

August 8, 2023

The Honorable Lina M. Khan, Chair
U.S. Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Federal Trade Commission: Health Breach Notification Rule, 16 CFR Part 318, Project No. 205405

Dear Chairwoman Khan:

On behalf of the physician and medical student members of the American Medical Association (AMA), I am pleased to offer our comments in response to the U.S. Federal Trade Commission's (FTC or Commission) request for public comment on its Health Breach Notification (HBN) Rule ("HBN Rule" or "Rule"). The AMA appreciates the Commission's efforts to clarify existing notice obligations for entities covered by the Rule,¹ to strengthen the Rule's applicability to keep pace with recent technological advances, as well as FTC's commitment to regulating the use of digital health platforms, apps, and other similar software programs that collect, use, store, and share personal health data. We note, however, potentially serious unintended consequences from several proposals, particularly the newly proposed "health care provider" definition.

Revised and Newly Added Definitions

The AMA appreciates that the Commission continues to specifically exclude from the Rule's scope of application entities that are subject to the Health Insurance Portability and Accountability Act (HIPAA).² This clear delineation avoids the potential for burdensome, competing notice obligations under the HBN Rule and the HIPAA statutory regime.

a. Revised definition of "PHR identifiable health information"

The AMA agrees with the Commission that broadening the existing definition of "personal health record (PHR) identifiable health information" as proposed, will serve to clarify to consumers the scope of products and services affected by the HBN Rule, and to entities covered by the Rule, their compliance obligations. The FTC's stated intention³ to include the following data types within the Rule's scope will go a long way toward building consumer trust and enhancing awareness of requirements within the regulated community:

1. Traditional health information such as diagnoses or medications;

¹ Health Breach Notification Rule, 88 Fed. Reg. 37819, 37833 (proposed June 9, 2023).

² *Ibid* at 37834, third column.

³ *Ibid* at 37823, first column.

2. Health information derived from consumers' interactions with apps and other online services such as health information generated from tracking technologies on websites or mobile apps; and
3. Emergent health data (such as health information inferred from non-health-related data points, such as location and recent purchases).

The broader and more clearly articulated proposed definition seems well-positioned to diminish confusion in the health care community regarding “what happens” to individual health information once it is no longer held by a HIPAA covered entity, and what protections apply to this information when it is generated or inferred entirely outside of a health care setting.

b. New definition of “health care provider”

We are very concerned that the proposal to introduce a new definition of “health care provider” in a Rule that explicitly excludes HIPAA covered entities from its scope will cause needless confusion. The text of the definition⁴ does little to bring clarity of any kind. To track down the cross-referenced meaning of the term requires reference to no less than 40 statutory and regulatory provisions.

The Commission’s objective in coining the new term remains unclear and the preamble text does little to illuminate the FTC’s intended effect in crafting this definition. Based on the recurrence of the new term, “health care provider” in the proposed regulatory text, and there is only one,⁵ the term is used to clarify that in order to qualify as PHR identifiable health information, the information must have been created or received by a health care provider, health plan, employer, or health care clearinghouse.

Those familiar with HIPAA will quickly recognize that health care provider,⁶ health plan, and health care clearinghouse, are the three types of covered entity defined in the HIPAA regulations. A reasonable reading of the proposed regulations could only infer that the FTC intends, as part of its definition of PHR identifiable health information, that such information must have been created or received by a HIPAA covered entity (encompassing what are traditionally recognized as health care providers, health plans, and health care clearinghouses), with the addition of employers, and the new set of “health care providers” beyond those that are subject to HIPAA, pursuant to FTC’s proposed definition.

What are “health care providers” if they are not HIPAA covered entities? Perhaps the most helpful sentence in the proposed HBN rule appears in footnote 42,⁷ discussing, in part, the FTC’s recent enforcement action against Flo Health, Inc., a menstruation tracking app:

“Under the definitions cross-referenced by the Rule, **Flo – which markets itself as a ‘health assistant’ – is a ‘health care provider,’** in that it ‘furnish[es] health care services and supplies.’” [emphasis added]⁸

⁴ *Health care provider* means a provider of services (as defined in 42 U.S.C. 1395x(u)), a provider of medical or other health services (as defined in 42 U.S.C. 1395x(s)), or any other entity furnishing health care services or supplies. Health Breach Notification Rule, footnote 1, *supra*, at 37835, middle column.

⁵ *Id.* “Health care provider” is referenced as part of the proposed revision to the definition of PHR identifiable health information. See proposed 16 CFR Part 318, §318.2(i)(4)(i).

