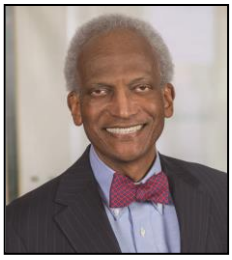
Brace For HIPAA Audits As They Arrive In Early 2016

By James E. Bowers, Susan Huntington and Eric D. Fader, Day Pitney LLP



Forced to respond to an audit report recently released by the U.S. Department of Health and Human Services' Office of Inspector General that found less than effective enforcement of the Health Insurance Portability and Accountability Act's privacy standards,[1] HHS' Office for Civil Rights will commence its long-awaited HIPAA audits in early 2016. Ever since OCR completed its pilot audit program and program examination in 2014, it has been widely expected that OCR would follow up with implementation of a permanent audit program, which has yet to happen despite announcements and audit preparations by OCR to launch the second phase of its audit program.

OIG's Findings

In its report examining OCR's oversight of covered entities' compliance with the HIPAA privacy rule,[2] OIG determined that OCR's oversight has been primarily reactive — simply responding to complaints in the overwhelming number of its investigations. Although the Health Information Technology for Economic and Clinical Health Act requirement for audits has been in effect since early 2010, OCR has not fully implemented an audit program to proactively identify and assess covered entities' possible noncompliance with the privacy standards. The concern is that covered entities (such as doctors, pharmacies and health insurance companies) that do not adequately safeguard protected health information (such as medical conditions, prescriptions or treatment history) could expose patients to an invasion of privacy, identity theft or other harm. OIG's primary recommendation was that OCR commence full implementation of a permanent audit program.[3]

OCR's Response

With its feet to the fire, OCR has accepted this finding and undertaken to launch audits in early 2016 using a contracted vendor, FCi Federal Inc., to conduct the audits. OCR will target specific common areas of noncompliance identified in its pilot audits and subsequent enforcement actions. Unlike the pilot audits which included only 20 covered entities, the second phase audits will encompass a much larger number of covered entities as well as business associates. As for the audit approach, the audits will consist of a combination of desk reviews of policies as well as onsite reviews. Over the next few months, OCR will be updating the audit protocol and refining the list of potential audit subjects.

Major Area of Noncompliance

The most common deficiency found by OCR in its pilot audits was an organization's failure to conduct a security risk assessment to identify and mitigate risks to PHI (e.g., PHI on exposed servers, unencrypted laptops, unchanged default passwords, outdated security software and inadequate training). As hard as it is to believe, many HIPAA entities still have not implemented this "lesson learned." As recently as a few weeks ago, OCR announced a $750,000 settlement with Indiana-based Cancer Care Group PC, because it had failed to conduct an enterprisewide

risk analysis and implement follow-on device and media control policies to protect the transportation of unencrypted PHI. OCR contends that a risk assessment could have identified the control weakness.[4]

Preparation for Audit

With the initiation of OCR's audit program fast approaching, potential targets must maintain readiness for audit examination because HIPAA noncompliance can be costly and disruptive to an organization. Preparation for an audit begins with a thorough review of the compliance requirements found in the HIPAA Audit Program Protocol. OCR has stated that it plans to update the audit protocol, so interested parties should stay abreast of this development on OCR's website. The audit compliance requirements are divided into three categories: security, privacy and breach notification.

As noted above, during the pilot audit phase, a common deficiency identified was the failure to conduct a security risk assessment. A risk assessment identifies and assesses risks to the security of PHI, evaluates security controls put in place to mitigate those risks and monitors the effectiveness of those controls on an ongoing basis. An adequate control environment contains many elements, including policies, procedures, systems, audits, people and training. The risk assessment focuses on evaluating and prioritizing security risks. Risk activities should be prioritized based upon the likelihood of occurrence of a security breach and the likely severity of such a breach. Organizations should consider conducting their risk self-assessment under attorney-client privilege to encourage maximum disclosure without fear of exposure.

