Published on *The National Law Review* https://natlawreview.com

Entities of All Types Should Consider Commenting on the FTC's Health Breach Notification Rule by August 20, 2020

Article By:

Iliana L. Peters

Jane P. Dennis

On May 22, 2020, the Federal Trade Commission (the "FTC") published its decennial request for public comment (the "RFC") on the FTC's Health Breach Notification Rule (the "HBN Rule").[1] The HBN Rule applies to vendors that maintain electronic personal health records ("PHRs"), but that are not regulated by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy, Security, and Breach Notification Rules (the "HIPAA Rules"). Companies covered by HIPAA or the HBN Rule, and those that are not covered by either, should review the RFC and consider submitting comments for purposes of contributing to the discussion on breach notification requirements at both the state and federal level.

The HBN Rule and the HIPAA Rules

In 2009, the Department of Health and Human Services ("HHS") drafted the HIPAA Breach Notification Rule while the FTC drafted the HBN Rule, pursuant to sections 13402 and 13407 of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), respectively. HHS and the FTC worked closely to conform the requirements under both jurisdictions given that the rules were intended to be complimentary for entities dealing with similar PHRs.[2]

The HBN Rule requires vendors of electronic PHR and PHR-related entities that are not subject to the HIPAA Rules to provide notice without unreasonable delay and in no case later than sixty calendar days after discovery of a breach to each affected U.S. citizen, the FTC, and in some cases, the media.[3] The HIPAA Breach Notification Rule imposes the same time standard for breach notification to individuals by HIPAA covered entities, with notification also required to be provided to HHS and, in certain cases, the media.[4]

The FTC's HBN applies to "personal health records" (an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual), while the HIPAA Rules pertain to the broader term of "protected health information" (individually identifiable information, with certain exceptions).[5]

As is the case with business associates ("BAs") under HIPAA, the HBN Rule requires third party

service providers, PHR vendors, and PHR-related entities to provide notification to such vendors following the discovery of a "breach of security." Specifically, the HBN Rule states that "[b]reach of security means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual."[6]

In terms of a risk assessment, the HBN Rule provides that unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information *unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information*.[7]

While the HBN Rule's risk assessment considers whether unsecured electronic records of PHR were acquired without authority, HIPAA's risk assessment evaluates whether an individual's unsecured protected health information was compromised, specifically, "an acquisition, access, use, or disclosure of protected health information […] is presumed to be a breach *unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least [four] factors*[.]"[8]

The FTC'S Request for Comment

As a part of its review of the HBN Rule, the FTC published a number of questions, including requests for updates it should consider to account for the health care industry adopting standardized application programming interfaces ("APIs"), that consider expanding the definitions of entities covered by the HBN Rule and about overlap with other breach notification requirements, such as HIPAA. Further, as the FTC noted in its questions, technology advances have come front and center and accelerated during the COVID-19 public health emergency, where patients have been encouraged to use certain technologies instead of having in-person visits for health care services. Important FTC's questions in this regard include:

- What modifications, if any, should be made to the [HBN] Rule to account for changes in relevant technology, economic conditions, or laws? For example, as the health care industry adopts standardized [APIs] to help individuals to access their electronic health information with smartphones and other mobile devices (as required by rules implementing the 21st Century Cures Act 9), will the number of entities subject to the […] HBN Rule increase?

- Are there modifications or changes the [FTC] should make to the [HBN] Rule to address any developments in health care products or services related to COVID–19?

- Does the [HBN] Rule overlap or conflict with other federal, state, or local laws or regulations? If so, how?

- Should the definition of "PHR identifiable health information" in § 318.2(d) be modified in light of technological advances in methods of de-identification and re-identification? If so, how, consistent with the Act's requirements?

- Should the definitions of "PHR related entity" in § 318.2(f), "Third party service provider" in § 318.2(h), or "Vendor of personal health records" in Section 318.2(j) be modified in light of changing technological and economic conditions, such as the proliferation of mobile health applications ("apps"), virtual assistants offering health services, and platforms' health tools? If so, how, consistent with the Act's requirements?

- What are the implications (if any) for enforcement of the Rule raised by direct-to-consumer technologies and services such as mobile health apps, virtual assistants, and platforms' health tools?

Considerations for Commenting

Based on the questions posed, there are key takeaways on potential changes to the FTC's HNB Rule. First, the FTC has taken notice of the prevalence of third party apps that deal with consumer health information, and many of these entities already fall under the FTC's jurisdiction; however, if the scope of the HBN Rule is expanded, there may be an additional affirmative obligation to provide notice in the event of a breach of PHR. As APIs gain traction and more individuals use direct-to-consumer apps to access their health information, this group of vendors may become subject to changes made to the FTC's HNB Rule. Second, HIPAA covered entities, BAs, and all other vendors that deal with PHRs may consider requesting that the FTC coordinate with HHS to ensure there is consistent application of the definition of breach, especially as it relates to a risk assessment. Finally, other companies may want to submit comments as well for the purposes of highlighting conflicting state law requirements related to data breach risk assessments.

Comments to the FTC may be submitted by August 20, 2020 here.

Footnotes

[1] *See* 74 Fed. Reg. 42962 (Aug. 25, 2009).

[2] *See* 78 Fed. Reg. 5566, 5639 (Jan. 25, 2013).

[3] *See* 16 C.F.R. § 318, *et seq.*

[4] *See* 45 C.F.R. § 164.404, *et seq.*

[5] 16 C.F.R. § 318.2(d); 45 C.F.R. § 160.103.

[6] 16 C.F.R. § 318.2(a).

[7] 16 C.F.R. § 318.2(a) (emphasis added).

[8] 45 C.F.R. § 164.402(2) (emphasis added).

National Law Review, Volume X, Number 176