



August 8, 2023

Chair Lina M. Khan
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW,
Suite CC-5610 (Annex H)
Washington DC 20580

RE: Health Breach Notification Rule: Notice of Proposed Rulemaking and Request for Public Comment, Project No. P205405

Dear Chair Khan:

The Confidentiality Coalition appreciates the opportunity to provide comments to the Federal Trade Commission (Commission or FTC) on the Health Breach Notification Rule: Notice of Proposed Rulemaking and Request for Public Comment (proposed Rule or NPRM).¹

The [Confidentiality Coalition](#) is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, and others, committed to advancing effective health information privacy and security protections. Our mission is to advocate policies and practices that safeguard the privacy and security of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

I. General Comments

The Confidentiality Coalition strongly supports the proposed amendments to clarify that the Health Breach Notification Rule (Rule) applies not only to websites, but also to mobile apps, online services, and similar technologies. As the Commission notes, apps, and other direct-to-consumer health technologies, such as fitness trackers and wearable blood pressure monitors, have proliferated since the initial issuance of the Rule, and consumer use of these apps has grown even more since the COVID-19

¹ 88 Fed. Reg. at 37819 (June 9, 2023).

pandemic. When Congress included the breach notification requirement in Section 13407 of the HITECH Act it clearly meant to capture all entities offering personal health records (PHRs) or products and services through PHR websites or similar technologies that were not subject to the privacy and security requirements of HIPAA. It is therefore appropriate and timely for the FTC to update the Rule to recognize and consider the technological changes that have occurred in the almost decade and a half since the HITECH Act became law. The Coalition has also long supported the enactment of broader privacy and security protections for all health information that falls outside the purview of HIPAA, and has advocated for a robust, national privacy law. We continue to work with Congress and government agencies to bring that about, but until that occurs, the Rule should at a minimum cover the types of data and entities intended to be covered by Congress when it enacted the health breach notification requirement, and irrespective of the exact technology used.

II. Specific Comments

1. Clarification of Entities Covered

a. PHR Identifiable Information

The proposed Rule revises and creates several definitions to clarify that mobile health apps and similar technologies not covered by HIPAA are covered by the Health Breach Notification Rule (Rule). First, the Commission revises the definition of “PHR identifiable information” consistent with the definition of “individually identifiable health information” (IIHI) in section 1171(6) of the Social Security Act, stating that this definition is intended to cover traditional health information (such as diagnoses or medications), health information derived from consumers’ interactions with apps and other online services (such as health information generated from tracking technologies employed on websites or mobile applications, as well as emergent health data (such as health information inferred from non-health related data points, such as location and recent purchases). The Commission requests comment as to whether any further amendment of the definition is needed to clarify the scope of data covered.

We support the revised definition and agree that it should encompass not only traditional health data, but also health data generated from health apps and health data that can be inferred from non-health related data points, such as location and recent purchases. We caution, however, that consistent with the definition of IIHI in the statute and the HIPAA Privacy Rule, the data must be “individually identifiable” i.e., there must be a “reasonable basis to believe that the information can be used to identify an individual.”

The Commission made this point in the preamble to the 2009 Rule, stating (emphasis added):

Even if a particular data set is not “deidentified,”² however, entities still may be able to show, in specific instances, that there is no reasonable basis to identify individuals whose data has been breached, and thus, no need to send breach notices. For example, consider a Web site that helps consumers manage their medications. The Web site collects only email addresses, city, and medication information from consumers, but it keeps email addresses secured in accordance with HHS standards and on a separate server. It experiences a breach of the server containing the city and medication information (but no email addresses). A hacker obtains medication information associated with ten anonymous individuals, who live in New York City. In this situation, the Web site could show that, even though a city is revealed, thus preventing the data from being categorized as “deidentified,” there is no reasonable basis for identifying the individuals, and no breach notification needs to be provided.³

The Department of Health and Human Services Office for Civil Rights (OCR) has also recently addressed this issue, noting:

There are limited situations in which an IP address or geographic location by itself may not be PHI, such as where the individual uses a computer at a public library instead of using their personal electronic device. This is because the IP address or geographic location will not be related to the individual when using a public device. However, even in such cases, the IP address or geographic location from such devices, combined with any information provided by users through a webpage or mobile app, could be used to identify the individual and therefore may be PHI.⁴

