August 20, 2020

The Honorable Joseph J. Simons
Chairman
U.S. Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

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

Dear Chairman Simons:

On behalf of the over 80,000 members of the American College of Surgeons (ACS), we appreciate the opportunity to submit comments to the Federal Trade Commission (FTC) Health Breach Notification (HBN) Rule proposed rule published in the Federal Register on May 22, 2020.

The ACS is a scientific and educational association of surgeons founded in 1913 to improve the quality of care for the surgical patient by setting high standards for surgical education and practice. The ACS supports the FTC’s efforts to update its privacy and security standards to ensure patients are aware when their personal health record (PHR) information is accessed or acquired inappropriately, and we appreciate the opportunity to comment. As the use of direct-to-consumer technology continues to become commonplace in the management of patient conditions, the ACS believes it is important to keep patients’ identifiable health information safe, without stifling innovation. Our responses to a number of specific questions the FTC posed in the HBN Request for Comment are included below.

Questions

1. Does the Rule accomplish the Recovery Act’s goal of advancing the use of health information technology while strengthening the privacy and security protections for health information?

Pursuant to the American Recovery and Reinvestment Act of 2009 (Recovery Act), the FTC issued the Health Breach Notification (HBN) Rule that created certain protections for Personal Health Records (PHRs),
or electronic records of identifiable health information that can be drawn from multiple sources and that are managed shared, and controlled by or primarily for the individual. Because vendors of PHRs and PHR-related entities were collecting consumers’ health information, but were not subject to the privacy and security requirements of the Health Insurance Portability and Accountability Act (HIPAA), the Recovery Act directed the FTC to issue a rule requiring PHR vendors, PHR-related entities, and their third-party service providers to provide notification of any breach of unsecured individually identifiable health information.

The ACS believes protecting patient health records and identifiable information is of the highest importance, but without adequate assurances of a universal patient identifier (UPI) and other solutions that track patients across multiple platforms, the continual increase of privacy and security requirements will likely lead to inefficient and overly costly privacy solutions. A UPI or alternative patient matching solution would allow patient information to move between clinicians, patients, payers, in a secure and private manner, while also guaranteeing that the correct data are being exchanged for the correct patient. A patient matching solution would also be beneficial in the instance of a data breach or hack, because it would allow for a streamlined identification of those whose data had been compromised.

2. What benefits and costs has the Rule imposed on consumers and businesses, including small businesses?

Securing privacy in a digital world has the features of a never-ending task. Hackers seek to breach constantly, some with the threat of openly revealing personal information or holding institutions for ransom. Updating systems to meet the necessary privacy and security requirements can impose great costs on technology vendors, and these perpetual updates can add significant costs to businesses. Ultimately, these costs will be passed down to those utilizing the technology. For example, steps to develop privacy logic, test, implement, and maintain updates to privacy and security software are major expenses that will raise fees paid by consumers. The ACS believes that as the federal government continues to update their privacy and security requirements, possible increased costs on consumers should be considered. The ACS recommends that the agencies work together to develop consistent standards for privacy and security solutions to avoid conflicting and inefficient regulatory requirements across state and federal agencies that would lead to greater resource use by technology developers and associated increase in costs for consumers.
3. What modifications, if any, should be made to the Rule to account for changes in relevant technology, economic conditions, or laws? For example, as the healthcare 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), will the number of entities subject to the Commission’s HBN Rule increase?

As the healthcare industry adopts standardized Application Programming Interfaces (APIs), the use of direct-to-consumer products and third-party applications that allow individuals to access their electronic health information with their personal devices will become increasingly commonplace. Therefore, patients’ PHRs will be stored and managed in many systems that fall within the FTC’s jurisdiction, making a greater number of these entities subject to the FTC HBN.

The ACS believes that if interoperability is going to extend beyond the reach of PHI under HIPAA, it is extremely important that privacy is secured wherever the data are, without hindering the movement of data into knowledge management solutions that will enhance patients’ health and the broader healthcare industry. The College is extremely supportive of privacy and security solutions that allow all patients, but especially patients with various conditions who seek solutions for their ailments or wish to prevent an ailment, to feel comfortable with the security of their PHR when their information is shared through APIs.

As the FTC considers modifying the HBN rule, the ACS recommends that the FTC work with the Office of the National Coordinator for HIT (ONC), the Centers for Medicare and Medicaid (CMS), the Office for Civil Rights (OCR), and the Office of Human Research Protections (OHRP) to carefully reassess regulations that were not created within the scope of the current digital landscape and to ensure there is consistent application of the definition of data breach, especially as it relates to a risk assessment. The ACS also believes it is critical that these agencies work together to create a single solution for protecting PHI and PHR, instead of another system that these entities will be required to comply with. Having differing standards for privacy across agencies and technology-types is extremely inefficient as technology vendors and their business associates must comply with conflicting or overlapping regulations. While the College understands that an overhaul of these longstanding privacy and security regulations will be challenging, at the very least, HHS should aim to eliminate conflicts and duplication across federal and state privacy laws.
In addition, as previously expressed in comments to the ONC and as expressed earlier in this letter, the ACS is concerned about the potential privacy risks posed by enhanced access to personal health information once it moves beyond what is covered under HIPAA and is under the control of vendors and products in the health IT space, including third-party mobile apps. While potentially outside the scope of the FTC’s specific authority, we urge HHS to, in addition to updating data breach regulations, facilitate the development of privacy certification for mobile apps to include clear requirements on how they communicate data use and privacy to users. We encourage HHS to look at the existing FDA process as a model for the certification of mobile health apps.

