AHIMA
American Health Information Management Association®

233 N. Michigan Ave., 21st Fl., Chicago, IL USA 60601-5809 | www.ahima.org | 312.233.1100

August 7, 2023

Lina Khan
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

Re: Health Breach Notification Rule, Project No. P205405

Dear Chairwoman Khan:

On behalf of the American Health Information Management Association (AHIMA®), I am responding to the Federal Trade Commission (FTC) Health Breach Notification Rule proposed rule, as published in the June 9, 2023 Federal Register.

AHIMA is a global nonprofit association of health information (HI) professionals with more than 67,000 members and more than 100,000 credentials in the field. The AHIMA mission of empowering people to impact health® drives our members and credentialed HI professionals to ensure that health information is accurate, complete, and available to patients and providers. Our leaders work at the intersection of healthcare, technology, and business and are found in data integrity and information privacy job functions worldwide.

The following are comments and recommendations on selected sections of the proposed rule.

II. Analysis of the Proposed Rule

1. Clarification of Entities Covered

The FTC proposes to modify the definition of "PHR identifiable health information" to include information (1) that is provided by or on behalf of the individual; (2) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual; (3) relates to the past, present, or future physical or mental health or condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual; and (4) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse.

The FTC proposes to add the definition "healthcare provider" to mean a provider of services, including medical or other health services, healthcare services, or healthcare supplies. The FTC also proposes to add the definition "healthcare services or supplies" to mean any online service, such as a website, mobile application, or Internet-connected device that provides mechanisms to track health and personal data.

AHIMA supports the proposed modifications to broaden the definition of "PHR identifiable health information" and add the new definitions of "healthcare provider" and "healthcare services or supplies" to include apps, websites, and devices that consumers use to track health and personal data. Consumers have increasingly relied on digital tools and health apps to monitor and track their health and personal data, particularly during the rise of the COVID-19 pandemic. According to a recent study, two in five US adults are now using health apps, with the top motivations being exercise, fitness, step or heart rate monitoring, and sleep or weight tracking.[1] However, many companies offering these services are not covered by the Health Insurance Portability and Accountability Act (HIPAA), and consumers risk being unaware of the limited protections surrounding their data and rights when their data is shared with a third party. AHIMA supports the FTC's proposals to expand the definition of healthcare provider to include non-HIPAA covered entities in these regulations.

Given the rise in the use of these apps and the scope of data tracked, AHIMA urges the FTC to ensure social determinants of health (SDOH) data is captured under the definition of "PHR identifiable health information." In addition to clinical data related to a patient's health status, SDOH data includes but is not limited to data on education, safe housing, access to nutritious foods, transportation, and environmental factors. When appropriately collected, used, and securely shared, SDOH data gives providers insight into various elements that make up a patient's medical and non-medical story and creates the opportunity for collaboration to improve health and well-being.

In 2022, AHIMA partnered with NORC at the University of Chicago to study the operational realities of how SDOH data is collected, coded, and used in real-world healthcare settings. Key findings included that nearly eight in 10 healthcare organizations collect SDOH data but face challenges related to the collection, coding, and use of this data, stemming from a lack of standardization and integration of the data, insufficient workforce training, and limited sharing of SDOH data.[2] AHIMA launched Data for Better Health™, a multi-year strategic initiative aiming to provide tools, resources, and education to support a better understanding of the importance of collecting, sharing, and using SDOH data and how it can be used to improve health and healthcare outcomes.

This valuable yet sensitive data that may be included in health apps must be protected as part of the patient's personal health record to prevent unauthorized access to this information that may lead to further bias or discrimination against consumers. AHIMA urges the FTC to work with stakeholders to create guidance including examples of the data that should be included in the definition of "PHR identifiable health information" and ensure this is reviewed and updated regularly.

