Nassau Lawyer

JUNE 2017 | VOL. 66 | NO. 10 | WWW.NASSAUBAR.ORG

Increased Enforcement of HIPAA Security Rules

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR), is taking a tough stance on Health Insurance Portability and Accountability Act (HIPAA) violators, and there does not seem to be an end in sight. In 2016, settlements because of OCR's enforcement actions totaled $23.5 million, almost four times higher than the previous year.[1] With an increased focus on health-care entities' treatment of patient protected health information (PHI), it is clear that health-care entities falling under the purview of HIPAA (Covered Entities) must be prepared to strictly comply with privacy and security requirements.

Vigorous Enforcement of Rules is Likely to Continue in 2017

After the passage of the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) and the applicable HIPAA Breach Notification Rules, OCR has prioritized enforcing the applicable privacy and security rules. Up until 2016, however, enforcement actions and the resulting settlement amounts had remained fairly steady.

For instance, settlements totaled $7.9 million and $6.2 million in 2014 and 2015, respectively. Thus, the $23.5-million total for 2016 is truly a drastic increase, and not one that can be explained by a large settlement accounting for the majority of the total. Instead, OCR increased its enforcement efforts, in part through use of its Regional Offices,[2] and set the groundwork for that trend to continue in 2017.

OCR has mandatory investigations in place for any breach of PHI affecting *over* 500 patients. In September of last year, however, OCR announced an initiative to investigate more widely breaches affecting *fewer* than 500 patients.[3] In other words, a limited number of affected patients will no longer be a shield from an OCR investigation; OCR will be investigating and enforcing HIPAA to the fullest extent.

A case from 2012 is illustrative. On December 28, 2012, OCR finalized its first settlement with a health-care entity for a breach of PHI affecting fewer than 500 patients.[4] OCR settled with the Hospice of North Idaho after the theft of a laptop computer containing PHI of 441 individuals. Hospice of North Idaho had to pay $50,000 due to the lack of an annual security risk analysis, and "not adequately adopt[ing] or implement[ing] security measures sufficient to ensure the confidentiality of ePHI that it created, maintained, and transmitted using portable devices…."[5]

In addition to investigating smaller breaches, OCR remains vigorous in enforcing the HIPAA Security Rule for breaches affecting over 500 patients.[6] Earlier this year, on February 16, 2017, OCR announced a $5.5-million settlement with Memorial Healthcare Systems based upon the ePHI of "115,143 individuals [being] impermissibly accessed by [] employees and impermissibly disclosed to affiliated physician office staff."[7] Furthermore, a former employee's credentials had been used for a year on a daily basis without detection.[8]

While policies were in place at Memorial Healthcare Systems, the policies lacked required HIPAA procedures for reviewing, modifying, or terminating a user's access rights.[9] HIPAA requires Covered Entities to have audit controls and to review audit logs regularly. Failing to do so can lead to hefty penalties.

Phase II Audits Will Only Increase Enforcement

Moreover, the third round of Phase II HIPAA Audits will commence in 2017 and is likely to involve comprehensive on-site visits of Covered Entities and business associates and additional enforcement actions.[10] OCR's audit program commenced with a pilot program in 2011 and 2012 of 115 Covered Entities. The audit program morphed into "Phase II" in 2014, with desk and on-site audits beginning last year. A desk or on-site audit involves a pre-audit questionnaire to gather information about the Covered Entity, followed by a close review of Security Rule and Breach Notification Rule compliance.[11]

OCR states that it uses the audits to supplement its enforcement actions, investigations and compliance reviews to uncover and address risks and vulnerabilities to PHI. However, commencement of an enforcement action remains a high risk. In fact, a careful review of enforcement actions over the past 18 months reveals that the vast majority of Covered Entities have been cited for an inadequate risk analysis (or lack thereof), which is the cornerstone of the Security Rule and the current audits.

In other words, while the stated goal of the Phase II HIPAA Audit is to develop OCR's audit program, the problems cited thus far by OCR will likely result in more enforcement actions pursuant to its right to begin a compliance review, if it finds substantial violations.

Thus, it is highly recommended that Covered Entities take proactive steps to prepare for a HIPAA Phase II Audit, which will also mitigate liability associated with a breach.

Health-Care Entities Should Make Cybersecurity a Top Priority

Through its enforcement actions and Phase II HIPAA Audits, OCR's clear focus is on the HIPAA Security Rule and the requirement to conduct a risk analysis. In order to be fully prepared and mitigate its liabilities, a Covered Entity must conduct an assessment to identify vulnerabilities and risks to the confidentiality and integrity of PHI. As discussed, with OCR cracking down on violations of HIPAA and HITECH, it is likely that, if a Covered Entity is not in compliance, an enforcement action will be in its future.

OCR has enforced violations of HIPAA with increased vigor in 2016 and is unlikely to waiver this year. Thus, the increase in frequency of cyberattacks and associated HIPAA enforcements means that cybersecurity and protection of PHI should be a top priority for any Covered Entity or business associate. By being prepared and having an organized approach, health-care entities can avoid unnecessary enforcement actions, which will allow them to focus on what is most important—the health of their patients.

John J. Cooney

Nicole Della Ragione

John J. Cooney, Esq. is a partner at Ruskin Moscou Faltischek and chair of the Firm's Cybersecurity and Data Privacy practice group. His e-mail is jcooney@rmfpc.com.

Nicole Della Ragione, Esq. is an associate at the firm and a member of its Cybersecurity and Data Privacy practice group. Her e-mail is ndellaragione@rmfpc.com.

1 Reece Hirsch, *HIPAA Turns 20: Looking Back at 2016 and at the Challenges Ahead*, 16 Privacy & Security L. Rep. (BNA) No. 221 (Feb. 6, 2017).
2 Posting to OCR-PRIVACY-LIST@LIST.NIH.gov (Aug. 18, 2016), https://list.nih.gov/cgi-bin/wa.exe?A2=OCR-PRIVACY-LIST;65d278ee.1608.
3 *Id.*
4 Hospice of N. Idaho, Resolution Agreement (U.S. Dep't Health and Hum. Serv. Dec. 28, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/honi-agreement.pdf.
5 *Id.*
6 Press Release, $5.5 million HIPAA settlement shines light on importance of audit controls, U.S. Dep't Health and Hum. Serv. (Feb. 16, 2017), https://www.hhs.gov/about/news/2017/02/16/hipaa-settlement-shines-light-on-the-importance-of-audit-controls.html.
7 *Id.*
8 *Id.*
9 *Id.*
10 Hirsch, *supra* note 1.
11 *Id.*