Anesthesiologists Should Beware of HIPAA Audits

Neda Mirafzali, Esq.
Clark Hill, PLC, Birmingham, MI

The acronym "HIPAA" has become a household name since the enactment of the Health Information Portability and Accountability Act of 1996, which, among other things, established rules for protecting and securing patients' health information. In fact, it is not uncommon to hear about breaches of patient information costing healthcare providers and suppliers six and seven figure civil monetary penalties or settlements. Typically, such settlements and penalties have arisen out of patient complaints that the privacy of their protected health information (PHI) has been compromised. However, beginning November 2011, patient complaints will not be the only way in which the Department of Health and Human Services (HHS) Office of Civil Rights (OCR) will learn about non-compliant entities.

Section 13411 of the American Recovery and Reinvestment Act of 2009, which established the Health Information Technology for Economic and Clinical Health (HITECH) Act, requires the Secretary of HHS to "provide for periodic audits to ensure that covered entities and business associates" comply with the requirements of the HIPAA Privacy Rule, Security Rule and Breach Notification Rule (collectively, the HIPAA Rules). To achieve this end, the OCR has engaged, under a $9.2 million contract, KPMG, LLC (KPMG) to conduct performance audits of covered entities in the form of a pilot audit program. The pilot will include up to 150 audits of covered entities to ensure compliance with HIPPA. The pilot program will conclude in December of this year.

Who Will be Audited

During this pilot program, covered entities of all sizes will be audited. According to the OCR, it "will audit as wide a range of types and sizes of covered entities as possible;

covered individual and organizational providers of health services, health plans of all sizes and functions, and health care clearinghouses may all be considered for an audit." Business associates will not be audited during the pilot, but will be included in future audits. A *covered entity* is defined as (i) a health plan, (ii) a healthcare clearinghouse, or (iii) a healthcare provider transmitting any health information in electronic form. As such, anesthesiologists, anesthesia groups, CRNAs, ambulatory surgery centers, physician offices and clinics electronically transmitting any health information are eligible to be audited by the OCR.

What Audited Entities Can Expect

Although the OCR will begin with roughly twenty (20) audits to test and finalize the audit protocols, audited entities can expect the HIPAA audits to include a request for documentation, an on-site field visit and a report. Initially, the OCR is using the audit process to detect compliance with the HIPAA Rules and identify best practices, and to discover compliance risks and vulnerabilities.

Step 1: Notification Letter

The OCR will send entities written notification letters. Included in the notification letter will be a request for documentation evidencing their HIPAA privacy and security compliance efforts.

The OCR provided a sample notification letter on its website.[1] Included in the sample letter is the following language briefly advising the audited covered entity of what to expect:

> *In the attached letter, KPMG LLP requests certain information be provided by you in order to facilitate the audit process. Additionally, they provide contact information for the audit firm personnel responsible for conducting the audit. Please recognize that KPMG LLP is requesting and reviewing these documents solely as a contractor to OCR and on its behalf and pursuant to its audit authority. This letter serves to notify you that the audit shall begin within the next 30 to 90 calendar days from the date of this letter. The results of the audit firm's work, including your management's written response to any reportable findings will be presented in a final report to OCR.*

Audited entities will have ten (10) business days in which to provide the requested documentation.

Step 2: Receipt and Review of Documentation and Planning Field Work

After KPMG receives the requested documentation from the audited entities, it will review the documentation and begin planning the audit field work—the on-site visit to the audited entity. Following KPMG's review, audited entities should expect KPMG to notify them within thirty (30) to ninety (90) days prior to the on-site visit.

[1] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/sample-ocr_notification_ltr.pdf

Step 3: On-Site Visit

KPMG will send auditors to conduct on-site field work of the audited entities. Audited entities can expect the field work to span between three (3) to ten (10) days, depending on the size of the entity, the complexity of the audit and the auditor's need to access information and personnel. The on-site field work will include interviews with the covered entity's leadership (*e.g.*, the compliance officer, legal counsel, health information manager, medical records director, etc.), examination of the physical space and operations, consistency of the entity's practice with its stated policies and observation of the entity's compliance with the HIPAA Rules.

