$4.8M HIPAA Fine Part Of Wider HHS Crackdown

Law360, New York (May 28, 2014, 1:24 PM ET) --
The U.S. Department of Health and Human Services Office for Civil Rights ("OCR") continues to surprise health care organizations with big ticket enforcement penalties for violations of the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act, collectively referred to herein as HIPAA.[1]

Julie A. Sullivan

The OCR's most recent targets, New York-Presbyterian Hospital and Columbia University, entered into a settlement with the OCR earlier this month to resolve allegations that the organizations had violated HIPAA by failing to secure thousands of patients' electronic protected health information ("ePHI") housed on the hospital and university's shared network.[2] At $4.8 million — $3.3 million to be paid by New York-Presbyterian and $1.5 million to be paid by Columbia University — this represents the largest HIPAA settlement to date. A fine of this magnitude for a technical HIPAA security rule violation underscores OCR's commitment to impose harsh consequences to parties obligated to comply with HIPAA who fail to do so.

The alleged breach, which was jointly reported to the OCR by the organizations and occurred in September 2010, involved the unauthorized disclosure of the ePHI of 6,800 individuals, including their respective patient status, vital signs, medications and lab results.[3] The organizations reported the alleged breach promptly upon learning from an individual who had found a deceased partner's ePHI from New York-Presbyterian Hospital on the Internet. The investigation revealed that a physician employed by Columbia University who created applications for both organizations had caused the breach when the physician deactivated a personally owned computer server on the hospitals' shared network containing New-York Presbyterian patient information, which inadvertently resulted in patient information being accessible on Internet search engines.[4]

OCR determined that both organizations: (1) lacked appropriate technical safeguards that would have prevented this breach; (2) had failed to conduct accurate and thorough risk analyses on their systems that would have identified this vulnerability; and (3) had failed to develop adequate risk management plans to address potential security threats to patient information.

Finally, OCR determined that New York-Presbyterian also failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its policies on access management. Both parties agreed to prepare substantial corrective action plans to address their respective HIPAA program deficiencies.

Prior to this settlement, the largest HIPAA civil monetary penalty levied was for $4.3 million in 2011 against Cignet Health, a company that operates a health plan and four physician offices.[5] Notably, however, $3 million of that fine was due to Cignet Health's failure to cooperate with the OCR's investigation into the allegations that the company had denied 41 patients access to their medical records in violation of their rights under HIPAA.

In the New York-Presbyterian Hospital and Columbia University settlement, no allegations of obstruction or failure to cooperate were lodged against the organizations and the OCR noted that the organizations promptly and appropriately self-reported the breach upon discovery and notified both the affected patients and media outlets, as required by HIPAA for a breach of this magnitude.

OIG Critique of Security Rule Enforcement Prompts OCR Response

In November 2013, HHS' Office of Inspector General (OIG) released a report criticizing the OCR's performance in its oversight and enforcement of the HIPAA security rule in its first two years since the department delegated such responsibilities to the OCR in July 2009. The OCR's security rule duties included ensuring that covered entities comply with the rule, investigating and resolving potential HIPAA violations, performing periodic audits of covered entities, and complying with federal internal control and cybersecurity requirements.[6]

In its report, the OIG concluded that from July 2009 through May 2011, the OCR had not assessed the risks, established priorities or implemented controls to provide for the periodic audits of covered entities' security rule compliance. The OIG also concluded that the OCR failed to consistently follow investigative procedures for security rule investigations, noting documentation deficiencies which caused the OIG to doubt that the OCR adequately identified and mitigated vulnerabilities to ePHI and that such deficiencies could undermine the OCR's findings and penalties. Finally, the OIG concluded that the OCR had itself failed to comply with applicable federal cybersecurity requirements for its own information systems used to store data, including ePHI involved in investigations, due to its focus "on system operability to the detriment of system and data security."[7]

In response to the OIG's report, OCR Director Leon Rodriguez detailed significant changes and improvements that occurred since the OIG's review 30 months earlier, which took a lot of steam out of the OIG's findings.[8] The one finding that Rodriguez acknowledged had not been rectified, which was the insufficiency of OCR's audits for security rule compliance. Rodriguez blamed a lack of funding to support the mandated audit activities, as the designated funding source for these audits expired in December 2012.

Nonetheless, Rodriguez pledged that the OCR would "leverage more civil penalties" to help foot the bill for security rule audits and enforcement efforts. He pointed out that, from 2008 through 2012, OCR obtained corrective action from covered entities in more than 13,000 cases in which OCR investigations indicated HIPAA privacy and/or security rule noncompliance, including 11 resolution agreements between OCR and covered entities to settle potential HIPAA violations, which yielded approximately $10 million in fines.[9]

Perhaps fueled by the OIG report criticizing its efforts, the OCR certainly appears recommitted to its cause in terms of security rule attention and enforcement. A review of OCR enforcement activity since the OIG report, or shortly before the report during OCR's draft report review and comment period, demonstrates a significant uptick in fines relating to security rule violations, including:

- $4.8 million settlement with New York-Presbyterian and Columbia University for failure to secure a shared network hosting ePHI in May 2014.[10]

- $1.72 million settlement with Concentra Health Services Inc. resulting from insufficient security management processes being in place, including a failure to encrypt a laptop stolen from Concentra in April 2014.[11]

- $1.7 million settlement with WellPoint Inc. resulting from WellPoint ePHI being accessible on the Internet due to poorly implemented changes to WellPoint's information systems in July 2013.[12]

