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

Some HIPAA Happenings

Article By:

Health Care Practice at Steptoe Johnson

Proposed Modifications to HIPAA Regulations under Consideration

On December 14, 2018, HHS issued its Request for Information on Modifying HIPAA Rules to Improve Coordinated Care as part of its Regulatory Sprint to Coordinated Care initiative. (See 83 Fed. Reg. 64302.) The public comment period ended on February 12th. HHS is seeking comments on ways to modify the HIPAA Rules (*i.e.*, the HIPAA Privacy Rule, the HIPAA Security Rule, and the HIPAA Breach Notification Rule) to "remove regulatory obstacles and decrease regulatory burdens in order to facilitate efficient care coordination and/or case management and to promote the transformation to value-based health care, while preserving the privacy and security of PHI."

HHS has also identified the following four aspects of the HIPAA Privacy Rule for potential modification in order to advance the goals of improving efficient care coordination and/or case management and move toward value-based health care while preserving PHI privacy and security:

- Promote information sharing among covered entities for treatment and care coordination and/or case management;
- Encourage covered entities to share treatment information with family members and caregivers, especially in light of the current opioid crisis;
- Implement the HITECH Act's accounting of disclosure requirement to include treatment, payment, and health care operations disclosures from an electronic health record (EHR) in a way that is both helpful to individuals while also reducing the regulatory burden and disincentives to adopt and use EHRs; and
- Modify and possibly eliminate the requirement that Covered Entities make a good faith effort to obtain written acknowledgments of receipt of their Notices of Privacy Practices.

In its Request for Information, HHS also sought comments on 54 questions within these four issue areas. There is no indication as to if and/or when HHS would propose modifications to the HIPAA Rules following this Request for Information so continued monitoring is important to ensure compliance.

New Cybersecurity Tool for the Health care Industry

On December 28, 2018, HHS released a four-part publication entitled “Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients.” The HICP is the result of a collaborative effort by HHS and the private sector, beginning in May 2017, to develop a voluntary set of cybersecurity principles and practices for the health care sector. While the HICP is a voluntary set of cybersecurity principles and practices, the HICP may establish security standards for the health care industry, which may be taken into consideration in litigation, by policymakers, and by regulators.

The HICP focuses on (a) the five most prevalent cybersecurity threats facing the health care industry including: phishing attacks (*e.g.*, credential theft; malware dropper attacks), ransomware, equipment or data loss or theft, accidental or intentional data loss by organization insiders, and attacks against connected medical devices and (b) ten cybersecurity practices to address those threats including email protection systems, endpoint protection systems, access management, data protection and loss prevention, asset management, network management, vulnerability management, incident response, medical device security, and cybersecurity policies.

The HICP also includes two technical volumes of cybersecurity practices including a technical volume for small health care organizations and a technical volume for medium and large health care organizations. The two technical volumes provide detailed information regarding how these ten cybersecurity practices can be used to mitigate the five key types of cybersecurity threats. The fourth part of the publication includes a compilation of useful cybersecurity resources and templates.

HICP documents are available at the following link: https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx.

HIPAA Enforcement Brisk

HIPAA enforcement continues to be active. On the HHS website, it was reported that, as of December 31, 2018, the Office of Civil Rights (OCR) has received over 197,049 HIPAA complaints and has initiated over 924 compliance reviews since the April 2003 compliance date of the HIPAA Privacy Rules. To the date reported, OCR has also referred 708 cases to the U. S. Department of Justice for criminal investigation. While not all cases investigated resulted in a finding of a violation or resulted in the imposition of penalties, OCR has settled or imposed civil money penalties totaling $96,581,582 during this period; however, in just 2018 alone, OCR reported settlements and judgments totaling $28,683,400, nearly thirty percent (30%) of the total since the 2003 compliance date. The settlements and judgments in 2018 ranged from $100,000 to $16,000,000, with four equaling or exceeding $3,000,000. Thus, given increased enforcement, and the continued threat of cybersecurity attacks, it is a good time to review your policies and practices, and take advantage of the compliance resources provided by HHS such as the tool noted above and, as applicable, to be sure you are in compliance.

National Law Review, Volume IX, Number 91