AHIMA requests the FTC to provide further clarity on the difference in this rule's application to equipment and devices provided by a consumer's healthcare provider versus products and devices consumers purchase independently, particularly as it relates to physical devices. For example, AHIMA encourages the FTC to clearly delineate how these regulations would not apply to a medical device such

[1] Available at: https://www.businessofapps.com/news/two-in-five-us-adults-now-use-health-apps/
[2] Available at: https://ahima.org/media/03dbonub/ahima_sdoh-data-report.pdf

as a heart rate monitor prescribed to a patient undergoing rehabilitation post-surgery, compared to how these regulations would apply to a patient using a fitness tracking app with a heart rate monitoring wristband that they purchased independently. This clarification would assist healthcare providers and other entities in understanding their role in the breach notification process, and whether their devices are applicable under HIPAA, including the limits of their business associate agreements with such device manufacturers, and the FTC rules.

2. Clarification Regarding Types of Breaches Subject to the Rule

The FTC proposes to modify the definition of "breach of security" to include that a breach of security includes an unauthorized acquisition of unsecured PHR identifiable health information in a personal health record that occurs as a result of a data breach or an unauthorized disclosure.

AHIMA supports expanding the definition of "breach of security" to include unauthorized acquisitions of unsecured PHR identifiable health information as a result of unauthorized disclosures. A recent study from Duke University on personal devices and health apps for mental health data found that data brokers often advertise and sell this highly sensitive data.[3] The threat of this practice has been made clear through the FTC's two recent enforcement actions against GoodRx and Easy Healthcare, in which these companies violated privacy promises made to users about data sharing by disclosing PHR identifiable health information to third party companies. Not only is sharing this information without consumer consent problematic, but sharing consumer health information increases the risk of additional unauthorized acquisition and sharing of this information among bad actors. Actions from PHR vendors selling data or otherwise intentionally disclosing it without consumer consent must be included in the definition of "breach of security" to ensure the broad applicability of the Health Breach Notification Rule includes such practices.

3. Revised Scope of PHR Related Entity

The FTC proposes to revise the definition of "PHR related entity" to make clear that PHR related entities include entities that offer products and services not only through the websites of vendors of personal health records, but also through any online service, including mobile applications. The FTC also proposes to narrow this definition to entities that access or send unsecured PHR identifiable health information to a personal health record, rather than entities that access or send any information to a personal health record.

AHIMA agrees with the revised definition of "PHR related entity" and the proposal to narrow the definition to entities that access or send unsecured PHR identifiable health information to promote targeted and easier enforcement of the Health Breach Notification Rule. We agree that most firms that perform services such as attribution, analytics, and data collection on consumer use of products would be considered third-party providers rather than PHR related entities. However, we urge the FTC to review this definition regularly to ensure it encompasses all relevant entities and to propose changes to this definition, as needed, as third-party service providers continue to evolve over time.

AHIMA encourages the FTC to clarify what criteria would qualify an entity as a PHR related entity and publish a list of examples received by commenters. Part of this clarification should include a clear

[3] Available at: https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf

delineation of what would cause an entity to fall under the definition of PHR related entity. This is likely to be an ongoing and evolving process as unique characteristics of various entities can change over time. For example, if an entity creates a product but also sells personal health record software, that entity could be considered a third-party service provider, a PHR related entity, or potentially both. If there is any overlap between an entity falling under the definition of PHR related entity and third-party service provider, AHIMA believes such an entity should be considered a PHR related entity.

AHIMA agrees with the FTC's conclusion to consider it a breach of security if a third-party service provider, such as an analytics firm, receives PHR identifiable health information and sells it to another entity without the consumer's authorization. Consumer consent to the original collection of data does not encompass the sharing of that data with other entities that are not involved in providing the service consumers are using. In cases where entities do seek consumer consent for this practice, AHIMA believes the request for consent must be clear, conspicuous, and written in plain language.

As mentioned in other areas of this comment letter, AHIMA encourages the FTC to include SDOH data under the definition of PHR identifiable health information and thus believes apps, companies, and entities that collect and/or use SDOH data should be included under the definition of PHR related entity. As such, we also encourage the FTC to ensure that SDOH data is covered as part of the data prohibited for disclosure by PHR related entities.

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

The FTC proposes to revise the definition of "personal health record" to include an electronic record of PHR identifiable health information on an individual that has the technical capacity to draw information from multiple sources and that is managed, shared, and controlled by or primarily for the individual, even if the consumer elects to limit information from a single source only.

