OCR Releases Results of HIPAA Compliance Audit Pilot

Save to myBoK

By Kathy Downing, MA, RHIA, CHP, PMP and Mac McMillan, FHIMSS, CISM

The American Recovery and Reinvestment Act (ARRA) of 2009, in section 13411, requires the US Department of Health and Human Services (HHS) to conduct periodic audits to ensure covered entities and business associates are meeting HIPAA compliance requirements.

The findings of a HHS pilot program, which was initiated by ARRA in the fall of 2011, should serve as a reminder to HIM professionals and privacy officers to review and update their internal HIPAA audit programs. An annual review of the audit process and areas of focus for the privacy and security program is recommended for all HIPAA-covered entities.

During HHS' pilot audit program there were 115 total audits through December 2012 that measured performance against 169 requirements in three focus areas: privacy, security, and breach notification.

The pilot audit program, administered by the HHS Office for Civil Rights (OCR), was focused on covered entities of all sizes and types, including healthcare providers, health plans, and healthcare clearinghouses. A random selection was applied to the 3.5 million organizations in the audit pool. The selection was based on factors such as revenue, size, type, number of patients, number of employees, geography, and affiliation with other entities. HHS intended to evenly distribute the audits across the country, across facility size per revenue, across stand-alone versus affiliated entities, and across types of entities.

In addition to heath plans and hospitals, the types of healthcare providers included were long-term care facilities, pharmacies, laboratories, dental offices, medical offices, and healthcare clearinghouses. This distribution is important to permit OCR to analyze a diverse outcome from the audits, and to report the results in a balanced fashion to Congress.

OCR Audit Division by Level

During the OCR audit pilot program, the selected entities were divided into four levels. In order to take a balanced look at how the industry was performing against the compliance requirements, OCR selected entities in the following groupings for 2012.

Level 1	Level 2	Level 3	Level 4
Large providers or health plans with extensive use of HIT and revenue and/or assets greater than $1 billion.	Large regional hospital systems or insurance companies with both paper and HIT-enabled flows and revenue and/or assets between $300 million and $1 billion.	Community hospitals, outpatient surgery, and regional pharmacies that had some but not extensive HIT and revenues between $50 million and $300 million.	Smaller providers with little or no use of HIT and revenues less than $50 million.

Total number of providers selected, by level:

	Healthcare Providers	Health Plans	Healthcare Clearinghouses	Total Audits

Level 1	11	13	2	26
Level 2	16	12	3	31
Level 3	10	11	1	22
Level 4	24	11	1	36
Total Audits	61	47	7	115

Source: HHS. "Enforcement Highlights." July 31, 2013. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html.

The Pilot Findings

OCR shared a summary of their findings from the pilot program audits during the HIPAA Summit that took place in Washington, DC, in February. Around 10 percent of the covered entities selected and audited had no audit findings. This means that for the remaining 90 percent of the audits, corrective actions were necessary. OCR is considering whether to pursue further review or investigation for some of these non-compliant entities, which could lead to a formal settlement action. HIM professionals should stay tuned and observe how OCR's rulings play out over the next few months. With the changes to the enforcement provisions of HIPAA now in place under the Omnibus Rule, formal sanctions could happen faster than they did in 2012.

Security Audit Findings

The majority of OCR's findings—60 percent—were security related. Some of the main areas where security compliance fell short, listed in order from most to least prevalent, are: risk analysis, access management, contingency planning and backup strategy, audit controls and monitoring, media control and destruction, work station security, security incident procedures, encryption, and integrity.

The most common root causes of noncompliance identified were the lack of resources, technology, and an expressed lack of understanding of the HIPAA requirements, as well as a general lack of security expertise. Covered entities need to refocus efforts to complete their risk analysis and assessment, and in some way address all requirements of the HIPAA Security Rule.

