INFORMATICS PROFESSIONALS. LEADING THE WAY.

August 1, 2023

April Tabor
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Ste CC-5610 (Annex H)
Washington, DC 20580

Re: 6750-01-P Health Breach Notification Rule, Project No. P205405

Submitted electronically at regulations.gov.

Dear Secretary Tabor:

The American Medical Informatics Association (AMIA) appreciates the opportunity to submit comments regarding the proposed amendments to the Federal Trade Commission's (FTC) Health Breach Notification Rule (HBNR) Request for Comment (RFC).

AMIA is the professional home for more than 5,500 informatics professionals, representing frontline clinicians, researchers, public health experts, and educators who bring meaning to data, manage information, and generate new knowledge across the research and healthcare enterprise. As the voice of the nation's biomedical and health informatics professionals, AMIA plays a leading role in advancing health and wellness by moving basic research findings from bench to bedside, and evaluating interventions, innovations and public policy across care settings and patient populations.

In 2020, AMIA submitted comments to the FTC's regular 10-year review of the HBNR. AMIA made recommendations to FTC and FTC addressed them as follows:

- Near-term
    - Explicitly includes usernames / passwords maintained by non-HIPAA covered entities (NCE) as being considered personal health record (PHR) identifiable health information, thus subject to the HBNR if breached.
        - *FTC did not address this in the current proposed rule.*
    - Expand on the concept of "unauthorized access" under the definition of "Breach of security," to be presumed when a PHR or PHR related entity fails to adequately disclose to individuals how user data is accessed, processed, used, reused, and disclosed.
        - *FTC addresses this in the second proposed amendment in this proposed rule.*

- Long-term, which FTC has largely addressed in this proposed rule
    - Expand the purview of the HBNR to include technology beyond PHRs, including technology described by ONC in its 2016 report on NCEs, such as mHealth and health social media;

- Ensure uniformity in applying the HBN Rule so that all NCEs that generate health data are subject to the Rule's provisions, not just PHRs;
- Expand and promote reporting pathways to affected individuals, not simply firms who notice a breach;
  - *We emphasize to FTC that a simple pathway for individuals to report to the FTC is imperative.*
- Ensure the HBNR acts as a deterrent to poor data management and security practices through enforcement that is sufficiently stringent and appropriate to compel secure/responsible management of health data;
- Ensure alignment with the European General Data Protection Rule, the California Consumer Protection Act, and other relevant consumer data privacy policy.

Thank you for accepting several of AMIA's past suggestions in our 2020 letter to FTC. We appreciate FTC's leadership and awareness of the rapidly changing digital health landscape with the rise of clinically and consumer directed health apps, wearable technology, and the increased use of telehealth.

Generally, AMIA encourages FTC to ensure that HBNR and HIPAA are aligned such that there are no gaps in regulation over the covered entities and other non-covered entities that work with PHR; to align definitions with other agencies, including the definition of PHR; and to provide clarity around whether a non-health data source is being used in a health context and qualifies for coverage under the HBNR. AMIA also strongly encourages interagency coordination on such issues, particularly regarding standardizing definitions of terms and processes of addressing breaches.

I. Clarification of Entities Covered

AMIA thanks the FTC for adopting AMIA's 2020 comments on health apps qualifying under the scope of the HBNR. We reiterate and expand on our 2020 comments regarding the issues of data syphoning that need to be considered as well. This is also relevant under FTC's proposed amendment regarding scope (amendment III). The phenomenon of data syphoning was not contemplated in the HITECH Act or subsequent regulation. Data syphoning occurs when applications (apps) share health data without an individuals' knowledge or consent. A prescient example is the inclusion of private health information (PHI), deliberate or not, when web trackers are used on health system web pages. This data syphoning issue prompted the FTC and Health and Human Services to warn hospital systems and telehealth providers about these privacy and security risks from online tracking technologies, as protecting PHI is their responsibility under the Health Insurance Portability and Accountability Act (HIPAA) while companies not covered by HIPAA still have a responsibility under the HBNR itself.[1] AMIA applauds FTC for addressing data syphoning as recently as July 20, 2023. This recent example reinforces the importance of rules being specifically elucidated around data syphoning in the HBNR, as well as specifics around who is responsible for such breaches under the HBNR. HIPAA is clear that the health system is responsible for breaches related to data syphoning, however the HBNR is less clear.