4. 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?

With increased sharing of PHR and other identifiable health information, patient and stakeholder education is critical. It is imperative that patients have control over and understand the implications of sharing data with third-party entities that are non-covered entities under HIPAA. Patients and stakeholders will need further education about the potential for data to be commercialized or misused in ways that can impact coverage, access to care, and interfere with the physician-patient relationship. Therefore, the ACS recommends that the FTC, in consultation with the ONC, CMS and other federal agencies work together to set parameters for the appropriate use of data by third-party entities, including setting standard terms and conditions to ensure that patients understand what they are agreeing to when consenting to sharing health information—and assisting with public education of stakeholders. The ACS believes that these duties, along with other penalties for improper data sharing, should not fall on the shoulders of physicians, whose clinical practice is already disrupted by multiple mandates and regulatory burdens. Instead, when issues arise, we believe that the responsible party should be those who licensed the applications for use in the healthcare environment, because the licensing organization is responsible for authorizing which data is transferred to the application and who should be able to access the data. They should also ensure that user-friendly authentication tools are incorporated into their software—this could include requiring physicians or other parties trying to access a patient’s identifiable health information to verify their credentials authenticating that they are the proper recipient of the data.

In addition to educating patients, it is also equally important for federal agencies to educate the physician community about new data sharing risks,
as well as what role and obligations the physician has in terms of making
data available, authenticating the identity of requestors of data, and
otherwise authorizing access to data.

5. Should the Rule address any developments in healthcare related to
COVID-19?

The COVID-19 Pandemic required the healthcare industry to make many
adjustments, including the use of alternative communication platforms that
allowed patients to continue meeting with their physicians and other health
care providers virtually. During the COVID-19 Public Health Emergency
(PHE), HHS released temporary provisions for policies related to telehealth
services that refrained from imposing financial penalties for use of non-
HIPAA-compliant platforms, but even with temporary flexibilities allowed
during the PHE, the alternative communication platforms would be
required to notify individuals in the event of a breach. Should these
provisions continue, these platforms would be covered under the FTC’s
jurisdiction.

With the necessary increase in utilization of virtual communication
platforms during the PHE, also came more insight on how virtual care
platforms, such as telehealth, can be better utilized. The current platforms
have shown evidence of constrained functionality issues, where patient or
provider systems cannot adequately connect to each other, therefore
requiring workarounds to effectively communicate. When physicians and
patients must resort to texting, phone calls, or alternative video
conferencing options such as FaceTime, privacy and security issues
become more complex and patients’ health information is much more
vulnerable to being used inappropriately. The ACS believes there is great
opportunity for the technology sector to improve the functionality of
telehealth platforms and solve privacy and security issues so telehealth can
be used more effectively.

In addition to increased utilization of virtual communication platforms,
exposure notification, contact tracing, and symptom tracking applications
are being developed by state health departments and private third-party
technology companies. These applications help patients track exposure to
another person who has tested positive for the virus. While some new
applications are using Bluetooth signals to track exposure without using

The Washington Post. Retrieved by:
personal information and gather data from other sources to ensure privacy for the users, that may not be the case in all new technology due to lack of regulation. New apps may prove to be extremely beneficial in contact tracing and reducing exposure to COVID-19, but may also hold PHR information that could be at risk for breach if inadequate privacy safeguards are implemented. It is important that the FTC ensure that they have considered technologies such as this, when updating the HBN rule.

6. Does the Rule, which does not apply to HIPAA-covered entities or to business associates of a HIPAA-covered entity, support or hinder harmonization with HIPAA?

Please see our response to question #5.

7. 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?

Currently, PHR identifiable health information is defined as “individually identifiable health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and identifies the individual; or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.\textsuperscript{2}” In addition to the entities mentioned in the definition where identifiable patient health information is collected, created, or received—health care provider, health plan, employer, or health care clearinghouse—the ACS recommends considering the addition of clinical data registries, health data warehouses, and data lakes. Registries which deidentify and anonymize patient health information would not require the same assurances for privacy. With increasing interoperability, identifiable patient information will be used to track patients longitudinally with shared clinical data across the health information ecosystem through various APIs. In these instances, secured privacy is essential. We believe that it is important that the government ensures that registries with identifiable patient health information and other tools when used for quality improvement and knowledge management remain covered entities under all updated privacy regulations.

\textsuperscript{2} 16 CFR § 318.2
The ACS appreciates the opportunity to provide feedback on this proposed rule and looks forward to continuing dialogue with CMS on these important issues. If you have any questions about our comments, please contact Jill Sage, Quality Affairs Manager, at jsage@facs.org.

Sincerely,

David B. Hoyt, MD, FACS
Executive Director