August 8, 2023

Submitted via the Federal eRulemaking Portal: http://www.regulations.gov

The Honorable Lina M. Khan
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Health Breach Notification Rule, Project No. P205405

Dear Chairwoman Khan:

The College of Healthcare Information Management Executives (CHIME) respectfully submits our comments to the Federal Trade Commission (FTC or Commission) in response to the Notice of Proposed Rulemaking to amend the Health Breach Notification Rule (the "HBN Rule" or the "Rule"), as published in the *Federal Register* on June 9, 2023 (Vol. 88, No. 111).

Background

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs) and other senior healthcare IT leaders. With over 5,000 members, CHIME provides a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate; exchange best practices; address professional development needs; and advocate for the effective use of information management to improve the health and healthcare in the communities they serve.

Summary

The Commission's HBN Rule[1] requires vendors of personal health records ("PHRs") and related entities that are not covered by the Health Insurance Portability and Accountability Act ("HIPAA") to notify individuals, the FTC, and, in some cases, the media of a breach of unsecured personally identifiable health data. As part of a regular review of Commission rules, the FTC in 2020 sought comment on whether changes were needed to the HBN Rule. In September 2021, the FTC issued a policy statement affirming that health apps and connected devices that collect or use consumers' health information must comply with the Rule.

CHIME has continued to advocate directly for the expansion of the personal health record definition and for the utilization of the FTC enforcement authority in prior comments to the Health Breach Notification Regulatory Review; request for public comment.

CHIME has consistently supported the FTC's efforts to protect consumer's health information. Specifically, we applauded the Commission's Policy Statement *On Breaches by Health Apps and Other Connected Devices* issued on September 15, 2021.[2] This Policy Statement provided much needed clarity and

[1] Federal Trade Commission's Health Breach Notification Rule, 16 C.F.R. Part 318
[2] Federal Trade Commission. (September 15, 2021). Statement of the Commission: On Breaches by Health Apps and Other Connected Devices [Policy Statement].

recognition of the FTC's authority under the HBN Rule[1] as a result of the proliferation of apps and connected devices that capture sensitive health data. It further provided that under the Rule's requirements, vendors of personal health records ("PHR") and PHR-related entities must notify U.S. consumers and the FTC, and, in some cases, the media, if there has been a breach of unsecured identifiable health information, or face civil penalties for violations.

The FTC acknowledged – nearly two years ago – in the Policy Statement that the Commission "has never enforced the Rule, and many appear to misunderstand its requirements." Therefore, in issuing the Policy Statement, it served "to clarify the scope of the Rule, and place entities on notice of their ongoing obligation to come clean about breaches." **Today, we applaud the FTC for prioritizing and protecting the privacy and security of personal health data, which has brought several cases involving the misuse of consumers personal health data, including two enforcement actions that alleged HBN Rule violations.[2][3]**

Key Recommendations

In our comments, CHIME provides responses to address the proposals included in this Notice of Proposed Rulemaking (NPRM). We believe that the following areas are especially important for the Commission to consider when finalizing the provisions in this important proposed rule, and our detailed recommendations are included below.

The Commission's HBN Rule requires vendors of personal health records ("PHRs") and related entities that are not covered by the Health Insurance Portability and Accountability Act ("HIPAA") to notify individuals, the FTC, and, in some cases, the media of a breach of unsecured personally identifiable health data. **CHIME appreciates that the Commission has thoroughly clarified via numerous guidance documents and the Policy Statement that the Rule does not apply to HIPAA-covered entities (e.g., hospitals and doctor's offices). HIPAA-covered entities (CEs) and those that act only as a HIPAA business associate (BA) have existing legal responsibilities that are in the Health and Human Services (HHS) Breach Notification Rule.[6]**

As many Americans turn to apps and other technologies to track diseases, diagnoses, treatment, medications, fitness, fertility, sleep, mental health, diet, and other vital areas, this Rule is more important than ever. Consumers as patients can use both mobile medical apps and mobile apps to manage their own health and wellness, such as to monitor their caloric intake for healthy weight maintenance, while other apps are created to help healthcare providers improve and facilitate patient care.[4] Entities not covered by HIPAA offering these services should take appropriate care to secure and protect consumer data. **CHIME believes it is time for vendors of PHR and PHR-related entities with lax data security – and sometimes blatant disregard of the law – of their ongoing obligation to be transparent about breaches and unauthorized disclosures under the Rule.**

Detailed Recommendations

The FTC is proposing to revise the Rule, 16 CFR part 318, in seven ways.