In addition to conducting a risk assessment, adequate audit preparation requires a review of the myriad of HIPAA policy requirements relating to, for example, privacy practices; uses and disclosures of PHI; training; complaint handling; discipline; administrative, technical and physical security safeguards; and security incident management. These policies will likely be requested and examined by OCR in a desk audit prior to an onsite visit.

Potential audit targets should also compile any previous audit reports, evaluations or assessments regarding implementation of the HIPAA security, privacy and breach notification standards. Further, they should be prepared to turn over this information to OCR for examination. Well before receiving an audit notice, organizations should develop an audit response plan that outlines key considerations such as who will be the organization's lead responder to the audit team, a list of responsive documents and how personnel will be prepared to answer questions.

Consequences of an OCR Audit

Any audit can be disruptive to an organization's business, but the OCR audits and the resulting reports may create unintended liability exposures.

Auditors will develop and share a draft report with each audited entity. Before the report is finalized, the entity will have the opportunity to discuss concerns and describe corrective actions implemented to address identified concerns. The auditor will incorporate into the report the steps the entity has taken to resolve any compliance issues identified by the audit, as well as describe any best practices of the entity, before submitting the final report to OCR. OCR maintains that it will use the audit reports to determine what types of technical assistance should be developed, and what types of corrective action are most effective. However, should an audit report indicate a serious compliance issue, OCR may initiate a compliance review to address the problem. Thus, a substandard audit result could trigger a full-blown compliance investigation, even in the absence of a data breach.

Another concern is that while OCR will not post a listing of audited entities or the findings of an individual audit which clearly identifies the audited entity, the audit reports are not confidential or protected under any privilege. Consequently, in the event of a breach or complaint investigation, state attorney general offices will be able to request a copy of the entity's OCR audit report to demonstrate knowledge of prior deficiencies. In addition, audit reports will likely be discoverable and could be used to prove knowledge of substandard compliance in possible subsequent litigation. Lastly, in states like Connecticut, where case law has established that the HIPAA regulations could be the standard for protecting privacy under state law,[5] a substandard OCR report could be viewed as a de facto violation of the state law on privacy.

Conclusion

Preparation for an OCR audit should not be taken lightly. Health care companies are facing very real risks as they strive to comply with the HIPAA security, privacy and breach notification requirements. Today's regulatory climate swelters with million-dollar settlements, disruption to the business, regulatory and class action litigation exposure and, most of all, loss of consumer confidence.

With OCR audits slated to begin in early 2016, now is the time for covered entities and business associates to begin to prepare by performing self-assessments based on the OCR's audit protocol and taking corrective action to address identified vulnerabilities. Additionally, organizations should consider having legal counsel involved at the beginning of any OCR audit due to the unpredictable nature of government audits and the potential consequences associated with the audit reports.

---

[1] U.S. Department of Health and Human Services, Office of Inspector General, "OCR Should Strengthen Its Oversight Of Covered Entities' Compliance With The HIPAA Privacy Standards," September 2015, OEI-09-10-00510.

[2] The HIPAA privacy rule provides standards for using, sharing and disclosing patients' protected health information.

[3] OIG made five recommendations: (1) fully implement a permanent audit program; (2) maintain complete documentation of corrective actions taken by covered entities; (3) develop an efficient method in its case tracking system to search and track covered entities' history of investigations; (4) develop a policy requiring OCR staff to check whether covered entities were previously investigated; and (5) continue to expand outreach and education efforts to covered entities. OCR concurred with all five recommendations.

[4] U.S. Department of Health and Human Resources, News, Cancer Care Group, P.C., HHS.gov, "$750,000 HIPAA settlement emphasizes the importance of risk analysis and device and media control policies," September 2, 2015.

[5] *Byrne v. Avery Center*, 314 Conn. 433 (2014)

***

James Bowers is senior counsel in Day Pitney's Hartford, Connecticut offices. Susan Huntington is counsel in Day Pitney's Hartford, Connecticut offices. Eric Fader is counsel in Day Pitney's New York office.

This article was first published in Law360 on October 14, 2015.