Given the importance of the distinction between individually identifiable data and non-individually identifiable data for regulatory compliance, we urge the FTC to provide clear guidance, including examples of common scenarios, on when data fields that are not in themselves direct identifiers will be regarded as reasonably capable of identifying an individual and when this would not be the case.

b. Health Care Provider

The FTC seeks comment on defining “health care provider” in a manner that is broader than a more limited definition of that term used in other contexts (e.g., referring primarily to persons and entities such as doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies. The Coalition supports the broader definition of the term “health care provider” for purposes of the Rule since it appropriately recognizes

² Presumably, the Commission is referring here to the de-identification safe harbor method only, since if a statistical determined that there was no reasonable basis for identifying the individuals in accordance with 45 CFR 164.514(b)(1), the data would have qualified as de-identified even with the city revealed.

³ 74 Fed. Reg. 42969 (August 25, 2009)

⁴ See OCR Guidance “[Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates](#),” December 1, 2022, footnote 21.

that health care apps and similar technologies are furnishing health care services, even though these are not provided by health care professionals or in traditional healthcare settings. As long as consumers are sharing data involving their health with health apps for purposes of obtaining services or supplies related to their health, the purveyors of these supplies and services should be classified as health care providers to ensure that the data collected and generated by them is covered by the Rule.

c. Healthcare Services or Supplies

The proposed Rule creates a definition for the term “healthcare services or supplies” that includes any online service, such as a website, mobile application, or internet-connected device that provides mechanisms to track diseases, health conditions, diagnoses or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet, or that provides other health-related services or tools. The Commission states that this definition is intended to make clear that the Rule applies to online services and that it applies not only to medical issues, but also wellness issues. We appreciate and support both of these clarifications, since all online technologies providing health services or supplies should be covered by the Rule, whether in the form of websites, mobile apps, or other technologies, and both medical and wellness issues are unquestionably health issues.

Recommendations:

- ***We support the new and revised definitions to make clear that all health apps that fall outside HIPAA are covered by the Rule, whether they provide medical or wellness services, and irrespective of whether the services are provided by traditional health care professionals.***
- ***We ask that the Commission make clear that only “individually identifiable” health information is covered by the Rule, and that it provide clear guidance and specific examples on when there is a reasonable basis to believe that certain data fields could be used to identify an individual, and thus would be considered individually identifiable.***

2. Clarification Regarding Types of Breaches Subject to the Rule

The Commission proposes to revise the definition of “breach of security” to clarify that a breach includes an unauthorized acquisition of identifiable health information that occurs as a result of a data breach or an unauthorized disclosure, such as a voluntary disclosure made by the PHR vendor or PHR related entity where such disclosure was not authorized by the consumer. We support this clarification and agree that a breach of security should not be limited to involuntary unauthorized acquisitions, but should also encompass voluntary disclosures, such as to third parties, where this is unauthorized.

However, we ask that the Commission make clear that an “unauthorized” disclosure is one that an individual is not clearly made aware of in an entity’s privacy notice or is otherwise not permissible under applicable state privacy laws, whether this is in the form of an affirmative express consent, a right to opt out or appropriate disclosure in an

entity's privacy notice. Adopting a new substantive privacy standard of "affirmative express consent" is beyond the jurisdiction of the Commission and would create yet another privacy framework for affected entities to have to comply with layered over the growing number of comprehensive state privacy laws. In addition, as the Commission has itself noted,⁵ consents may not be the most effective or consumer-friendly mechanism for ensuring that personal information is used and disclosed in a manner consistent with consumers' reasonable expectations. While we strongly support clear and robust privacy standards for personal health information, these standards should be established by Congress in comprehensive privacy legislation that addresses all aspects of the collection, use and disclosure of personal health information and for all non-HIPAA entities. This legislation should supersede state privacy laws so that all entities are held to a single, strong national standard for the protection of personal health information that falls outside HIPAA.

Finally, if the Commission redefines a "breach" to include unauthorized voluntary disclosures, regulated entities will need time to bring their existing practices fully into compliance with this change. This may include updating their privacy notices, policies and procedures, and contractual arrangements with third-party service providers.

