HIPAA – A Paper Tiger No More?

By Daniel F. Murphy, Balch & Bingham LLP, Birmingham, AL

Introduction

The Department of Health and Human Services (HHS) has held authority to enforce the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule since 2003 and the Security Rule since 2006.

Despite its ability to impose fines, civil monetary penalties (CMPs), and criminal sanctions, HHS neither settled nor enforced the Privacy or Security Rule until 2008. The HHS Office of Inspector General (OIG) concluded in 2008 that the Centers for Medicare and Medicaid Services (CMS) "had not provided effective oversight or encouraged enforcement of the HIPAA Security Rule by covered entities."[1]

Operating in a low-enforcement atmosphere, many covered entities began to perceive the Administrative Simplification Provisions of HIPAA[2] as somewhat of a paper tiger with complex rules and potentially severe penalties, but no teeth. Cast against aggressive OIG and Department of Justice (DOJ) enforcement of federal fraud and abuse laws, covered entities directed relatively few resources to HIPAA compliance efforts. Risk stratification exercises and cost-benefit analyses generally did not justify high-intensity HIPAA compliance programs.

On the crest of statutory and regulatory enhancements to HIPAA enforcement since 2008, two recent high stakes HIPAA enforcement cases suggest covered entities may need to recalibrate their investments in HIPAA compliance. By imposing CMPs totaling $4.35 million on Cignet Health of Prince George's County, MD (Cignet) and settling alleged Privacy Rule violations with Massachusetts General Hospital (Mass General) for $1 million, the HHS Office for Civil Rights (OCR) has signaled the potential gravity of HIPAA non-compliance. OCR also has provided, however, valuable HIPAA compliance guidance to other covered entities through its Corrective Action Plans (CAPs).

The Tiger Sharpens Its Claws

HHS Secretary Donna Shalala delegated authority to enforce the Privacy Rule to OCR in December 2000[3] and, after a lengthy rulemaking process, compliance with the Privacy Rule became mandatory for most covered entities on April 14, 2003.[4] For over five years, OCR neither penalized nor entered into a settlement with any covered entity for violations or alleged violations of the Privacy Rule.[5]

On the Security Rule side, HHS similarly undertook little enforcement action at first. HHS Secretary Tommy Thompson delegated authority to enforce the Security Rule to CMS in 2003[6] and this authority took effect on March 16, 2006 upon implementation of the HIPAA Enforcement Rule.[7] Nearly three years after CMS' Security Rule enforcement authority vested, however, OIG found "CMS had no effective mechanism to ensure that covered entities were complying with the HIPAA Security Rule or that ePHI was being adequately protected."[8]

Around the time of OIG's unfavorable audit of CMS' Security Rule enforcement, two developments began to set the stage for enhanced HIPAA enforcement. First, HHS reassigned Security Rule enforcement to OCR and took its first actions against alleged HIPAA violators. Second, Congress significantly expanded HIPAA's enforcement reach and statutorily authorized penalties in the Health Information Technology for Economic and Clinical Health Act (HITECH Act), which was enacted as part of the American Recovery and Reinvestment Act of 2009, and became law on February 17, 2009.[9]

HHS Changes

HHS made headlines in the healthcare community by entering into a Resolution Agreement with Providence Health & Services (Providence) on July 18, 2008 to settle potential HIPAA Privacy and Security Rule violations related to the loss of electronic backup media and laptop computers that contained individually identifiable health information.[10] Under the Resolution Agreement, Providence agreed to pay HHS $100,000 and to implement a CAP addressing the provider's HIPAA compliance program.[11] OCR also entered into $2.25 million Resolution Agreement and Corrective Action Plan with CVS Pharmacy, Inc. (CVS) on January 16, 2009 in connection with alleged unsecure disposal of pharmacy customers' protected health information (PHI).[12] For example, media reports suggested CVS discarded prescription labels and bottles containing PHI in unsecured dumpsters outside of CVS retail locations.[13] Then, on July 27, 2009, HHS Secretary Kathleen Sebelius stripped CMS of its Security Rule enforcement powers and delegated them to OCR.[14]

Legislative Changes

The HITECH Act expanded the scope, enforcement powers, and penalties available under HIPAA. Business Associates of covered entities previously were bound to follow HIPAA contractually through Business Associate Agreements (BAAs) with covered entities. HITECH extended the applicability of HIPAA security provisions and the breach notification requirements introduced by HITECH directly to Business Associates.[15] Following HITECH's enactment, Business Associates that failed to comply with the Security Rule were no

longer merely in breach of BAAs, but also subject to the same civil and criminal penalties that apply to covered entities.[16] Prior to HITECH, HHS had no official protocol for covered entities to self-report certain HIPAA violations. In contrast to OIG's Anti-Kickback Statute Self-Disclosure Protocol and CMS' Self-Referral Disclosure Protocol, which are voluntary, HITECH mandates that covered entities report to OCR breaches of "unsecured protected health information."[17] In its interim final rule for breach notification, which currently governs HIPAA breach notifications, only breaches that pose a "significant risk of financial, reputational, or other harm to the individual" must be reported.[18] Mandatory breach notifications come with no offers of immunity or reduced penalties for the reporting entities.