Addressable standards often were handled improperly by many covered entities. Failures to address, failure to address with a reasonable alternative control, or failure to document a credible rationale were most commonly cited as discrepancies by OCR. Encryption, for instance, often was not enabled, and documentation explaining why could not be identified. This particular requirement, while a HIPAA issue for now, will become a meaningful use issue as well once stage 2 of the "meaningful use" EHR Incentive Program goes into effect. Stage 2 of the meaningful use program calls for providers to "address" encryption as part of their security risk analysis, and assess the appropriateness of encrypting electronic protected health information as a means of securing it. Every organization should be developing its enterprise-wide encryption strategy for data at rest and in motion.

Privacy Audit Findings

The privacy findings showed issues with the following areas, listed in order from most to least prevalent: minimum necessary, business associate agreements, personal representatives, judicial and administrative processes, identity verification,

authorizations, deceased individuals, and group health plans.

For privacy, the areas needing more focus from HIPAA-covered entities included training, policies and procedures, compliance management, and sanctions processes. Compliance management is becoming more important as the number of patients who submitted complaints was over 28,000, with over 19,000 of those requiring corrective actions by the covered entity. OCR has referred more than 515 cases to the US Justice Department for possible criminal prosecution.

In 2013, the focus thus far has been seeking feedback and comment regarding the audit process, reviewing the results from the pilot year and identifying changes to the audit process and protocol. There was an Information Collection Request published by HHS on March 19, 2013, that intends to collect information on how effective the audits were and solicit opinion on the audit process. They are also looking to obtain:

- Estimates of costs incurred by covered entities, in time and money, spent responding to the audit-related requests
- Assessment of attitudes toward the audit overall and with regard to the audit program features, including communications received and the audit on-site visit
- Assessment of whether improvements in HIPAA compliance were achieved as a result of the OCR audit
- Measurement of the overall effect of the HIPAA audit program on covered entities
- Feedback on the effect of the HIPAA audit program on day-to-day business operations

The information collected in this survey will be used to update and improve the HIPAA audit program going forward, OCR says. The comment period opened on March 19, 2013, and lasted for 60 days.

Internal HIPAA Audits—Where To Begin?

Now that the audit findings are available, covered entities should revisit their internal audit strategy for privacy and security compliance. Entities can enhance their readiness for an audit by using the audit protocols provided by OCR. These protocols are a valuable tool and should be used to create an internal audit program for a HIPAA-covered entity. The protocols can also help to prepare an entity's staff and can expose potential areas of noncompliance as well as areas for general improvement.

Figure 1 provides a sample of what is included in the OCR audit procedures. These audit protocols can be sorted by the topic of privacy, security, or breach and exported as needed. Users should be careful to download the latest version each time they want to use the OCR tool since it is a dynamic protocol and may change without notice. Changes are currently being made to incorporate the Omnibus Rule provisions.

Figure 1

Below is an example of OCR audit program protocol, which provides examples of meeting HIPAA compliance with the privacy, security, and breach notification rules.

Section	Established Performance Criteria	Key Activity	Audit Procedures
§164.502	A covered entity must accommodate reasonable requests by individuals to receive communications of protected health information from the covered healthcare provider by alternative means or at alternative locations.	Confidential communications	Inquire of management as to whether a process exists to ensure the entity complies with confidential communications requirements. Obtain and review the process and evaluate the content to determine if the entity is in compliance.

Source: OCR. "Audit Program Protocol."
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html.

Reference

US Department of Health and Human Services' Office for Civil Rights. "Audit Program Protocol."
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html.

Kathy Downing (kathy.downing@ahima.org) is a director of HIM practice excellence at AHIMA. Mac McMillan (mac.mcmillan@cynergistek.com) is chief executive officer at CynergisTek, Inc.

Article citation:
Downing, Kathy; McMillan, Mac. "OCR Releases Results of HIPAA Compliance Audit Pilot"
Journal of AHIMA 84, no.10 (October 2013): 60-62.