Recommendations:

- **We support the revision to the definition of "breach of security" to make clear that it includes voluntary unauthorized disclosures as well as involuntary unauthorized disclosures.**
- **We ask that the Commission clarify that an "unauthorized" disclosure is one where the individual is not clearly made aware of the disclosure in an entity's privacy notice, or the disclosure is otherwise not permissible under applicable state privacy laws.**
- **The Commission should offer technical guidance and sufficient time for PHR vendors and PHR related entities to come to compliance with the operational and contractual changes that may be required as a result of this expansion of what constitutes a breach of security under the Rule.**

3. Revised Scope of PHR Related Entity

The Commission proposes to revise the definition of "PHR related entity" to clarify that PHR related entities include entities offering products and services not only through the websites of vendors of personal health records, but also through any online service, including mobile applications. It also proposes to add language to the definition of "third party service provider" to make clear that an entity is not rendered a PHR related entity when it accesses unsecured PHR identifiable health information in the course of providing services.

⁵ See the Commission's Advance Notice of Proposed Rulemaking on Commercial Surveillance and Data Security, where the Commission stated "[T]he permissions that consumers give may not always be meaningful or informed." 77 Fed. Reg. at 51274 (August 22, 2022). The Commission also asked a series of questions about the effectiveness and administrability of consumer consents. See 87 Fed. Reg. at 51284.

We support both of these changes. On the first, we agree that the broadened scope of the definition is necessary to reflect the reality that websites are no longer the only means through which consumers access health information online. On the second, we agree that the change is necessary to avoid third party service providers also falling under the definition of “PHR related entity,” thereby potentially creating duplicate notification requirements. This would be confusing to consumers and provide no additional benefits. We also agree that by ensuring that such entities remain third party service providers, it will hold PHR vendors and PHR related entities accountable for their conduct, and thereby create incentives for responsible data stewardship and, where practicable, data de-identification.

Recommendation: We support the proposed changes to the definition of a “PHR related entity” to make clear that it covers mobile apps and similar technologies, and the clarification to the definition of “third party service provider” to ensure that such entities do not also fall under the definition of “PHR related entity.”

4. Clarification of What it Means for a Personal Health Record to Draw Information from Multiple Sources

The Commission proposes to revise the definition of “personal health record” to make clear that a product is a personal health record *if* it can draw information from multiple sources, even if the consumer elects to limit information from a single source only, in a particular instance. We support this change, since whether an app qualifies as a personal health record should not depend on the prevalence of consumers’ use of a particular app feature, like sleep monitor-syncing. We also believe it is appropriate to treat an app as a personal health record if it is capable of drawing health information from at least one source as long as, consistent with the statutory definition, it is capable of drawing other information from another source. It would create a significant loophole if health apps such as the diet and fitness app that has the ability to pull information from the user’s phone calendar to suggest personalized healthy eating options based on the user’s identifiable health information (such as weight, height, age) did not fall under the Rule simply because it draws health information from only one source.

Recommendation: We support the changes to the definition of “personal health record to clarify that it does not depend on whether a user enables a feature, and to ensure that all health apps envisioned by Congress are covered by the Rule.

5. Facilitating Greater Opportunity for Electronic Notice

a. Notice Via Electronic Mail

The Commission proposes to authorize expanded use of email and other electronic means of providing notice of a breach to consumers by allowing written notice to be sent by electronic mail if an individual has specified electronic mail as the primary contact method. We support this change, which will not only be less burdensome and costly, but will usually also be much quicker and more likely to reach the consumer. Consumers may have several addresses or spend time in different physical locations, with email or other electronic notice the most reliable and efficient way to reach them.

We also support the Commission's interpretation of the new language as allowing entities to send an email or in-app alert notifying their users that they will receive breach notices by electronic mail and offering them the opportunity to opt out of electronic mail notification and instead receive notice by first class mail. We encourage the Commission to make this opt out option clear in the regulatory text itself.

b. Model Notice

The Commission has developed a model notice that entities may use, in their discretion, to notify individuals. We appreciate the Commission providing a model notice and agree that it will help entities required to provide notice of breaches of security under the Rule. We support allowing entities to decide whether to use the model, since this allows greater flexibility to address circumstances that may not be foreseeable.