The Commission is proposing to revise several definitions in order to clarify the Rule and better explain its application to health apps and similar technologies not covered by HIPAA. Consistent with this objective, the

https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf

[1] Federal Trade Commission's Health Breach Notification Rule, 16 C.F.R. Part 318

[2] *FTC proposes amendments to strengthen and modernize the Health Breach Notification Rule*. (2023, June 12). Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-proposesamendments-strengthen-modernize-health-breach-notification-rule

[3] CFR §§ 164.400-414

[4] *Device Software Functions Including Mobile Medical Applications*. (2022, September 29). U.S. Food And Drug Administration. https://www.fda.gov/medical-devices/digital-health-center-excellence/device-software-functionsincluding-mobile-medical-applications

proposed Rule would modify the definition of “PHR identifiable health information” and add two new definitions (“health care provider” and “health care services or supplies”). To ensure that entities covered by the Rule understand their obligations under the Rule, the Commission is proposing changes to clarify that mobile health applications are covered by the Rule, giving important guidance to the marketplace on the Rule’s scope. The FTC is also proposing a new definition for the term ‘‘health care services or supplies’’ to include 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 FTC is proposing to revise the definition of breach of security to clarify that a breach of security “includes an unauthorized acquisition of PHR identifiable health information in a personal health record that occurs as a result of a data security breach ***or an unauthorized disclosure*** [emphasis added].”

Additionally, the Commission is proposing to revise the definition of PHR related entity in two ways. Consistent with its clarification that the Rule applies to health apps, the FTC is proposing to clarify the definition of ‘‘PHR related entity’’ to make clear that the Rule covers entities that offer products and services through the online services, including mobile applications, of vendors of personal health records. In addition, the Commission is proposing to revise the definition of ‘‘PHR related entity’’ to provide that 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 – are PHR related entities.

CHIME strongly supports each of these proposals, as they are consistent with our previous public comments supporting the Rule’s coverage of these entities. By adopting these changes, the FTC would fill the gap left by HIPAA regulations and would assist in supporting cross-governmental efforts to empower patients with their health data.

At the same time, these proposed revisions would ensure third-party application developers and the platforms that host those applications would be held to regulatory requirements that better protect individual privacy and health data security**. We have previously and continue to strongly encourage the FTC to push further into this space by utilizing and enforcing the clear, concise and existing authority under the Rule to hold non-HIPAA covered third-parties (i.e., vendors of PHR and PHR-related entities) responsible when they illegally disclose – intentionally or not – covered information.**

Further, by focusing on the type of data (content), as opposed to how the data is stored or where a consumer may access it (modality), the FTC is providing assurance that new technologies only now being introduced – or not even yet developed – will be captured by either HIPAA or the HBN Rule. In turn, this helps ensure privacy and security remain a cornerstone of health care technology development and innovation, as well as in the future.

CHIME believes that these proposals, coupled with actions from the FTC, will make consumer data more secure and help ensure that those entities who are entrusted with crucial private data are held accountable. Not only does it hold bad and unsecure actors accountable, but it also creates a disincentive that urges all businesses with PHR and PHR-related entities to strengthen their data security practices. As one of only a handful of federal privacy laws protecting consumers’ health information, the HBN Rule plays a vital role in holding companies accountable for how they disclose consumers’ sensitive health information. We believe that these proposed changes would give the FTC the welcomed authority to fully enforce the Rule – and CHIME looks forward to a final rule cementing these policies as legal requirements.

The FTC is seeking comment as to whether the proposed changes sufficiently clarify the Rule’s application to developers and purveyors of products that have the technical capacity to draw information from more than one source. **CHIME believes that it does.** Additionally, the Commission is inviting comment on its interpretation that an app is a personal health record because it has the technical capacity to draw information from multiple sources, even if particular users of the app choose not to enable the syncing features. **CHIME supports this proposed interpretation.**

CHIME agrees and appreciates with the FTC that this proposal would make clear that the HBN Rule covers online services related not only to medical issues (by including in the definition terms such as ‘‘diseases, diagnoses, treatment, medications’’) but also wellness issues (by including in the definition terms such as fitness, sleep, and diet).” **CHIME applauds the Commission for their intention to ensure app developers understand their notice obligations, even if an app is positioned as a “wellness” product rather than a “health” product. Our members take the protection of their patients’ healthcare data as not only a legal obligation, but their mission. Patient data safety is crucial for maintaining trust in the patient-provider relationship; ensuring that patient data remains safe even when they are outside of the four walls of the hospital or other healthcare setting only helps strengthen that bond.**

