Simplified.

While CTA welcomes the FTC's inclusion of email notifications as a positive step that will make such notices less likely to be ignored or missed, the agency should take measures to

[57] 47 C.F.R. § 64.2011(b).

simplify the definition of "electronic mail" in the proposal.[58] The NPRM would define "electronic mail" as "(1) email in combination with one or more of the following: (2) text message, within- application messaging, or electronic banner."[59] CTA cautions, however, that defining "electronic mail" to require multiple forms of notification could result in over-notification, and ultimately notice fatigue that may lessen the perceived importance of the message. It could also incentivize the over-collection of consumer personal information, as a company might collect more data than it otherwise would have to meet the NPRM's "electronic mail" notification definition. Requiring two methods of notification, as Proposed Rule 318.2(d) would require, is also a more stringent requirement than in existing data breach notification regimes, including the HIPAA Breach Notification Rule[60] and Europe's General Data Protection Regulation, the latter of which notes that covered entities "are best placed to determine the most appropriate contact channel to communicate a breach to individuals, particularly if they interact with their customers on a frequent basis."[61]

[58] NPRM at 37,827.

[59] *Id.* at 37,835, Proposed Rule § 318.2(d).

[60] 45 C.F.R. § 164.404(d).

[61] *See* European Data Protection Board, Guidelines 9/2022 on personal data breach notification under GDPR, Version 2.0, European Data Protection Board, ¶¶ 90, 92 (Mar. 28, 2023), https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf ("Examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual. The [European Data Protection Board ("EDPB")] recommends that controllers should choose a means that maximizes the chance of properly communicating information to all affected individuals.").

Proposed Rule 318.5(a)(1) would also require companies to obtain consumer consent prior to providing notice via electronic mail.[62] CTA encourages the FTC to facilitate streamlined and effective notices by allowing covered entities to notify a consumer by email of a breach of security if the company regularly communicates with the consumer via email. Simplifying the email notification proposal will help ensure that consumers receive critical information about incidents impacting their personal information in a timely and efficient manner, and through the channel that they expect to receive communications from the affected entity.

B. The NPRM's Consumer Notice Requirements Should Not Include an Explanation of Potential Harms or a List of the Third Parties That Obtained a Consumer's Information.

CTA cautions the FTC against requiring covered entities to describe theoretical harms related to a breach in a HBNR notice or to list the third parties that obtained a consumer's information. Doing so will cause consumer confusion and will require companies to provide consumers with information that is not actionable. The Commission should also remove or revise the exemplar notices to delete references to theoretical harms or lists of third parties that obtained consumer PHR identifiable health information.

The NPRM proposes adding obligations that notices to consumers (1) "include a brief description of the potential harm that may result from the breach"[63] and (2) "include the full name, website, and contact information (such as a public email address or phone number) of any third parties that acquired unsecured PHR identifiable health information as a result of a breach of security."[64] The Commission should reject these proposals for a number of reasons.

---

[62] *See* NPRM at 37,836, Proposed Rule § 318.5(a)(1) ("Written notice may be sent by electronic mail if the individual has specified electronic mail as the primary method of communication.").

[63] *Id.* at 37,837, Proposed Rule § 318.6(a).

[64] *Id.*

First, requiring an explanation of potential, speculative harm will create consumer confusion, further misinformation, and encourage unnecessary litigation. A company that recently experienced a data security incident – especially a large-scale incident – will not immediately know if the compromised information will be used for nefarious purposes, but the notice requirement may require it to speculate about the effects.

Second, requiring companies to list third parties that obtained a consumer's PHR identifiable health information may interfere with investigatory efforts, including law enforcement inquiries or other internal investigations.

Third, requiring companies to list the third parties that obtained a consumer's PHR identifiable health information, without more context, will invite litigation against these entities as it presumes that the third parties intentionally acquired the information without authorization. At a minimum, if the third parties did not intend to receive a consumer's PHR identifiable health information, the notice must state that.

Fourth, neither the description of potential, speculative harm nor the list of third parties that obtained the consumer's PHR identifiable health information constitutes actionable information that the consumer can use to protect themselves from financial harm and/or identity theft. Instead, this information may only serve to alarm and confuse consumers.

The HIPAA Breach Notification Rule also does not include either of these requirements.[65] For all these reasons, the FTC should (1) reject these two proposals; and (2) either delete or revise the exemplars provided in Appendix A of the NPRM to remove reference to these requirements.

[65] 45 C.F.R. § 164.404(c).

VI. CONCLUSION.

While CTA shares the Commission's commitment to protecting sensitive consumer health data, the NPRM would, if adopted, dramatically expand the breadth of the HBNR into a wide breach reporting rule with impacts throughout the economy – which Congress did not envision for the HBNR when it passed the HITECH Act. The Commission should not take this overly expansive approach.

Respectfully submitted,

By: */s/ René Quashie*
René Quashie
Vice President, Digital Health

/s/ Rachel Nemeth
Rachel Nemeth
Senior Director, Regulatory Affairs

Consumer Technology Association
1919 S. Eads Street
Arlington, VA 22202
(703) 907-7651

August 8, 2023