August 18, 2020

Honorable April J. Tabor, J.D.
Acting Secretary
Federal Trade Commission
7th Street SW
Washington, D.C. 20024

Re: Health Breach Notification Rule, 16 CFR part 318, Project No. P205405

Submitted electronically at: https://www.federalregister.gov/documents/2020/05/22/2020-10263/health-breach-notification

Ms. Tabor:

The American Medical Informatics Association (AMIA) appreciates the opportunity to submit comments regarding the Federal Trade Commission's (FTC) Health Breach Notification Rule 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.

We thank the FTC for establishing this review process and requesting comments on the Health Breach Notification Rule (HBN Rule). The HBN Rule's underlying premise is to make health breaches of non-HIPAA covered entities (NCEs) publicly known.[1] This is an important supplemental to HIPAA's Breach Notification Rule,[2] especially due to the dramatic expansion of health data generated across both clinical systems and consumer devices, and the rapid adoption of

[1] Herein we refer to NCEs as being equivalent to both the terms established by the HITECH Act and FTC regarding PHRs and PHR related entities, as well as "mHealth technologies" and "health social media," described in a report by the HHS Office of the National Coordinator for Health IT, "Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA" (2016). mHealth technologies include entities that collect or deal in PHRs and cloud-based or mobile software tools that intend to collect health information directly from individuals and enable sharing of such information, such as wearable fitness trackers. Health social media includes internet-based social media sites on which individuals create or take advantage of specific opportunities to share their health conditions and experiences. Taken together, these mHealth technologies and health social media that are outside the scope of HIPAA are referred to as "non-covered entities" or NCEs.

[2] 45 CFR §§ 164.400-414

standard application programming interfaces (APIs) meant to provide individuals with better access to their health data through mobile and web-based applications (apps).

However, we are deeply concerned that the HBN Rule is structurally flawed given that the FTC has received only three notices of breaches involving 500 or more individuals in the last ten years.[3] The legislative definitions established by the HITECH Act of 2009,[4] and subsequent definitions established by the FTC[5] are ill-suited to the current and emerging ecosystem of consumer health apps. "Personal health records" (PHRs), "PHR identifiable health information," and "PHR related entity" portend elements of an ecosystem that never developed. Hence, we are concerned that the HBN Rule has not adequately ensured accountability for actors of the ecosystem that has developed.

While we are cognizant of the limitations imposed by the HITECH Act definitions, we recommend the FTC take near-term action and develop guidance that:

1. Explicitly includes usernames / passwords maintained by an NCE as being considered PHR identifiable health information, thus subject to the HBN Rule if breached; and
2. Expand on the concept of "unauthorized access" under the definition of "Breach of security,"[6] 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.

These steps should be within purview of current FTC powers and jurisdiction. The first will better reflect how traditional breaches occur in an app-led (as opposed to a PHR-led) ecosystem, by recognizing that breaches will be of individuals' accounts rather than a company's database of individually identifiable health information. The second recommendation is meant to provide warning to apps that provide inadequate transparency into data use, reuse, and exchange, especially those apps that engage in myriad data transfers under umbrella terms of service (ToS) agreements. AMIA's Health Data Privacy Principles, firmly states: "Informed consent requires clearly worded, understandable explanations of how an individual's health data will be used and the circumstances in which it will be disclosed; a commercial application Terms of Service agreement is not equivalent to, nor a substitute for, informed consent."[7] We expand below, but this kind of "data syphoning," when apps share health data without individuals' knowledge or express consent, is among the greatest threats to consumer safety posed by our emerging app ecosystem.

Beyond these concrete steps, AMIA recommends that additional policy development be considered by HHS, Congress, and the FTC to achieve the following goals:

---

[3] Breach Notices Received by the FTC. Available at: https://www.ftc.gov/system/files/documents/rules/health-breach-notification-rule/breach_notices_received_by_the_ftc.pdf

[4] *Public Law 111-5, 123 Stat. 115 (2009).*

[5] FTC HBN Rule. 16 CFR part 318

[6] 16 CFR 318.2(a)

[7] Health Data Privacy. AMIA Privacy Principles. Available at: https://www.amia.org/sites/default/files/AMIA-2020-Policy-Priorities.pdf#page=21

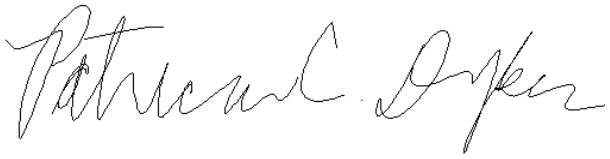
August 18, 2020

- Expand the purview of the HBN Rule to include technology beyond PHRs, include 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;
- Ensure the HBN Rule 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.

The landscape for health data is evolving rapidly, underpinned by APIs and a growing ecosystem of apps generating new kinds of health data and delivering new kinds of consumer-facing services. The FTC has an opportunity to reorient the HBN Rule to account for this evolution, and it has an obligation to promote and enforce consumer protections commensurate with consumers' expectations.

Below we provide rationale and examples to support our recommendations. We hope our comments are helpful as you review the applicability and utility of the HBN Rule. Should you have questions about these comments or require additional information, please contact Jeffery Smith, Vice President of Public Policy at jsmith@amia.org or (301) 657-1291. We look forward to continued partnership and dialogue.