⁶ Per the regulatory definition noted above, a health care provider is considered a covered entity only if they transmit health information in electronic form in connection with a transaction, as further defined in the HIPAA regulations. 45 CFR §160.103.

⁷ Health Breach Notification Rule, footnote 1, *supra*, at 37823, middle column.

⁸ *Supra*, citing See Joint Statement of Commissioner Rohit Chopra and Commissioner Rebecca Kelly Slaughter, Concurring in Part, Dissenting in Part, In the Matter of Flo Health, Inc., FTC File No. 1923133 (Jan. 13, 2021),

The AMA strongly urges the Commission to abandon this highly ambiguous and potentially harmful definition. To lump together apps such as FitBit and Flo, in the same regulatory definition as physicians, is a disservice to consumers of public health and the industry as a whole.

By the FTC’s own account, “HHS has defined the term ‘health care provider’ . . . referring primarily to persons and entities such as doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies.”⁹ The HHS definition aligns with the common understanding and usage of the term: “A health care provider is an individual health professional or a health facility organization licensed to provide health care diagnosis and treatment services including medication, surgery and medical devices.”¹⁰

The concept of a health care provider being an individual or organization who is qualified to render medical care is not only the plain meaning of the term, but one that is entrenched in the public’s perception, as well as the health care industry itself. Recent years have already seen escalating confusion in the roles of medical professionals,¹¹ resulting in patient harm and sometimes death,¹² yet the Commission proposes to include physicians in the same definition as calorie counters and meditation apps.

The potential for harm posed by this definition is very easily avoided. The new health care provider definition serves no other purpose within the Rule than to flesh out the definition of PHR identifiable health information. As noted in the above discussion, instead of defining PHR identifiable health information as proposed, the FTC should delete the unhelpful, unnecessary, and potentially harmful definition of health care provider and should simply provide, as a basis for the PHR identifiable health information definition, that the information must have been created or received by a HIPAA covered entity (also defined in the proposed Rule), with the addition of employers, and the new set of non-HIPAA covered entities that the FTC seeks to include. To create a more appropriate definition for these apps, tracking devices, etc., that are now confusingly colored as “health care providers” under the proposals, the FTC could, for example, term them more descriptively as “health apps and diagnostic tool services.” **It is critical to make this distinction.**

c. Revised definition of “breach of security”

The AMA applauds the FTC’s revision of this definition to clarify that health apps and other products experience a “breach of security” under the Rule when they disclose users’ sensitive health information

https://www.ftc.gov/system/files/documents/public_statements/1586018/20210112_final_joint_rcrks_state_ment_on_flo.pdf; See also, FTC’s statement, “These changes clarify that developers of health apps and similar technologies providing these types of “health care services or supplies” qualify as “health care providers” under the Rule.” *Id.*

⁹ Health Breach Notification Rule, footnote 1, *supra*, at 37824, first column, citing informal input the Commission received from staff at other federal agencies, and finding (incorrectly, we assert) that the proposed health care provider definition is consistent with the statutory provision at 42 USC 1320d.

¹⁰ Wikipedia entry for “Health care provider,” available at https://en.wikipedia.org/wiki/Health_care_provider.

¹¹ See, e.g., *Battlefield Widens with Hundreds of Scope-creep Bills Introduced*, A. Robeznieks, May 31, 2023, available at: <https://www.ama-assn.org/practice-management/scope-practice/battlefield-widens-hundreds-scope-creep-bills-introduced>.

¹² *Why Stopping Scope Creep is about Protecting Patients*, interview with Rebekah Bernard, MD, S September 7, 2022, transcript available at <https://www.ama-assn.org/practice-management/scope-practice/why-stopping-scope-creep-about-protecting-patients>.

without authorization;¹³ noting that cybersecurity intrusions or nefarious behavior are not necessary components of a breach.

We appreciate FTC’s adoption of the AMA’s recommendation to define ‘unauthorized access’ as presumed when entities fail to disclose to individuals how they access, use, process, and disclose their data and for how long data are retained.¹⁴ The current proposals help to clarify that the Rule covers unauthorized disclosures of consumers’ PHR identifiable health information to third party companies.

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

The AMA supports FTC’s revised definition of PHR and the addition of the phrase, “has the technical capacity to draw information from multiple sources,” even if the synching feature is not enabled. In addition, the AMA urges FTC to broaden the PHR definition to include when an app only draws health information from one place, but extracts non-health information drawn from other sources, as well as when a PHR only draws identifiable health information from one place with non-identifiable health information coming from others.