The Commission is requesting comment on the proposal that the HBN Rule’s application would be straightforward: either the app has the technical means (e.g., the application programming interface or API) to draw information from multiple sources, or it does not. Additionally, CHIME agrees with the Commission that adding the phrase “technical capacity to draw information” would clarify that a product is a PHR if it can draw any information from multiple sources, even if it only draws health information from one source. **If an app or other product draws any health information from anywhere, CHIME believes that it should be considered PHR.**

The FTC is also requesting comment about whether the “proposed bright-line rule” – that is, apps with the ‘‘technical capacity to draw information’’ are covered – should be adjusted to take into account consumer use, such as where no consumers (or only a de minimis number) use a feature. **CHIME supports the “proposed bright-line rule” and believes that it should be finalized as proposed, without adjustment. It would be extremely burdensome and challenging for the FTC to consistently and accurately gauge and monitor consumer use of every individual application’s features.**

Additionally, consistent with the Recovery Act definition, the Policy Statement, FTC enforcement actions under the Rule, and public comments received, the Commission is proposing to amend the definition of “breach of security”[5] by adding the following sentence to the end of the existing definition: “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.”

The proposed definition is intended to make clear to the marketplace 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. **CHIME strongly supports these proposals.**

In response to public comments expressing concern that mailed notice is costly and not consistent with how consumers interact with online technologies like health apps, the Commission is proposing to revise the Rule to authorize electronic notice in additional circumstances. Specifically, the proposed Rule would adjust the language in the ‘‘method of notice section’’ and add a new definition of the term ‘‘electronic mail.’’ **CHIME supports these proposals.**

FTC is also proposing to require that any notice delivered by electronic mail be ‘‘clear and conspicuous,’’ a newly defined term, which aligns closely with the definition of ‘‘clear and conspicuous’’ codified in the FTC’s Financial Privacy Rule. **CHIME supports this proposal.** Among other things, for a notice to be clear and conspicuous, the FTC is proposing that it must be reasonably understandable and designed to call attention to the nature and significance of the information in the notice. **CHIME believes that clarity is key and consistency is crucial when it comes to privacy regulations, and appreciates this proposal.**

CHIME is supportive of the FTC’s approach to revise the ‘‘method of notice section’’ and to structure the breach notification in two parts in order to increase the likelihood that consumers encounter the notice. We also support the proposals which expand the required content that must be provided in the notice to consumers. As part of relaying what happened regarding the breach, the Commission is proposing that the notice to individuals also include a brief description of the potential harm that may result from the breach, such as medical or other identity theft. **CHIME strongly supports this proposal and**

[5] § 318.2(a)

agrees with the FTC's belief that it is important that notifying entities explain to individuals not only the steps individuals should take to protect themselves from potential harm resulting from the breach, but also what steps the notifying entity is taking to protect affected individuals following the breach or unauthorized disclosure.

The Commission asserts that: "Any protections offered by notifying entities likely will be tailored to the facts and circumstances of each breach and could, in certain circumstances, include credit monitoring or other support such as identity theft protection or identity restoration services." CHIME believes that there is more that can be done before a consumer's data is sold or a breach happens, and we encourage the FTC to enforce real-world and stringent privacy and security protections on companies to better protect consumer data. That includes making sure consumers understand what they are agreeing to prior to using a company's technology.

CHIME applauds the FTC for utilizing and clarifying its existing authority to protect American consumers and patients who are often unaware of how their data is being used, and in some cases, may be under the false impression that it is still safeguarded under HIPAA. Clear, transparent communication to consumers about how, when, and what PHR identifiable health information has been breached or disclosed without their authorization is critical.

Conclusion

In closing, we would like to thank the FTC for providing the opportunity to comment on this important Notice of Proposed Rulemaking (NPRM). CHIME looks forward to continuing to support the Commission in its efforts to implement policies to protect consumers. We have long stood as staunch supporters of all efforts in both Congress and the federal agencies that ensure patient data stays secure and is never compromised in a way that could jeopardize patient care or trust in the American healthcare system. We will continue to support new and continued efforts to build on these important policies.

CHIME appreciates the chance to help inform the important work being done by the Commission. We look forward to continuing to be a trusted stakeholder and resource to the FTC and continuing to deepen the long-standing relationship we have shared.

Should you have any questions or if we can be of assistance, please contact Chelsea Arnone, Director, Federal Affairs at carnone@chimecentral.org.

Sincerely,

Russell P. Branzell, CHCIO, LCHIME
President and CEO
CHIME