AHIMA supports the FTC's proposal to revise the definition of "personal health record" (PHR). These changes align with comments AHIMA made to the FTC in 2020 when responding to the FTC's initial request for information (RFI) related to the Health Breach Notification Rule.[4] By updating the definition of PHR, the FTC ensures that current-day technologies that store and exchange patient health data are held accountable for maintaining users' privacy.

When the original Health Breach Notification Rule was published, PHR technology was nascent, and the tools used inside provider facilities shared more similarities than differences. Since then, the technology space for health data has rapidly expanded with consumer technology advancement. Patients now have access to their health data at the tip of their thumbs through phone and tablet devices and subsequently, the privacy regulations governing such technologies need to be updated.

One of the most important changes proposed by the FTC in this rule is ensuring that patients do not need to connect a PHR to multiple sources for the PHR to be considered under FTC jurisdiction. Many mobile applications today specialize in one type of data capture for an individual. These applications include step trackers, tools for accessing patient portals, weight management tools, and other healthcare-related products. AHIMA supports the FTC's inclusion of this updated provision in the proposed rule, and we support its finalization.

[4] Available at: https://ahima.org/media/1yildq3j/ftc-breach-notification-comments_ahima.pdf

The Office of the National Coordinator for Health Information Technology (ONC) is nearing completion of its information blocking implementation roadmap. This includes the requirement that providers covered by the rule make patient data available via an application programming interface (API) from their electronic health record (EHR) for patients to access and download their data. Implementation of this requirement is crucial for the FTC's privacy oversight activities as individuals will increasingly have the ability to transmit their data beyond a HIPAA-regulated environment into one governed by the FTC. Currently, the Health Breach Notification Rule does not include apps individuals store their health data in. Such lack of oversight strengthens the reasoning behind AHIMA's support for the proposed changes and we encourage the FTC to continue reviewing other data privacy regulations to ensure there is sufficient oversight over non-HIPAA-covered actors.

5. Facilitating Greater Opportunity for Electronic Notice

The FTC proposes to allow the notice of breach of security to be delivered via electronic mail in combination with one of the following: text message, in-app messaging, or electronic banner. The FTC includes a model notice that entities may use to notify individuals and invites comments on if this model notice should be mandatory.

AHIMA supports the option to deliver the breach of security notice via electronic mail along with one other electronic method. We believe this proposal is comprehensive and timely given the ubiquitous digital environment. While we appreciate the FTC maintaining the consumer's option to receive notice via first-class mail and believe the consumer's preferences for communication should continue to be honored, AHIMA believes entities should be required to notify consumers they are eligible to choose electronic mail as their primary contact method. Further, we encourage the FTC to clarify that the in-app messaging method must include push notifications in the event of a breach. A breach of security is an extremely timely issue and consumers may not check the app regularly. As such, they should be made aware of a breach as soon as possible.

AHIMA appreciates the FTC providing the model notice and applauds the agency for providing entities with resources to comply with these requirements. Making the model notice mandatory can lead to industry consistency and it may be easier for consumers to understand the message and the contents if they are familiar with a uniform, standardized notice. If made mandatory, the FTC must ensure the model notice is accessible to all entities and we encourage the FTC to determine ways to ensure the model notice is easy to complete across different methods (e.g., in addition to electronic mail, in-app messaging, first-class mail, and more). Further, the information included in the model notice should be consistent across all communications, regardless of the medium used.

6. Expanded Content of Notice

The FTC proposes to require that the content of notice be expanded to include a description of the potential harm that may result from the breach and contact information of any third parties that acquired unsecured PHR identifiable health information as a result of the breach of security, if the vendor knows. The FTC also proposes to require the notice to include what the entity is doing to protect affected individuals.

AHIMA supports the FTC's expanded requirements for the content of a breach notification. Victims of a breach must be able to understand the extent of a breach and what the entity is doing to protect the victim

from further breach. Once a breach has occurred, it is often the case that the data is difficult to recapture. However, victims of a breach can take rapid steps to protect themselves from further harm. Additionally, knowing what a vendor is doing to protect victims can assist consumers in making purchase decisions for third-party products such as credit monitoring and fraud detection. While AHIMA supports the idea of requiring breached entities to disclose who performed the breach, it can be difficult during or after a cyberattack to determine who performed the intrusion. We recommend the FTC provide consideration for vendors unable to identify the entity who participated in the breach due to cyberattack.