Sincerely,



Patricia C. Dykes, PhD, RN, FAAN, FACMI
Chair, AMIA Board of Directors
Program Director Research
Center for Patient Safety, Research, and Practice
Brigham and Women's Hospital

Enclosed: AMIA Comments to Health Breach Notification Rule, 16 CFR part 318, Project No. P205405

August 18, 2020

Concerns of under-notification

As stated previously, we were surprised to learn that the FTC has received only three notices of breaches involving 500 or more individuals in the last ten years.[8] We note that the FTC views consumer protections outside The FTC identifies three reasons for so few notices:

1. Commission has predominantly received notices about breaches affecting fewer than 500 individuals;[9]
2. Most PHR vendors, related entities, and service providers have been HIPAA-covered entities or "business associates" subject to HHS's rule;[10] and
3. The HBN Rule does not apply to health information secured through technologies specified by HHS[11] (i.e. data encrypted at rest and in motion according to NIST).[12,13]

While we see these as valid reasons an NCE would forego notice to the FTC, we are concerned about the potential for widespread under-notification of health breaches due to:

- Structural flaws in HBN Rule definitions;
- Increasing prevalence of data syphoning among NCEs; and
- Difficulty faced by consumers who wish to report breaches.

Structural flaws in HBN Rule definitions

First, we note that to activate the HBN Rule, PHR identifiable health information needs to be exposed. PHR identifiable health information is defined similarly to "protected health information" under HIPAA, while pertaining to NCEs. While exposure of PHR identifiable health information is serious, most breaches will involve usernames/passwords or other information that will enable subsequent abuse of an individual's health data. We are unclear if the FTC treats exposure of usernames/passwords as a breach under the HBN Rule because these datatypes are not explicitly health related. We note that most breaches of apps will be of this nature, rather than result in troves of ECGs being stolen.

For example, the misconfiguration of a popular mobile app development platform, known as Firebase, was found to expose sensitive information from more than 4,000 Android apps in March 2020. This information included passwords, telephone numbers, and chat messages.[14] Nearly 10,000 apps were inappropriately allowing data in the apps to be modified by potential attackers and 4,282 apps were leaking sensitive information. It has been estimated that more than 1.5 million apps were using the Firebase platform, across Android and iOS, in March 2020, including a high likelihood that

[8] Breach Notices Received by the FTC. Available at: https://www.ftc.gov/system/files/documents/rules/health-breach-notification-rule/breach_notices_received_by_the_ftc.pdf
[9] 85 FR 31085 Available at: https://www.federalregister.gov/d/2020-10263/p-14
[10] 85 FR 31085 available at: https://www.federalregister.gov/d/2020-10263/p-17
[11] 85 FR 31085 available at: https://www.federalregister.gov/d/2020-10263/p-17
[12] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
[13] https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html
[14] https://www.forbes.com/sites/daveywinder/2020/05/12/revealed-4000-android-apps-expose-millions-of-passwords-phone-numbers-and-messages/#31eefaf7438d

among those users were health apps who generate health data. In another example, Under Armour's MyFitnessPal was breached in 2018,[15] compromising more than 150 million accounts. While the Under Armour breach was widely reported, it unclear why notice of this breach was not through the HBN Rule.

Data Syphoning

Second, the rising phenomenon of data syphoning, was not contemplated in the HITECH Act or subsequent regulation. Data syphoning occurs when applications (apps) share health data without individuals' knowledge or consent. Recent research has sought to understand how user data are shared by top rated health apps and to characterize privacy risks to app users, both clinicians and consumers, finding that sharing of user data is routine, yet far from transparent.[16] Seventy-nine percent of sampled apps shared user data and 55 unique entities, owned by 46 parent companies, received or processed app user data, including developers and parent companies (and service providers.[17] Similar circumstances have been well documented by news and media outlets.[18] At issue with this phenomenon is the lack of express consent and the pervasive use of terms of service agreements to provide blanket cover for any and all data transfers – current and future.

Consumer-led reporting

Beyond definitions, another source of concern is that notices received by the FTC are designed to come from businesses who have been breached,[19] rather than 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.[20] This is problematic given what we know about health social media. 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.[21] However, it was not Facebook that discovered and notified users, it was the users themselves. This consumer-led reporting to the FTC

[15] https://www.cnbc.com/2018/03/29/under-armour-stock-falls-after-company-admits-data-breach.html
[16] Q Grundy Q, Chiu K. et al. Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. BMJ 2019;364:l920 https://www.bmj.com/con.tent/364/bmj.l920
[17] Ibid.
[18] Harwell D. Is your pregnancy app sharing your intimate data with your boss?. Washington Post. April 10, 2019. https://www.washingtonpost.com/technology/2019/04/10/tracking-your-pregnancy-an-app-may-be-more-public-than-you-think/?utm_term=.06d4c3edf544
[19] FTC Health Breach Notification Form. Available at: https://www.ftc.gov/system/files/documents/plain-language/2017_5_2_breach_notification_form.pdf
[20] FTC Complaint Assistant. https://www.ftccomplaintassistant.gov/#crnt&panel1-1
[21] 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-cancer-privacy-loophole.html. 1 Aug 2018.

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

did not make the list of breaches, nor is it clear that user-reporting had its intended impact of changing Facebook's behavior.[22]

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

In addition to the reasons cited by the FTC, we strongly believe the structural flaws of misaligned definitions, increasing prevalence of data syphoning, and the inability of consumers to report breaches, are contributing to widespread underreporting. This, in turn, is compromising the consumer protections at the core of the HBN Rule. Consumers expect that the FTC is working to promote and enforce consumer protections and the approach taken with this rule creates pro-business activity / supports pro-business activity that is at odds with consumers' expectations.

[22] 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.
[23] Kelion, L. Babylon Health admits GP app suffered a data breach. BBC News. https://www.bbc.com/news/technology-52986629 9 June 2020.

AMIA | American Medical Informatics Association
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814