c. Expanded Content of Notice

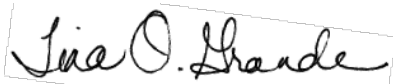
The Commission proposed several additions to the content requirements of the notice, including a brief description of the potential harm that may result from the breach, such as medical or other identity theft. While we understand that the intent of this change is to help individuals better understand the potential risks and determine what steps to take, we are concerned that informing consumers of potential harms that may not occur is more likely to alarm and confuse consumers than aid them. Potential harm is speculative and uncertain in comparison to known actionable harm. The Commission also proposes to require the notice to 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, if this information is known. The Commission does not explain the reason for this change, but presumably to allow consumers to contact the third party to ask that the data be deleted or returned in the case of voluntary unauthorized disclosures. However, it is not clear what the purpose would be in the case of involuntary disclosures, such as to malicious actors or hackers. (These entities would not be responsive to customers and PHR vendors and PHR related entities are unlikely to have such contact information.) In addition, in the case of inadvertent or unintentional disclosures to individuals, this could create privacy concerns for the recipients, who had no control over the disclosures made to them. As such, we encourage the Commission to allow, but not require, this information in the case of involuntary unauthorized disclosures. Finally, the Commission would require the entity to provide a brief description of what it is doing to protect affected individuals, such as offering credit monitoring or other services. We believe this is already encompassed by the requirement to describe what mitigation steps the entity is taking and will depend on the nature of the breach and the information involved. We recommend that the Commission reconsider the need for this additional requirement, since it could result in duplicative information being provided in the notice, whereas the more concise and to the point the notice is, the better for consumers.

Recommendations:

- ***We support the expanded ability to provide electronic notice, which will be more cost effective and, in many cases, reach consumers more quickly and reliably.***
- ***We appreciate the Commission's provision of a model notice that entities may use but believe use of the model should remain voluntary to provide greater flexibility for customization.***
- ***We support some of the expanded content requirements but ask that the Commission consider whether certain additional requirements, such as describing potential harms, are truly beneficial to consumers or more likely to cause confusion.***

Thank you for your consideration of our comments. Please do not hesitate to contact me at tgrande@hlc.org or 202-449-3433 if you have any questions.

Sincerely,

A handwritten signature in cursive script that reads "Tina O. Grande". The signature is written in black ink on a white background and is enclosed in a thin black rectangular border.

Tina O. Grande
Chair, Confidentiality Coalition and
Executive VP, Policy, Healthcare Leadership Council

2023 CONFIDENTIALITY COALITION MEMBERS



AdventHealth

Advocate Health

American Health Information Management Assoc.

America's Health Insurance Plans

American Hospital Association

American Pharmacists Association

American Society for Radiation Oncology

AmerisourceBergen

Amgen

AMN Healthcare

Anthem

Ascension

Association of American Medical Colleges

Association of Clinical Research Organizations

Augmedix

Bassett Healthcare Network

Baxter

Blue Cross Blue Shield Association

Blue Cross Blue Shield of North Carolina

Bristol Myers Squibb

Cardinal Health

CHIME

Cigna

City of Hope

College of American Pathologists

Connective Rx

2023 CONFIDENTIALITY COALITION MEMBERS



Cotiviti

CVS Health

Elevance Health

EMD Serono

Epic

Fairview Health Services

Federation of American Hospitals

Ferring Pharmaceuticals

Genentech

Genetic Alliance

Guardant Health

Healthcare Leadership Council

Intermountain Healthcare

IQVIA

Johnson & Johnson

Kaiser Permanente

Leidos

LifeScience Logistics

Marshfield Clinic Health System

Mayo Clinic

McKesson Corporation

Medical Group Management Association

Meharry Medical College

MemorialCare Health System

Merck

MetLife

2023 CONFIDENTIALITY COALITION MEMBERS



Mount Sinai Health System

MRO

National Association of Chain Drug Stores

National Community Pharmacists

NewYork-Presbyterian Hospital

NorthShore University HealthSystem

Novartis Pharmaceuticals

Optum Insight

Oracle Health

Pfizer

Pharmaceutical Care Management Association

Premier

Roots Food Group

SCAN Health Plan

Senior Helpers

State Farm

Stryker

Surescripts

Texas Health Resources

Tivity Health

United Health Group

Vizient

Wellvana Health

Workgroup for Electronic Data Interchange

ZS Associates