August 20, 2020

Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue NW
Suite CC-5610 (Annex B)
Washington, District of Columbia 20580

RE: *Federal Trade Commission Review of Health Breach Notification Rule*

ACT | The App Association's Connected Health Initiative (CHI)[1] appreciates the opportunity to provide input to the Federal Trade Commission (FTC) on whether changes should be made to a the Health Breach Notification Rule, which requires vendors of personal health records 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.[2]

CHI is the leading advocate for digital health policy and law advancements, representing a broad consensus of stakeholders across the healthcare and technology sectors. Our mission is to support the responsible and secure use of connected health innovations throughout the continuum of care to improve patients' and consumers' experiences and health outcomes. CHI is a long-time active advocate for the increased use of innovative technology in the delivery of healthcare and engages with a broad and diverse cross-section of industry stakeholders focused on advancing clinically validated digital medicine solutions.

CHI shares your commitment to advancing responsible health data stewardship and privacy throughout the continuum of care and recognizes that no data is more personal to Americans than their health data. CHI members acknowledge that significant threats to Americans' most sensitive data continue to evolve and put extensive resources into ensuring the security and privacy of health data to earn the trust of consumers, hospital systems, and providers. Breach notification requirements generally serve important functions. They not only notify the individual when their information has been

[1] http://www.connectedhi.com/.

[2] https://www.ftc.gov/news-events/press-releases/2020/05/ftc-seeks-comment-part-review-health-breach-notification-rule.

compromised, but they also provide insight into security issues that organizations may be facing.

However, digital health innovators do struggle to navigate the complex environment with respect to cybersecurity and privacy as they contend with HIPAA requirements at times and relevant FTC requirements at others, on top of state-specific requirements that can vary significantly.

As the FTC notes, it only lists two breaches of 500 or more individuals since this rule was put into place 10 years ago.[3] The FTC also notes that it never enforced its health data breach rules because "as the PHR [personal health record] market has developed over the past decade, most PHR vendors, related entities, and service providers have been HIPAA-covered entities or 'business associates' subject to HHS's rule."[4] This data indicates that most PHRs are subject to HIPAA with FTC health data breach rules governing the relatively few that are not.

Ultimately, CHI supports (and is currently leading efforts related to) the development of a new cross-sectoral privacy framework by Congress in the form of a general privacy bill that is intended to result in general privacy legislation. As part of such a solution, we support the proposition that any such general privacy bill treat health data as a subclass of "sensitive" personal information subject to heightened regulatory requirements, including with respect to breach notification requirements.

Until that time, innovators in the digital healthcare ecosystem will have to carefully navigate the different scopes and contexts of federal sector-specific laws and regulations. They will further have to continue to dedicate resources to tracking and complying with the range of state data breach laws and regulations, some of which conflict or overlap with FTC health data breach notification rules.

Building on the above, CHI offers the following views in response to various questions posed by FTC:

- We support Section 318.1 of the rule's providing that FTC health breach notification rules do not apply to HIPAA-covered entities or to any other entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity. We believe this bright line is critical and should be maintained to provide legal certainty to digital healthcare innovators.

[3] Health Breach Notification, 85 FR 31085 (May 22, 2020) (HBR RFI).

[4] *Id*. CHI also notes that thousands of breaches of HIPAA-covered impacting 500 or more patients have been reported over the years. *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

- CHI does agree that, “as consumers turn towards direct-to-consumer technologies for health information and services (such as mobile health applications, virtual assistants, and platforms’ health tools), more companies may be covered by the FTC’s Rule.”[5] Developers of technology already subject to the FTC’s general consumer protection authority are, and will continue, inventing third-party apps that utilize consumer health information and will likely meet the definition of a PHR provider.
- CHI supports FTC evolving the requirements of notification in Section 318.5 of the rule. As the FTC notes, in-app messaging, text messages, and platform messaging are tools available today that are used widely and should be allowed to be utilized to more effectively communicate with consumers that consent to it. It is common sense that consumers should be able to consent to receiving communications under the rule via these modalities as well as email.
- FTC can reduce costs and burdens on small businesses by developing explanatory resources clearly explaining the purpose and requirements of the health data breach notification rule and offering guidance on compliance with it. We note that CHI has collaborated closely with the Department of Health and Human Services’ Office of Civil Rights on the development of its HIPAA portal for developers.[6] CHI offers to partner with FTC in the creation of such a resource, which would ease compliance burdens and reduce costs.

[5] HBR RFI at 31086.

[6] https://hipaaqsportal.hhs.gov/.

CHI thanks you in advance for your time and consideration of the input above.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Connected Health Initiative
1401 K St NW (Ste 501)
Washington, DC 20005
p: +1 517-507-1446
e: bscarpelli@actonline.org

The Connected Health Initiative (CHI), an initiative of ACT | The App Association, is the leading multistakeholder spanning the connected health ecosystem seeking to effect policy changes that encourage the responsible use of digital health innovations throughout the continuum of care, supporting an environment in which patients and consumers can see improvements in their health. CHI is driven by the its Steering Committee, which consists of the American Medical Association, Apple, Bose Corporation, Boston Children's Hospital, Cambia Health Solutions, Dogtown Media, George Washington University Hospital, HIMSS, Intel Corporation, Kaia Health, Microsoft, Novo Nordisk, The Omega Concern, Otsuka Pharmaceutical, Podimetrics, Rimidi, Roche, United Health Group, the University of California-Davis, the University of Mississippi Medical Center (UMMC) Center for Telehealth, the University of New Orleans, and the University of Virginia Center for Telehealth.

For more information, see www.connectedhi.com.