Akin®

HHS Steps Up HIPAA Enforcement in 2016, Launching Phase 2 of the HIPAA Audit Program and Announcing Additional Enforcement Actions

Mar 24, 2016

Reading Time : **5 min**

By: Jo-Ellyn Sakowitz Klein, Marlee P. Gallant

Phase 2 HIPAA Audits Have Begun

The HITECH Act requires OCR to perform periodic audits of both covered entities and their business associates for compliance with the Privacy, Security, and Breach Notification Rules adopted under HIPAA and the HITECH Act.

Phase 1 of the HIPAA Audit Program was conducted as a pilot program in 2011 and 2012, and focused on HIPAA covered entities (e.g., health plans, hospitals and other health care providers that are directly subject to HIPAA). OCR assessed 115 entities and conducted a comprehensive evaluation of the effectiveness of the pilot program before implementing Phase 2.

Notably, Phase 2 audits will target business associates in addition to covered entities. Business associates include the many vendors, service providers and other entities that create, receive, maintain or transmit health information in the course of providing services for hospitals, health plans and other covered entities.

In announcing the launch, OCR Director Jocelyn Samuels indicated that Phase 2 will involve more than 200 desk and on-site audits of covered entities and business associates. According to OCR's website, Phase 2 will be broken into three rounds of audits: round one will involve desk audits of covered entities, round two will involve desk audits of business associates, and round three will involve on-site audits of both covered entities and business associates. OCR

expects the desk audits to be completed by the end of December 2016. The on-site audits are expected to examine a broader scope of requirements than the desk audits.

The Phase 2 audit process is already under way. OCR has begun sending entities emails seeking to confirm contact information. The agency intends to identify covered entities and business associates of various types and determine which may be appropriate to include in pools of potential auditees. Once entity contact information is obtained, a pre-audit screening questionnaire will be issued. Entities selected for audits will be notified by email and will be required to submit requested documents through a portal on the OCR website.

OCR is developing audit protocols for Phase 2, which will be posted on OCR's website once they are available. The audits are expected to focus on compliance with requirements relating to risk analyses and risk management, notices of privacy practices, affording patients access to their medical records and breach notification, among other issues.

There are several steps that covered entities and business associates should take now to prepare for the Phase 2 audit process, including:

- Review information available about the Phase 2 audits. The OCR website contains information on Phase 2, along with a list of frequently asked questions. You should review this information and determine how audit-related requests would be handled within your organization.
- Compile a list of business associates, complete with current contact information and business associate agreements. During the pre-audit screening process, OCR will ask for an inventory of business associates.
- Prepare to gather all HIPAA privacy, security and breach notification policies and procedures and other compliance documentation. You should confirm that you know the location of all core HIPAA compliance documentation. OCR expects audited entities to submit electronic versions of requested information within 10 business days of the date on the information request. In particular, you should ensure that a HIPAA-compliant risk assessment has been performed and that relevant documentation is readily available. You should address any gaps in documentation that may be discovered in the process.
- Conduct a practice audit based on the Phase 1 protocol. OCR has not yet released the Phase 2 audit protocol, but the Phase 1 audit protocol is still available online.

- Adjust settings on spam and junk mail folders to ensure that any audit-related communications are received. Entities subject to HIPAA should be on the lookout for emails from OCR. Audit-related emails will be sent from OSOCRAudit@hhs.gov and OCR expects entities to check spam and junk mail folders for correspondence.

Recent HIPAA Penalties and Settlements Send a Signal

Covered entities and business associates can also learn valuable lessons from OCR's recent enforcement actions. 2016 has already seen three major announcements in OCR enforcement actions. This activity signals the seriousness with which regulators continue to approach HIPAA compliance.

Most recently, OCR announced on March 17, 2016, that the Feinstein Institute for Medical Research agreed to pay $3.9 million to settle charges that it violated the HIPAA Privacy and Security Rules by failing to address potential risks to the confidentiality and integrity of electronic protected health information (ePHI). OCR initiated its investigation after Feinstein filed a breach report indicating that a laptop computer containing ePHI of approximately 13,000 patients and research participants was stolen from an employee's car in September 2012.

Just one day earlier, on March 16, 2016, OCR announced that North Memorial Health Care of Minnesota, a comprehensive, not-for-profit health care system, agreed to pay $1.55 million to settle charges that it violated the HIPAA Privacy and Security Rules by neglecting to execute a business associate agreement and failing to complete a HIPAA-compliant risk assessment. OCR launched its investigation of North Memorial after receiving a breach report in September 2011 indicating that an unencrypted laptop was stolen from the locked vehicle of a business associate's workforce member, impacting the protected health information of 9,497 individuals.

In addition, an HHS Administrative Law Judge ruled on February 3, 2016, that Lincare, Inc., a provider of respiratory care, infusion therapy and medical equipment to in-home patients, violated HIPAA and required Lincare to pay $239,800 in civil money penalties (CMPs) imposed by OCR. This was only the second time in history that OCR sought CMPs for HIPAA violations. OCR investigated a complaint that a Lincare employee had moved, leaving behind documents containing protected health information of 278 patients. The investigation revealed that Lincare had insufficient policies and procedures, including an unwritten policy requiring certain employees to store protected health information in their own cars. OCR indicated

that although Lincare was aware of the investigation and the deficiencies found, the company took only limited action to improve compliance.

Conclusion

OCR remains committed to HIPAA enforcement activities. Covered entities and business associates should heed the warning and act now to shore up compliance. Through audit preparedness activities, entities may achieve a higher level of compliance and reduce risks, giving the efforts value beyond improving readiness to respond to audit requests that may come. OCR has been abundantly clear: negative audit findings can lead to an investigation.

Categories

Cybersecurity, Privacy & Data Protection