These clarifications are needed and help to make the definition more straightforward and patient-centric. This new definition will provide individuals with greater confidence to use PHRs and health apps to better engage in their own health care journey and not have to worry whether changes they make in app preferences and functionalities could cause that app to no longer qualify as a PHR and remove the protections associated with the Breach Notification Rule. The AMA supports the ability of patients to access and use their health care data and wants to position patients to be more informed decision makers and true partners in the delivery of health care services.

The privacy of one’s own health information is of increasing importance to patients and FTC’s work in this area is critical. In a 2022 AMA/Savvy Cooperative Survey of 1000 patients, 92 percent of patients believe that privacy is a right and nearly 75 percent of patients are concerned about protecting the privacy of their health data. Almost 95 percent of patients state that companies that collect, store, analyze or use health data should be held accountable by the law. Nearly 80 percent of patients want to be able to “opt-out” of sharing some or all of their health data. More than 75 percent of people want to receive requests prior to a company using their health data for a new purpose. Overall, our survey indicates more needs to be done to create transparency on how apps use patient medical information.¹⁵

The AMA has extensive policy advocating for maintaining the privacy of patient information. We work to ensure that as health information is shared—particularly outside of the health care system—patients have meaningful controls over and a clear understanding of how their data is being used and with whom it is being shared. Above all, patients must feel confident that their health information will remain private. The AMA’s Privacy Principles¹⁶ also highlight how an entity must disclose to individuals exactly what data it is collecting and the purpose for its collection.

We believe such information should not be used for a materially different purpose than that disclosed in the notice at the point of collection of such information. This point speaks to the importance of protecting

¹³ Health Breach Notification Rule, footnote 1, *supra*, at 37821, middle column, citing 16 CFR 318.2(a).

¹⁴ *Ibid* at 37824, footnote 51.

¹⁵ <https://www.ama-assn.org/system/files/ama-patient-data-privacy-survey-results.pdf>.

¹⁶ <https://www.ama-assn.org/system/files/2020-05/privacy-principles.pdf>.

all an individual's data from data security breaches or unauthorized disclosures as some personal information (contextual or geographic location data) whose primary purpose may not appear to be health-related, could, in fact, be used as an individual identifier, or could be combined with outside data sources to be used for detrimental purposes against an individual.

The AMA believes that health care information is one of the most personal types of information an individual can possess and generate—regardless of whether it is legally defined as “sensitive” or protected health information under the HIPAA—and individuals accessing, processing, selling, and using it without the individual's best interest at heart can cause irreparable harm. These rights should apply to PHRs as individuals have the right to control how entities access, use, process, and disclose their data, including secondary (and beyond) uses.

In addition, FTC correctly notes how apps and other direct-to-consumer health technologies have become commonplace, and how consumer use of these health-related technologies increased significantly during the COVID-19 Pandemic. Moreover, with the work of the Office of the National Coordinator for Health Information Technology (ONC) on increasing information sharing and reducing [information blocking](#), as well as a broader definition of [electronic health information](#) (EHI), more health information is going to be interoperable and available to patients to share with and manage through a PHR. FTC's revised PHR definition will serve as another means to protect an individual's personal information (including identifiable and non-identifiable health information, as well as non-health information) and hold PHR vendors accountable for breaches and unauthorized disclosures.

Notification of Breach – Facilitating Greater Opportunity for Electronic Notice

The AMA supports the work of FTC to authorize expanded use of electronic notices to inform individuals of breaches and unauthorized disclosures. We agree that many interactions that an individual would have with a PHR vendor or health app would occur via electronic means, but individuals should have options about how they choose to be informed of a breach. An individual's preferences should be requested and recorded when they sign-up or enroll with a PHR or health app. Consumers should have the option to choose a combination of electronic means of notification, as well as standard notification via postal, first-class mail. Under any scenario, PHR vendors should be required to inform individuals in a timely manner via multiple modalities simultaneously to ensure that they receive clear and effective breach notifications.

The electronic mail options that FTC discusses (notification by email, text message, within-application messaging, or electronic banner) should all be made available to PHR users, and they should be required to choose a minimum of two means of electronic notification, as well as postal mail notices, if requested. Allowing consumers to choose the options that best suit their lifestyle should result in notifications that are most likely to reach them.

The AMA supports the new definition put forward in the Proposed Rule for “clear and conspicuous” notification. Ensuring that a breach or unauthorized disclosure is reasonably understandable and calls attention to the significance of the information that is included in the notice is imperative.

We also appreciate FTC's endeavor to create a model notice to assist PHR vendors in communicating with consumers when a breach occurs. These vendors should feel empowered to use the model notice provided, but FTC should require that if a vendor chooses not to use the notice, that all the elements and components included in the notice are adequately relayed in a comparable communication to the affected individuals. The content requirements described below are a good start. Each means of communication with individuals (notification by postal mail, email, text message, within-application messaging, or

electronic banner) may have its own nuances, so it is important that certain information is required to be transmitted to individuals, but vendors should not be mandated to use the model notice if it does not fit into the specific modality that an individual requests for notification.