[1] FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies. July 20, 2023. https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking

II. Clarification Regarding Types of Breaches Subject to the Rule

AMIA thanks the FTC for adopting AMIA's 2020 recommendation to adjust the definition of breach of security to include when a PHR or PHR-related entity fails to adequately disclose to individuals how user data is accessed, processed, used, reused, and disclosed. Adding the definition of "breach of security" is necessary, to ensure user data is protected according to the individual's need.

III. Revised Scope of PHR Related Entity

AMIA asks FTC to clarify the terms "PHR-service provider" and "third-party entity" and how they differ. For example, if a patient is prescribed a wearable cardiac monitor by their cardiologist, it is often the case that a third-party company is collecting and analyzing the data from the wearable monitor and returning that information back to the cardiologist. In such a case, does the physician give the patient the third-party's contact information so the patient can be in touch about their data? More likely, the physician will put in the order for the wearable and the company will send the device to the patient directly, giving the third-party entity the patient's address. If this third-party company's data is hacked, would it be the third-party company's responsibility to notify me that my information may have been leaked or my cardiologists' health system's responsibility? In any such scenario, the vendor would count as a "third-party entity," but if their link to the provider includes sharing of "PHR," such as EKG captured by their device, are they now a "PHR-service provider"? AMIA encourages FTC to clarify the threshold between the two definitions.

Similarly, when attempting to differentiate the two, we asked CHAT GPT to define how the FTC defines PHR-Service Provider and differentiate it from a third-party entity, CHAT GPT provides the following response:

> As of my last update in September 2021, the Federal Trade Commission (FTC) in the United States has not defined "PHR-service provider" explicitly in its regulations or guidelines. However, I can provide you with some general information about Personal Health Record (PHR) services and how they might relate to third-party entities.
>
> A Personal Health Record (PHR) is an electronic record of an individual's health information that is managed, controlled, and shared by the individual. It typically includes information such as medical history, medications, allergies, immunizations, lab results, and other health-related data. PHRs can be managed by various entities, including healthcare providers, health insurance companies, or standalone PHR-service providers.

Here's a general differentiation between a PHR-service provider and a third-party entity:

1. PHR-Service Provider: A PHR-service provider is a company or organization that offers individuals the ability to create, manage, and access their personal health records through an electronic platform or service. These providers may develop and operate dedicated websites or mobile applications where users can input, store, and access their health information securely. Examples of PHR-service providers might include companies like Microsoft HealthVault (which has been discontinued), Google Health, or other similar platforms.
2. Third-Party Entity: A third-party entity, in the context of PHRs, refers to any other company or organization that is not directly providing the PHR service to the individual but may have some involvement or association with the PHR data or platform. Third-party entities could include healthcare

> providers, health insurers, app developers, health data analytics companies, or any other entity that might have access to, process, or use the personal health information stored in the PHR. These entities might be authorized by the individual or may have gained access through data-sharing agreements or other arrangements with the PHR-service provider.
>
> It is essential to note that while the FTC doesn't have specific regulations for PHR-service providers, they do enforce privacy and security rules through various laws and acts such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. These regulations set standards for the protection of personal health information and may apply to both PHR-service providers and certain third-party entities that handle such data.
>
> Keep in mind that regulations and definitions may evolve over time, so I recommend checking the FTC's official website or other reliable sources for the most current information on how they define PHR-service providers and third-party entities.

Clearly an array of interpretations can be made, which is why the two definitions need to be further clarified.