Step 4: Draft Audit Report

Within twenty (20) to thirty (30) days following the auditor's on-site review of the audited covered entities, the auditor will prepare a draft audit report of its findings. The draft audit report will include information regarding the timeline and methodology of the audit, the best practices noted by the auditor, and any other information and data collected by the auditor. The draft audit report will also include specific recommendations to the covered entity to address compliance problems identified during the audit.

Step 5: Review of the Draft Audit Report

After receipt of the draft audit report from the auditor, audited entities will have ten (10) business days to review the draft audit report and provide the auditor their written comments, concerns and corrective actions taken to address any potential violations of the HIPAA Rules.

Step 6: Final Audit Report

The auditor will revise its draft audit report and submit a final audit report to the OCR. Final audit reports must include the following information:

- Identification and description of the audited entity, including the entity's full name, address, EIN, and contact person;
- The methods used by the auditor to conduct the audit;
- A review and description of each audit finding, which should include the following:
  - Condition: The defect or non-compliant status observed by the auditor, and evidence of each defect or non-compliant status;
  - Criteria: A clear demonstration that each negative finding is a potential violation of the HIPAA Rules, including a citation to the specific rule that is potentially violated;
  - Cause: The reason why the condition exists, including an identification of the supporting documentation used to determine such cause;
  - Effect: The risk or non-compliant status that results from the auditor's finding;
  - Recommendations for the audited entity to address each finding; and
  - Corrective actions taken by the audited entity, if any;
- Acknowledgement of any best practice(s) or success(es) of the audited entity; and
- The auditor's overall conclusion.

Audited entities can expect the auditor to take up to thirty (30) business days to submit its final audit report to the OCR.

What Anesthesiologists Can Do

While the OCR is conducting a limited number of audits during this year, anesthesiologists generally are not exempt from inclusion in this pilot program. This pilot period provides anesthesiologists and anesthesia groups with an opportunity to establish HIPAA compliance policies or to revisit existing ones. For those entities that have not had their policies updated recently, this may serve as a good opportunity to have their policies reviewed and updated as well as internally reviewing compliance with their own policies. Moreover, this may be a prime time for anesthesiologists, anesthesia groups and their staff to be trained or re-trained on HIPAA, the necessary requirements for compliance with the HIPAA Rules and consequences for breaching the HIPAA rules.

Anesthesiologists should also familiarize themselves with new risks and vulnerabilities for breaches of patient information. For instance, one such new risk or vulnerability includes the appearance of patient information on social media sites. Anesthesiologists should familiarize themselves with the implication of social media sites and should educate their staff on the proper and improper use of social media in a professional healthcare setting. Another example of increased vulnerability is the use of portable storage (*e.g.*, a flash drive or a thumb drive, laptops, etc.) devices to transport unencrypted patient information. Most breaches of patient information are unintentional. As such, anesthesiologists should be aware of existing and emerging risks and take measures to guard against such risks.

Lastly, anesthesiologists can expect HHS to issue new rules on breach notification this year, finalizing its Interim Final Rule issued in August 2009. Anesthesiologists should ensure that the new rules are incorporated into their compliance policies.

Conclusion

Most anesthesiologists will not be audited during this year; however, those that are can expect a request for information, an on-site visit and an audit report of the findings. Regardless of whether an anesthesiologist is audited, all anesthesiologists should take this opportunity to dust off their HIPAA compliance policies and ensure they reflect the most updated regulations that have been issued.

Neda Mirafzali, Esq. is an associate with Clark Hill, PLC in the firm's Birmingham, MI office. Ms. Mirafzali practices in all areas of health care law, assisting clients with transactional and corporate matters; representing providers and suppliers in health care litigation matters; providing counsel regarding compliance and reimbursement matters; and representing providers and suppliers in third party payor audit appeals. She can be reached at (248) 988-5884 or at nmirafzali@clarkhill.com.