March 22, 2016

OCR Kicks Off HIPAA Audits After Issuing Two Major Settlements

On Monday, the HHS Office for Civil Rights (OCR) launched phase two of its much-anticipated audit program for covered entities and business associates. The announcement comes in the wake of OCR's issuance of two major settlements—totaling more than $5 million—which highlighted the critical importance of managing the security basics, such as the business associate agreement (BAA) and the organization-wide risk analysis. These developments are summarized below, with practical tips that can help organizations mitigate related risks.

Summary

2016 Audit Program Begins

In announcing the 2016 audit program launch, OCR confirmed it will contact organizations by email to verify contact information and complete a pre-audit questionnaire. Organizations selected for audit will be subject to either a desk audit, an onsite audit or potentially both. Organizations will have a short period to produce requested documents, typically 10 business days, so it is important to have HIPAA privacy and security policies, security risk assessments, breach notification documentation, BAAs, and other HIPAA documentation up-to-date and readily available. While there is a detailed audit protocol from the phase one OCR audits, that protocol has not been updated for the final rules implementing the HITECH Act. OCR has committed to issuing an updated audit protocol closer to the date the audits will be conducted, which will set forth the criteria that auditors will review. Importantly, the phase two audits will extend to business associates. Although the risk of being selected for an audit is low, organizations would be well advised to review the existing and, when available, new audit protocols, conduct a compliance gap assessment and take corrective actions as needed, as part of overall HIPAA compliance efforts. Specific tips are highlighted below. While OCR states that the audits are primarily a compliance improvement activity, enforcement may follow where a serious issue is identified.

The North Memorial Settlement – The Importance of Business Associate Agreements

In the first of two recent settlements, North Memorial Health System, a nonprofit organization, will pay $1.55 million and enter into a two-year corrective action plan to settle charges that it violated HIPAA by failing to have a written BAA with a key contractor. OCR's investigation followed the 2011 theft of an unencrypted laptop from a contractor's workforce member's vehicle. The settlement notes that the laptop contained protected health information (PHI) of approximately 9,497 North Memorial patients. For its part, the contractor separately settled HIPAA violations for $2.5 million, and entered into a

For more information, please contact any of the following members of Katten's **Privacy, Data and Cybersecurity** practice.

Megan Hardiman
+1.312.902.5488
megan.hardiman@kattenlaw.com

Michael R. Callahan
+1.312.902.5634
michael.callahan@kattenlaw.com

Doron S. Goldstein
+1.212.940.8840
doron.goldstein@kattenlaw.com

Matthew R. Baker
+1.415.293.5816
matthew.baker@kattenlaw.com

related 20-year FTC consent order relating to its security procedures.[1] OCR also alleged that North Memorial failed to conduct an organization-wide risk analysis that covered all of its IT infrastructure.

OCR's investigation indicated that North Memorial failed to execute a BAA with the contractor as required by HIPAA Privacy and Security Rules. OCR asserted that North Memorial gave the contractor access to its hospital database, which stored the electronic PHI of 289,904 patients, as well as access to non-electronic PHI as it performed services on-site at North Memorial.[2] In total, OCR's investigation found that, from March 21, 2011, to October 14, 2011, North Memorial impermissibly disclosed the PHI of at least 289,904 individuals to the contractor without obtaining a proper BAA.[3] The investigation further indicated that North Memorial failed to complete a comprehensive risk analysis to identify all potential risks and vulnerabilities to the electronic PHI (ePHI) that it maintained, accessed or transmitted across its entire IT infrastructure, as required by the HIPAA Security Rule.[4] In settling the matter, North Memorial did not concede liability.

In addition to the $1.55 million payment, North Memorial agreed to a two-year corrective action plan (CAP) that requires it to develop policies and procedures related to business associate relationships and to conduct an organization-wide risk analysis and risk management plan, as required under the HIPAA Security Rule.[5] The CAP also requires North Memorial to train appropriate workforce members on all policies and procedures newly developed or revised pursuant to the CAP.[6]

OCR has previously (and repeatedly) emphasized the importance of having an organization-wide, thorough analysis, which it reinforces here with North Memorial. In addition, this settlement highlights the importance that OCR attaches to having BAAs where required, which OCR describes as another "cornerstone" of effective security.[7] Further, the settlement illustrates that, when a breach occurs with a business associate, the impacted covered entity should expect OCR to request a copy of the underlying BAA. Where that BAA cannot be found, the covered entity and business associates should expect potential enforcement.

FIMR Settlement: Basic Compliance Required of All Covered Entities (and Business Associates)

In the second settlement, Feinstein Institute for Medical Research (FIMR), a nonprofit research institute, will pay $3.9 million and enter into a three-year corrective action plan to settle charges it violated HIPAA, following its breach when an employee's unencrypted laptop containing patient information of 13,000 individuals was stolen. OCR's investigation determined that FIMR's security management process was limited, it had failed to conduct a thorough risk analysis, and lacked sufficient policies and procedures. In its press release, OCR emphasized that it expects research institutions that are covered entities to comply with the same standards as other covered entities.