- $1.21 million settlement in August 2013 with Affinity Health Plan Inc. for inadvertently disclosing ePHI belonging to hundreds of thousands of individuals by failing to erase the ePHI data on the rented photocopiers' hard drives, which was due in part to Affinity's failure to conduct an appropriate security risk analysis and implement security policies and procedures.[13]

- $250,000 settlement with QCA Health Plan Inc. for failing to have adequate security measures — again, including failure to encrypt a stolen computer — in place to reduce the risk to and vulnerabilities of its ePHI.[14]

- $215,000 settlement with Skagit County, resulting from seven patients' ePHI being accessed by unknown parties after the ePHI had been inadvertently moved to a publicly accessible server maintained by the county in March 2014.[15]

- $150,000 settlement in December 2013 with Adult & Pediatric Dermatology PC, resulting in part from a stolen unencrypted thumb drive containing the ePHI, which uncovered significant deficiencies in the practice's security management processes required by the security rule.[16]

In the past 11 months alone, OCR has received over $10 million in fines relating to security rule enforcement efforts and settlements, which already exceeds the $10 million that the OCR received over the four-year period of 2008 through 2012, from both privacy and security rule enforcement efforts that Rodriguez applauded in his response to the OIG report.[17] Undoubtedly this signals that the OCR has gotten its bearings on its security rule obligations and will continue to aggressively enforce the rule's requirements through significant monetary penalties for offenders.

It's Time to Focus on HIPAA Compliance

Recent OCR enforcement activities, perhaps most notably the New York-Presbyterian/Columbia University settlement, demonstrate the office is upping the ante for HIPAA violations that could have been prevented by appropriate physical, technical and/or administrative safeguards.

The OCR appears to be on high alert for covered entities and their business associates, which are now directly subject to HIPAA's requirements and the office's enforcement of those requirements as of September 2013, who have neglected their HIPAA compliance programs by ignoring the need for a meaningful risk assessment, delaying implementation of changes warranted by an assessment or failing to appropriately address violations that have already occurred. No longer is it only deep pockets that are worthy of OCR enforcement efforts; smaller entities, including public bodies and independent physician practices, are viable targets subject to significant fines.

The worst thing a covered entity or business associate can do is ignore their vulnerabilities or fail to assess them at all. Doing so can take you from a starting minimum penalty of $100 for unknown violations to $50,000 for uncorrected known violations. For any type of repeat violations, covered

entities and business associates could be faced with penalties up to $1.5 million per year for each aspect of HIPAA noncompliance.[18]

The OCR's director identified the single common thread that runs through all of OCR's security cases: "a failure of entities to do a thorough risk analysis — identifying where [protected health information] resides, what are the vulnerabilities of that information, determining the possible risks of those vulnerabilities and then implementing the necessary measures to protect that information."[19]

Rodriguez has demonstrated that HIPAA enforcement is a top priority for the OCR, and HIPAA experts have predicted that health care organizations will likely see the OCR issuing more and larger monetary penalties for HIPAA violations going forward. The enforcement activities of the past 11 months certainly hold true to this prediction. Accordingly, now is the time for covered entities and business associates alike to reevaluate their HIPAA programs to ensure compliance with both the privacy and security standards of HIPAA and avoid becoming the next entity to make headlines for its HIPAA noncompliance.

—By Julie A. Sullivan and Darryl T. Landahl, Brownstein Hyatt Farber Schreck LLP

Julie Sullivan is an associate and Darryl Landahl is a shareholder in Brownstein Hyatt Farber Schreck's Denver office.

[1] Public Law 104-191 and Public Law 111-5, respectively.

[2] See press release, data breach results in $4.8 million settlements available at: http://www.hhs.gov/news/press/2014pres/05/20140507b.html.

[3] Id.

[4] Id.

[5] See "Cignet Health Fined a $4.3M Civil Money Penalty for HIPAA Privacy Rule Violations" (2011), http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cignetcmp.html.

[6] See "The Office for Civil Rights Did Not Meet All Federal Requirements in Its Oversight and Enforcement of the Health Insurance Portability and Accountability Act Security Rule" (November 2013), https//oig.hhs.gov/oas/reports/region4/4110525.pdf.

[7] Id. at p. ii.

[8] See id. at Ex. B.

[9] See id.; see also Alaap Shah & Ali Lakhani, "OCR Lacks Insight Into HIPAA Security Rule Compliance" (2014), http://www.bna.com/ocr-lacks-insight-into-hipaa-security-rule-compliance/.

[10] See n.2.

[11] See press release, "Stolen laptops lead to important HIPAA settlements" on April 22, 2013, available at: http://www.hhs.gov/news/press/2014pres/04/20140422b.html.

[12] See press release, "WellPoint pays HHS $1.7 million for leaving information accessible over Internet" on July 11, 2013, available at: http://www.hhs.gov/news/press/2013pres/07/20130711b.html.

[13] See press release, "HHS settles with health plan in photocopier breach case (Aug. 14, 2013) available at: http://www.hhs.gov/news/press/2013pres/08/20130814a.html.

[14] See n.12.

[15] See press release on March 7, 2014, available at: http://www.hhs.gov/news/press/2014pres/03/20140307a.html.

[16] See press release, "Dermatology practice settles potential HIPAA violations" (Dec. 26, 2013), available at http://www.hhs.gov/news/press/2013pres/12/20131226a.html.

[17] See n.9.

[18] See generally 45 C.F.R. Part 164, Subpart D.

[19] See Beth Walsh, Rodriguez outlines OCR's enforcement priorities in "Clinical Innovation + Technology" on Sep. 23, 2013, available at: www.clinical-innovation.com/topics/privacy-secruity/rodriguez-outlines-ocrs-enforcement-priorities.