In previous AHIMA comment filings related to data privacy, we have highlighted the difficulty in determining harm for breaches of HIPAA data.[5] That difficulty is expanded when it relates to HIPAA-covered entities. Harm from a patient medical data breach could range anywhere from Medicare fraud to identity theft and is difficult to provide specifics on. While it is true that this information could be helpful if presented to victims of a breach, requiring an entity to include potential harm may only cause further anxiety to victims of data theft. We encourage the FTC to convene industry stakeholders to determine the best implementation of this requirement if it were to be finalized. The burden will remain on the FTC to find the best implementation strategy to maximize this proposed requirement's impact. AHIMA recommends that as part of that strategy, the FTC provide enforcement discretion for entities working in good faith to provide an exhaustive list of potential harms that may inadvertently neglect to include a specific harm. The spirit of this proposed requirement is to encourage communication to the breach victims, and we believe even with this leniency that the spirit will be upheld.

The FTC proposes to expand the list of PHR identifiable information to include health diagnosis or condition, lab results, medications, other treatment information, the individual's use of a health-related mobile application, and device identifier.

AHIMA supports the proposed expansion of the list of PHR identifiable information. We encourage the FTC to regularly review the list of PHR identifiable information to ensure it aligns with the current technical realities of health technology. For instance, as biometric technologies continue to advance there may be a need for this list to be expanded to include certain types of data such as retinal or fingerprint images. One potential option to ensure this list is accurate with current-day health data activities is for the FTC to convene a regular health IT expert panel. This panel could provide input to the FTC and recommendations on how best to keep these requirements up-to-date and relevant.

The FTC proposes to add within-application contact to the list of contact procedures for consumers to ask questions or learn more information about the breach and proposes to require that entities use two methods of contact procedures to notify individuals.

AHIMA supports this proposed requirement for organizations to add within-application contact information. During and after a breach, having open lines of communication can help provide breach victims with a sense of calm and provide them an avenue to find more information about the breach. AHIMA also supports the proposed requirement for entities to use two methods of contact procedures to notify victims of their data being breached. Requiring multiple contact options ensures victims of all backgrounds and technical capabilities are able to contact the vendor to learn more about how to protect themselves after a breach.

[5] Available at: https://ahima.org/media/tl2cdnyx/final-ahima-ocr-rfi-comment-letter_052322.pdf

AHIMA recommends the FTC review the HIPAA notification requirements for breach notification to ensure it aligns with the FTC's proposed requirements for contact between a vendor of PHRs and victim of a health breach. Creating a predictable environment for victims across all types of health data modalities ensures they feel more confident in acting after a health data breach.

7. Proposed Changes to Improve Rule's Readability

The FTC proposes to combine into single sections the Health Breach Notification Rule's breach notification and timing requirements and add a new section that plainly states the penalties for noncompliance.

AHIMA supports these proposed changes to improve readability and promote compliance among eligible entities.

III. Changes Considered but not Proposed and on Which the Commission Seeks Public Comment

1. Defining Authorization and Affirmative Express Consent

The FTC seeks comment on whether FTC enforcement actions provide sufficient guidance to put companies on notice about their obligations for obtaining consumer authorization for disclosures, or whether defining the terms "authorization" and "affirmative express consent" would better inform companies of their compliance obligations.

AHIMA recommends the FTC define the terms "authorization" and "affirmative express consent" to ensure there is no confusion on the requirements for companies to obtain consumer authorization or approval. When working in this regulatory environment, it is important for the FTC to ensure there is no room for companies to lessen their burden for obtaining disclosure. Additionally, providing specific definitions will help consumers understand their rights related to consenting to the release of data. A lack of specificity creates an environment of uncertainty, raising the potential for consumers to consent to the disclosure of their information when they may have had no intention of doing so. When discussing terms linked to decision making AHIMA recommends the FTC provide clear delineations to ensure everyone involved knows the rules of the road.

The FTC seeks comment on the definitions of "authorization" and "affirmative express consent" and what constitutes acceptable methods of authorization, particularly when unauthorized sharing is occurring.