The HITECH Act also increased the number of HIPAA enforcers and the scope of their enforcement powers. State Attorneys General may bring civil actions in federal district court against HIPAA privacy and security violators and seek damages of up to $100 per violation, capped at $25,000 for all violations of an identical requirement or prohibition during a calendar year.[19] Whereas HHS previously had the authority, but not the obligation, to perform HIPAA compliance audits, the HITECH Act requires HHS to perform "periodic audits to ensure that covered entities and business associates" comply with the Privacy and Security Rules.[20]

Prior to the HITECH Act, HIPAA authorized HHS to impose CMPs up to $100 per violation and $25,000 for all violations of an identical requirement or prohibition during a calendar year. The HITECH Act revised HIPAA to implement an increased, tiered approach to CMPs based on the level of culpability associated with a violation. As described in the currently effective interim final rule on the enforcement of the HITECH amendments to HIPAA, the following strata of penalties now apply: (i) between $100 and $50,000 per violation that "the covered entity did not know and, by exercising reasonable diligence, would not have known that the covered entity violated such provision"; (ii) between $1,000 and $50,000 per violation "due to reasonable cause and not to willful neglect"; (iii) between $10,000 and $50,000 per violation due to "willful neglect" corrected within 30 days of discovering the violation; and (iv) at least $50,000 per violation due to "willful neglect" not correcting within 30 days of discovery.[21] An overall cap of $1.5 million for identical violations during a calendar year applies to each tier of penalties.[22]

The Tiger Bites

Armed with new administrative and statutory enforcement powers, OCR levied the first CMPs in the history of HIPAA and settled another significant alleged violation in February 2011.[23]

According to OCR's Notice of Proposed Determination, Cignet breached the HIPAA Privacy Rule by failing to provide 41 individuals timely access to copies of their medical records, by failing to cooperate with the OCR investigation of patient

Armed with new administrative and statutory enforcement powers, OCR levied the first CMPs in the history of HIPAA and settled another significant alleged violation in February 2011.

complaints regarding access to their medical records, and by not correcting the violations within 30 days of discovering (or having a duty to have discovered) the violations.[24] Although Cignet's underlying violations appear to have been relatively straightforward, OCR found the infractions combined with Cignet's subsequent inactions warranted a finding of "willful neglect" not corrected within 30 days and thus the highest-tier CMPs possible. After denying the 41 patients access to their medical records, Cignet also failed to: respond to OCR investigation requests, respond to subpoenas duces tecum, and appear in federal district court for a hearing.[25] Cignet eventually delivered original medical records to DOJ in response to requests, but the production included medical records for 4,500 patients whose information was not the subject of the investigation.

In contrast to the Cignet matter, OCR's settlement with Mass General did not result in CMPs or involve lack of cooperation. The alleged breach involved the removal and loss of PHI on a subway by a Mass General Employee. The patient data at issue was particularly sensitive: names, medical records, and other information for a total of 258 patients, including patients with HIV/AIDS.[26] To resolve the alleged violations, Mass General agreed to pay $1 million to HHS and enter into a three-year CAP.

The Mass General CAP appears similar both to previous CAPs executed by OCR and to Corporate Integrity Agreements entered into by OIG. The CAP imposes corrective action obligations that echo the federal sentencing guidelines and various OIG compliance guidance documents. Specifically, Mass General agreed to develop, distribute, and update policies and procedures targeted at the alleged violation and related activities.[27] The CAP requires Mass General to train its personnel on the policies and procedures developed in response to the alleged violation. In addition, the President or Chief Executive Officer of Mass General must distribute an email communication to personnel describing sanctions that will apply for failures to reasonably safeguard PHI. Finally, the CAP obligates Mass General to monitor and audit its performance under the newly developed policies and procedures, and to provide a number of reports to OCR regarding its performance under the CAP.[28]

Regulatory and statutory developments since 2008 have bolstered the HIPAA enforcement arsenal and recent cases have shown HHS' willingness to use its new authority.