Beyond definitions, another source of concern is that notices received by the FTC are designed to come from businesses who have been breached,[2] rather than from the consumers whose data was the subject of the breach. When reviewing the form and the consumer-focused reporting pathways, we note structural impediments to consumer-initiated breach complaints. Across the FTC's Complaint Assistant there is no category or sub-category for consumers who know their health data have been breached.[3] This is problematic given what we know about PHR data and health social media data. A highly publicized incident from 2018 involved a vulnerability that exposed the names and other information of Facebook members belonging to cancer-related private groups.[4] However, it was not Facebook that discovered and notified users, it was the users themselves. This consumer-led reporting to the FTC did not make the list of breaches, nor is it clear that user-reporting had its intended impact of changing Facebook's behavior.[5]

A more contemporary example comes from an app popular in the UK, Babylon Health, which is a telehealth app that allows patients to speak to a doctor, therapist, or other health specialist via a smartphone video call and, when appropriate, sends an electronic prescription to a nearby pharmacy. A user of the app noticed that footage of another patient's appointment was inappropriately placed in their account and alerted the company of the breach. While this company is based abroad, they operate in the U.S. and the global nature of the app economy could easily find users of the app in the US. Without a better way for individuals to report anomalies to the FTC, consumers are dependent on

[2] FTC Health Breach Notification Form. Available at: https://www.ftc.gov/system/files/documents/plainlanguage/2017_5_2_breach_notification_form.pdf
[3] FTC Complaint Assistant. https://www.ftccomplaintassistant.gov/#crnt&panel1-1
[4] Fazini, K; Farr, C. Facebook recently closed a loophole that allowed third parties to discover the names of people in private, 'closed' Facebook groups. CNBC. https://www.cnbc.com/2018/07/11/facebook-private-groups-breast-cancerprivacy-loophole.html. 1 Aug 2018.
[5] Ostherr, K; Trotter, F. Facebook's FTC settlement doesn't protect privacy of users' health information. STAT. https://www.statnews.com/2019/07/31/facebook-ftc-settlement-health-information-privacy/. 31 July 2019.

companies to act in good faith to address problems, which negates a central premise of the FTC's mission to protect consumers.

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

Regarding FTC's question as to whether a health app is considered a PHR 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). For example, would an app be considered a PHR because COVID tracing is possible through cell phone tracking of college students on spring break? Other possible non-health apps that could be used for health information are those related to grocery shopping or health education apps. For example, education apps can help better understand an individual's learning style and that information could be used to disseminate health education that is individually tailored. These are just a few examples that demonstrate the tangled webs of apps and how PHR can initially be accessed. AMIA does not have a specific recommendation at this time as to which apps in these scenarios should be included as PHR and which should be excluded. AMIA suggests FTC create a list of proposed requirements and boundaries for the public to respond to that can result in a list of concrete terms defining which apps are considered PHR.

V. Facilitating Greater Opportunity for Electronic Notice

Regarding whether the method of notice needs to come through the app, the app's website, e-mail (which FTC defines as including e-mail and text, message, in-app message, or electronic banner), post, and phone, AMIA recommends focusing on ensuring the method of notice comes through the app, the app's website, and e-mail to keep the communication direct and simple. The app has several methods of contacting the consumer via electronic notification that are efficient, direct, and modern.

VI. Expanded Content of Notice

Regarding FTC's questions as to whether the notifying entities can provide notice as to the potential harms, whether all the potential harms should be listed for individuals, or more specific data elements, AMIA recommends streamlining these disclosures while also providing as much information as is reasonable. Known harms must be disclosed and examples of the potential harms from the breach should be shared, but an exhaustive list should not be expected simply because all the potential harms cannot be known and that amount of information may be confusing to individuals. In the event of a data breach, it is helpful to individuals to know a third party has your data. AMIA recommends entities be required to list everyone who had access to the individuals' data (as much as possible). AMIA recommends aligning with HIPAA's requirements for ease.

***

AMIA would be pleased to continue to serve as a resource to the FTC and support health data privacy. Thank you for your time and consideration of these comments and your ongoing work protecting individuals' data.

If you have questions or require additional information, please contact Reva Singh, AMIA's VP of Public Policy, at rsingh@amia.org.

Sincerely,

Gretchen Purcell Jackson, MD, PhD, FACS, FACMI, FAMIA
President and Board Chair, AMIA
Vice President & Scientific Medical Officer, Intuitive Surgical
Associate Professor of Surgery, Pediatrics, and Biomedical Informatics
Vanderbilt University Medical Center