Notification of Breach – Expand Content of Notice

The AMA supports the content modifications in the required notice to individuals. First and foremost, the content should be educational in nature and include plain, non-technical, and easy-to-understand language. The FTC should look at the notice to individuals as an additional opportunity for PHRs to educate consumers on the benefits of sharing personal health information, as well as relevant health data privacy issues. Underlying all this work for consumers are the privacy and security considerations they assume when moving their personal health data from a HIPAA regulated environment to a third-party app that likely functions outside of HIPAA. The FTC should require a breach notice to be used as an additional resource to consumers that explains the value of their personal health information, how to be empowered and exhibit more control over that information, and how they should consider sharing that information to help direct their own care journey.

The AMA supports the proposed requirement that a breach notice include a brief description of what happened during the breach and the potential harm that may result, such as medical or other identity theft. We agree that this information will help individuals better understand the connection between the information breached and the potential harm that could result from the breach of such information. Detailed contact information for any third parties that acquired unsecured PHR identifiable health information because of the security breach should be included. The notice should also be expanded to incorporate other types of unsecured PHR identifiable health information that were involved in the breach, including FTC's exemplar list (health diagnosis or condition, lab results, medications, other treatment information, the individual's use of a health-related mobile application, and device identifier).

In addition, the breach notice should include a brief description of what the entity that experienced the breach is doing to protect affected individuals, such as offering credit monitoring, identity theft protection, or other services. Informing individuals about these steps is important so that they know what additional actions they should take to protect themselves from potential harm. Moreover, we agree that the notice should specify multiple means for affected individuals to contact the notifying entity to ensure that communication between the two is encouraged and facilitated.

Changes to Improve the Rule's Readability

The AMA supports the FTC's intent to improve the Rule's readability. We believe the measure to include explanatory parentheticals and statutory citations may be a helpful step toward this goal and toward promoting comprehension. We find this has the potential to also foster greater consistency among definitions which may help to avoid misinterpretation of terminology. The AMA encourages the FTC to include parentheticals that are easily understood by a variety of audiences of different educational levels, and to consider potential language barriers.

Consolidated Notice and Timing Requirements

The AMA generally supports the non-substantive changes made to the consolidated notice and timing requirements. While we support the creation of a pathway that includes maintaining a log for breaches affecting fewer than 500 individuals, we see this as a less effective compromise than our previous recommendation to FTC on the matter.

The Honorable Lena M. Khan

August 8, 2023

Page 7

The public may be better served by the HBN Rule if it were to require public reporting of breaches affecting fewer than 500 individuals. Strengthening the FTC's enforcement activity in this way would lead to an increased level of transparency and more accurate reporting of those individuals whose information has been improperly disclosed. Accordingly, the AMA urges the FTC to provide additional information to the public regarding the notices it has received that impacted fewer than 500 individuals. For example, if the FTC received numerous notices that impacted 300-499 individuals, then perhaps the 500+ standard should be revised to require reporting for breaches impacting 300 or more individuals. Again, this emphasis on increased transparency would help to build confidence in the use of technologies such as mobile health apps, and would encourage the public to regard the FTC as a reliable information resource when evaluating which platforms they should entrust with their health data.

Revised Enforcement Provision

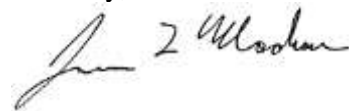
In general, the AMA believes that breach notification provided in the most clear and accessible manner will go furthest to attain the desired result of informing individual consumers with actionable information. We recommend that, as HBN violations are filed, the FTC will use actual examples as case study models for future educational resources in an effort to demonstrate what the standard reflects in different scenarios.

Conclusion

The importance of assuring the public that their health-related data remains protected once it is outside the scope of HIPAA cannot be overstated. In the current climate, where seemingly inconsequential data may be combined and used in efforts to punish individuals for accessing evidence-based health care, the protections included in the proposed Rule are more vital than ever to shore up consumer confidence and rein in unauthorized disclosures by entities entrusted with individuals' health information.

Thank you for the opportunity to provide comments on this proposal. Please contact Margaret Garikes, Vice President, Federal Affairs at margaret.garikes@ama-assn.org or 202-789-7409 with any questions or concerns.

Sincerely,

A handwritten signature in black ink, appearing to read "James L. Madara". The signature is written in a cursive, flowing style.

James L. Madara, MD