AHIMA recommends the FTC convene an expert group to further define authorization in this context to ensure all parties involved in the consent and release process are aware of what is included in active consent. Additionally, AHIMA recommends affirmative expressed consent not be included under the FTC Health Breach Notification Rule and recommends only explicit authorization be used as a litmus test for whether a consumer has given the affirmative to a vendor of PHRs for their information to be released. By eliminating the ability for vendors of PHRs to utilize affirmative expressed consent, the FTC ensures that health data disclosure requirements remain in alignment with HIPAA. Providing a predictable authorization environment ensures consumers are educated and empowered to make informed decisions about when to allow their data to be disclosed.

The FTC seeks comment on whether there are certain types of sharing for which authorization by consumers is implied because such sharing is expected or necessary to provide a service to consumers.

AHIMA recommends the FTC refrain from allowing implied consent to be a standard as it relates to the release of health data. Implied consent creates a slippery slope where vendors of PHRs could implement unclear and often misleading techniques which results in consumers unwittingly agreeing to share their data contrary to their personal privacy preferences. We acknowledge that in emergency situations implied consent from a patient unable to provide consent may be needed and we encourage the FTC to include this exception in any implied consent proposals. This ensures a predictable consent environment exists for health data both in the HIPAA-covered space and in the non-HIPAA-covered space. By eliminating the idea of implied consent, FTC is also creating an easier regulatory environment where enforcement is a process with clear black and white rules.

2. Modifying Definition of Third-Party Service Provider

The FTC defines a "third party service provider" as an entity that "(1) provides services to a vendor of personal health records in connection with the offering or maintenance of a personal health record or to a PHR related entity in connection with a product or service offered by that entity; and (2) accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services." The FTC seeks comment on the scope of entities that should be considered under this definition and what it means to "provide services."

AHIMA recommends the FTC convene an expert workgroup to further define what "provide services" means in a healthcare context. By convening a workgroup of industry experts, the FTC can ensure it is developing a comprehensive definition that will not be left up to interpretation. Ensuring no gray area remains in this definition will protect health data by eliminating potential third-party service provider loopholes. We believe the industry is best positioned to provide FTC with this input and together can create a definition that suits all parties' needs.

3. Changing Timing Requirements

The FTC seeks comment on whether earlier notification of consumers would better protect them or if it would lead to partial notifications, because the entity experiencing the breach may not have had time to identify all the relevant facts.

AHIMA recommends the FTC review the Cybersecurity and Infrastructure Security Agency (CISA) breach notification requirements[6] for providers and align the timelines with those requirements. Healthcare is considered one of the critical sectors in the country and that should extend to those groups operating outside of a HIPAA-covered space. By aligning with CISA's requirements, the FTC can ensure all parties handling sensitive health data are held to the same standard for breach notification and data protection.

The FTC also seeks comment on whether the timeline to notify the FTC should be extended to give entities more time to investigate breaches and related impacts, or if an extension would delay action and minimize the opportunity for entities to work with the FTC to gather facts immediately following a breach.

[6] Available at: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

AHIMA recommends the FTC limit the timeline between the discovery of a breach and notification to ensure victims are provided the information needed to make decisions about protecting their information. Providers governed by HIPAA are not afforded the ability to delay notification until after an investigation is completed and it is important for requirements to align in both HIPAA and non-HIPAA environments. The FTC could explore options to incentivize early breach notification to remove the stigma that breach notification automatically leads to penalty enforcement. Without these incentives, the stigma that delaying notification benefits breached entities will continue. Rapid notification leads to rapid response and empowering consumers to move expeditiously in protecting their data is crucial in an evolving cyber threat environment.

AHIMA applauds the FTC for proposing updates and revisions to the Health Breach Notification Rule to apply to the modern-day use of health apps and devices. As the FTC continues these efforts, AHIMA and its membership look forward to partnering with the FTC to protect consumer health and personal data from data breaches and unauthorized acquisitions. If AHIMA can provide any further information or if there are any questions regarding this letter and its recommendations, please contact Andrew Tomlinson, Director of Regulatory Affairs, at (312) 223-1086 or andrew.tomlinson@ahima.org.

Sincerely,

Lauren Riplinger, JD
Chief Public Policy & Impact Officer