



August 20, 2020

The Honorable Joseph J. Simons  
Chairman  
Federal Trade Commission  
400 7<sup>th</sup> Street, SW  
Washington, DC 20024

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

Submitted electronically via [www.regulations.gov](http://www.regulations.gov)

Dear Chairman Simons:

Thank you for the opportunity to provide comment on the Health Breach Notification Rule, 16 CFR part 318, Project No. P205405.

AHIMA is a global nonprofit association of health information (HI) professionals. AHIMA represents professionals who work with health data for more than one billion patient visits each year. AHIMA's 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 clinicians. Our leaders work at the intersection of healthcare, technology, and business, and are found in data integrity and information privacy job functions worldwide.

Our recommendations regarding certain aspects of the Commission's Health Breach Notification Rule (HBN) can be found below.

### **Changes in Technological and Economic Conditions**

Since the Commission's Health Breach Notification Rule became effective in 2009, use of mobile apps by consumers has rapidly accelerated. In 2018, the Office of the National Coordinator for Health IT (ONC) reported that more than eight in 10 individuals reported owning a tablet or smartphone.<sup>1</sup> Furthermore, according to Accenture's 2018 Consumer Survey on Digital Health, nearly half of healthcare consumers use mobile/tablet apps, compared to 16 percent in 2014.<sup>2</sup> At the same time, both the Office of the National Coordinator for Health IT (ONC) and the Centers for Medicare and Medicaid Services (CMS) seek to empower consumers by improving access to their data through modern technical standards and standardized application programming interfaces (APIs) and by fostering "an app economy that provides patients with innovation and choice."<sup>3</sup> Given these technological and policy advancements, we anticipate that the number of entities subject to the Commission's HBN Rule will increase. However, the

---

<sup>1</sup> Available at: <https://www.healthit.gov/sites/default/files/page/2019-05/Trends-in-Individuals-Access-Viewing-and-Use-of-Online-Medical-Records-and-Other-Technology-for-Health-Needs-2017-2018.pdf>.

<sup>2</sup> Available at: <https://www.accenture.com/us-en/insight-new-2018-consumer-survey-digital-health>.

<sup>3</sup> Available at: <https://www.healthit.gov/curesrule/final-rule-policy/empowering-patients-us-health-care-system>.

extent to which such mobile apps are covered by the HBN Rule is somewhat unclear based on the Commission's existing guidance. AHIMA believes the definitions of a "personal health record" at §318.2(d) and "vendor of personal health records" in §318.2(j) are sufficiently broad to encompass many of these types of existing and/or emerging technologies. However, the Commission's guidance on its website today frequently refers to PHRs and vendors of PHRs as "online services" and "web-based businesses" that offer "web-based apps."<sup>4</sup> Nor does the guidance reference the Commission's own [Mobile Health Apps Interactive Tool](#) which provides assistance to app developers who want to understand their responsibilities under federal laws. **To improve understanding by stakeholders as to whether the HBN Rule applies to mobile apps, we recommend the HBN guidance be updated and clarified to account for these technologies and related standards. Furthermore, we also recommend that the Commission consider updating the existing definition of a "PHR-related entity" at §318.2(f) as §318.2(f)(1) and §318.2(f)(2) appear to focus primarily on products and services offered through a vendor's website and may not be entirely reflective of today's environment as new platforms and related services are increasingly deployed and adopted.**

### **§318.1: Purpose and Scope**

§318.1 stipulates that the HBN Rule does not apply to HIPAA-covered entities or other entities to the extent that it engages in activities as a business associate of a HIPAA-covered entity. The limitations imposed in §318.1 has helped to make clear where application of the HBN Rule ends and the HIPAA Breach Notification Rule begins. **Expanding the scope of §318.1 to include HIPAA-covered entities and the business associates of a HIPAA-covered entity would be duplicative and unduly burdensome given that the HIPAA Breach Notification Rule already imposes similar breach notification provisions to such entities. For that reason, we recommend that the Commission maintain the HBN Rule's current scope in §318.1.**

### **Application of Definition of a Breach**

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 has reliable evidence demonstrating that there has not been, or could not reasonably have been unauthorized acquisition of such information."<sup>5</sup> Conversely, HIPAA's Breach Notification Rule presumes that "an impermissible use or disclosure of protected health information is a breach unless the covered entity or business associate 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."<sup>6</sup> This variance can prove operationally challenging for HIPAA-covered entities and business associates that may deal with personal health records. **We recommend the Commission work with HHS to ensure the consistent application of the definition of breach, particularly as it relates to risk assessments.**

---

<sup>4</sup> Available at: <https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule>.

<sup>5</sup> 16 CFR § 318.2(a).

<sup>6</sup> Available at: <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>.

## Overlap of State Laws

State laws and regulations that overlap or conflict with the HBN Rule can lead to confusion for consumers and entities that operate PHRs across state lines. For example, the risk of harm standard varies between states and in certain circumstances conflicts or overlaps with the HBN Rule.<sup>7</sup> **AHIMA recommends that the Commission be cognizant of such overlapping and conflicting laws and continue to work with states to limit such confusion.**

We appreciate the opportunity to submit comments on the Commission's Health Breach Notification Rule. Should you or your staff have any additional questions or comments, please contact Lauren Riplinger, Vice President, Policy & Government Affairs at [lauren.riplinger@ahima.org](mailto:lauren.riplinger@ahima.org) and (202) 839-1218.

Sincerely,



Dr. Wylecia Wiggs Harris, PhD, CAE  
Chief Executive Officer  
AHIMA

---

<sup>7</sup> Cal. Civ. Code § 1798.80 *et seq.*; Ga. Code § 10-1-910 *et seq.*; Ariz. Rev. Stat. § 18-551 *et seq.*; 815 Ill. Comp. Stat. 530/5 *et seq.*