OCR's investigation of FIMR stemmed from a self-reported breach after an employee's unencrypted laptop was stolen. Based on the resolution agreement, OCR's investigation appears to have identified widespread non-compliance. For example, OCR alleged that FIMR: (1) failed to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to all of the ePHI held by FIMR, including the ePHI on the employee's laptop; (2) failed to implement policies and procedures for granting access to ePHI by its workforce members and restricting access by unauthorized users; (3) failed to implement physical safeguards for the

---

1 The related 2012 settlement by business associate Accretive Health with the Minnesota attorney general for violations of the HIPAA rules and state law was widely touted within the industry as the first HIPAA enforcement action against a business associate. See Settlement Agreement, Release, and Order, 12-cv-00145, ECF No. 90 (July 30, 2012). Because the breach occurred prior to the issuance of final rules implementing the HITECH Act's extension of direct liability for HIPAA violations to business associates, OCR—the primary federal HIPAA enforcement agency—had indicated it would not enforce the HITECH Act changes against business associates until issuance of the final rules. However, this did not prevent the Minnesota attorney general from proceeding to enforce HIPAA, using newly expanded enforcement authority granted to state attorneys general under the HITECH Act. Accretive Health also entered into a related, 20-year consent order with the FTC, pursuant to which no fine or penalty was paid but in which Accretive Health agreed to establish and maintain a comprehensive information security program, and to periodic evaluations of that program. *See* Press Release, FTC approves final consent order settling charges that Accretive Health failed to adequately protect consumers' personal information (Feb. 24, 2014).

2 *See* North Memorial Resolution Agreement and Corrective Action Plan, I.2.A, (Mar. 16, 2016).

3 *See id.* at I.2.B.

4 *See id.* at I.2.C.

5 *See id.* at I.V.A-C.

6 *See id.* at I.V.D.

7 *See* Press Release, $1.55 million settlement underscores the importance of executing HIPAA business associate agreements (Mar. 16, 2016).

laptop; (4) failed to implement policies and procedures that govern receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility; and (5) failed to encrypt ePHI on the laptop or, alternatively, document why encryption was not reasonable and appropriate and implement an equivalent safeguard.

As part of an extensive three-year CAP, FIMR must conduct an organization-wide risk analysis and develop a corresponding risk management plan, develop a process for evaluating environmental or operational changes to the security of ePHI, revise its policies and procedures for privacy and security, and provide extensive training and reporting.

Tips to Mitigate Risks

Covered entities and business associates can enhance HIPAA compliance, and reduce audit risk, by taking a number of practical steps outlined below.

Business Associate Risks:

(1) train workforce (at onboarding and at least annually thereafter) to recognize situations where a BAA (or subcontractor BAA) is required and understand how to activate the organization's process for securing one;

(2) conduct periodic audits of existing outside service relationships to ensure that all necessary BAAs (or subcontractor BAAs) are, in fact, in place;

(3) periodically audit BAAs (and subcontractor BAAs) on file to ensure they are fully compliant (including as to the final HITECH rule content requirements), in full force and effect, and readily retrievable; and

(4) retain records of training and audits conducted for at least six years.

This also is an excellent time for covered entities and business associates to re-examine the effectiveness of their processes for conducting initial diligence and periodic audits of the security compliance of their key business associates and subcontractors.

Risk Analysis:

While not a new point, it remains critical for covered entities and business associates to conduct and document the requisite security risk analysis on a regular basis, and take prompt corrective action to manage identified risks. It is particularly important to ensure that the risk analysis covers all ePHI maintained, accessed or transmitted across the organization's entire IT infrastructure, including but not limited to all applications, software, databases, servers, workstations, mobile devices and electronic media, network administration and security devices, and associated business processes. This can be a challenge—particularly in light of the pace of developments and acquisitions/consolidations in the health care industry—but is essential. Organizations should develop a complete inventory of all electronic equipment data systems, and applications controlled by, administered or owned by the organization and its workforce that contain or store ePHI, including personally owned devices. Organizations should make sure their process includes equipment purchased outside of standard procurement processes.

Audit Preparation Tips:

(1) Confirm that all required HIPAA privacy and security policies and procedures are implemented and up-to-date;

(2) Make sure a through, organization-wide security risk analysis as described above has recently been conducted, and that resulting corrective actions have been taken;

(3) Confirm that BAAs are fully up-to-date and accessible, and follow the steps above to further reduce business associate risks;

(4) Use the audit protocols to conduct a gap assessment;

(5) Be prepared to provide documentation showing that breach notices have been provided as required by HIPAA; and

(6) Covered entities should ensure their notices of privacy practices are up-to-date and provided as required.

Other Basics:

(1) Encryption: Encryption of laptops, thumb drives and other mobile devices remains a critical risk mitigation strategy. HIPAA does not require encryption of ePHI in all cases "per se"; however, it does require organizations to specifically address, as part of their required risk analysis, whether encryption is a reasonable and appropriate safeguard (and if so, it requires organizations to encrypt; if not, it requires organizations to document why encryption is not reasonable and appropriate, and adopt an alternative safeguard). However, encryption per the HHS guidance provides a "safe harbor" from breach notification under HIPAA and generally obviates the need to make state law data breach notifications as well, in the event of loss of encrypted data. Further, because encryption will, in fact, be "reasonable and appropriate" in many cases, often it is effectively required.

(2) Training: The scope and frequency of training also should be regularly reviewed to ensure training covers key aspects of privacy and security policies. In addition, training should address current and emerging threats and risk areas. For example, in light of the significant role of phishing attacks and malware in cyber-breaches, training should include employee awareness of how to identify and respond to these types of attacks.