Conclusion

Until recently, appropriating significant resources for HIPAA programs out of a limited pool of compliance funds and manpower was difficult for HIPAA compliance personnel to justify to their boards. HIPAA has authorized substantial civil and criminal penalties for some time, but HHS collected no settlements or penalties until 2008. Regulatory and statutory developments since 2008 have bolstered the HIPAA enforcement arsenal and recent cases have shown HHS' willingness to use its new authority. It may be too early to declare an era of intense HIPAA enforcement, particularly given the unique facts of the Cignet and Mass General cases. Nevertheless, the risk profile of HIPAA compliance programs clearly has shifted, both in theoretical terms and in action.

Although the body of HIPAA enforcement actions remains limited, OCR has taken a consistent approach in dealing with settlements of alleged violations. In each HIPAA settlement to date, HHS has imposed a corrective action plan that closely tracks the elements of an effective compliance program identified in the OIG's compliance program guidance documents.[29] With more at stake than ever before under HIPAA, covered entities should consider dusting off their HIPAA compliance programs, or policies and procedures, and evaluating their effectiveness. A robust HIPAA program can either be integrated into the entity's overall compliance structure or designed as a stand-alone framework that incorporates, at minimum, the fundamental elements of an effective compliance program.

About the Author

Daniel F. Murphy (dmurphy@balch.com) is an attorney with Balch & Bingham LLP's Healthlaw Practice Group in Birmingham, AL. Mr. Murphy's practice covers healthcare transactions and regulation, with an emphasis on Stark, the Anti-Kickback Statute, Medicare reimbursement and compliance. He received his J.D. from the University of Virginia School of Law and B.A. from the University of Notre Dame. Prior to practicing law, Mr. Murphy worked in the corporate finance department of Baxter Healthcare Corporation in Vienna, Austria and Illinois and received a Fulbright teaching assistanship in Vienna. Mr. Murphy is also a member of AHLA's Young Professionals Council.

Endnotes

1 Department of Health and Human Services, Office of Inspector General, *Nationwide Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight,* OIG Publication A-04-07-05064 (Oct. 2008), *available at* http://oig.hhs.gov/oas/reports/region4/40705064.pdf.
2 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, §§ 261-263, 110 Stat. 1936.
3 Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82381 (Dec. 28, 2000).
4 Standards for Privacy of Individually Identifiable Health Information; Final Rule, 67 Fed. Reg. 53181 (Aug. 14, 2002).
5 OCR entered into the first Resolution Agreement for alleged HIPAA violations with Providence Health & Services on July 16, 2008. The Resolution Agreement is *available at* www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/agreement.pdf.
6 Statement of Organization, Functions, and Delegations of Authority, 68 Fed. Reg. 60694 (Oct. 23, 2003).
7 HIPAA Administrative Simplification: Enforcement; Final Rule, 71 Fed. Reg. 8389 (Feb. 16, 2006).
8 *See supra* note 1, at 3.
9 American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, Title XIII, 123 Stat. 115, hereinafter cited as ARRA.
10 *See supra* note 5.
11 *Id.*
12 *See* Resolution Agreement between CVS and HHS, *available at* www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cvsresagrcap.pdf.
13 *Id.*
14 Office for Civil Rights; Delegation of Authority, 74 Fed. Reg. 38630 (Aug. 4, 2009).
15 ARRA § 13401(a).
16 ARRA § 13401(b).
17 ARRA § 13402(a).
18 Breach Notification for Unsecured Protected Health Information; Interim Final Rule, 74 Fed. Reg. 42740 (Aug. 24, 2009); 45 C.F.R. § 164.402.
19 ARRA § 13410(e).
20 ARRA § 13411.
21 HIPAA Administrative Simplification: Enforcement, 74 Fed. Reg. 56123 (Oct. 30, 2009).
22 *Id.*
23 OCR also settled alleged HIPAA violations with Rite Aid Corporation on July 27, 2010 ($1 million for activities similar to those alleged against CVS) and Management Services Organization Washington, Inc. ($35,000 plus a Corrective Action Plan related to the disclosure of ePHI for marketing purposes). *See* www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.
24 Notice of Proposed Determination, *available at* www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/cignetpenaltynotice.pdf.
25 *Id.*
26 Resolution Agreement, *available at* www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/massgeneralracap.pdf.
27 *Id.*
28 *Id.*
29 *Available at* http://oig.hhs.gov/fraud/complianceguidance.asp.