CONTACT

STEPHEN ROSE
206.816.1375
SROSE@GSBLAW.COM

ERIC LINDENAUER
503.553.3117
ELINDENAUER@GSBLAW.COM

EMILY STUDEBAKER
206.816.1417
ESTUDEBAKER@GSBLAW.COM

OCR HIPAA AUDITS

May 2012

On June 10, 2011, KPMG was awarded a $9.2 million contract by the Department of Health and Human Services (HHS) to develop HIPAA audit protocols and then conduct audits based on those protocols of HIPAA Covered Entities and Business Associates. Almost immediately the speculation started on what would be audited and what documents might be requested as part of the HIPAA audit.

HHS gave very few clues of what might be audited but did release a sample letter that would be sent to those selected for audit. [View sample letter: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/sample-ocr_notification_ltr.pdf].

The sample letter did not answer the question of what might be audited as it merely states that accompanying it is a letter from the auditors requesting "certain information be provided by you in order to facilitate the audit process."

From reviewing what has been disclosed by various entities now being audited it appears that the "Sample—Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews" ("Sample Interview document") issued by HHS in February of 2008, gives a very good roadmap of topics that might be covered, documents that might be requested, and identification of personnel that might be interviewed during a HIPAA audit. [View "Sample Interview" document: http://www.gsblaw.com/pdfs/Official-HIPAA-Security-Compliance-Audit-checklist_document-by-DHHS[1].pdf].

It should be noted that one area where the HIPAA audit protocols may differ from the February 2008 Sample Interview document is that the Sample Interview document gives one the impression that all they need do is provide copies of the documents requested while the HIPAA audits make clear that one must produce copies of any documents requested and demonstrate that any policies, procedures, or plans requested have been actually implemented and have been determined to be effective.

While the Sample Interview document gives a fairly comprehensive listing of audit areas, there are some items that have been requested in the initial pilot phase that do not appear on the Sample Interview document. These items include, but are not limited to:

- Notice of Privacy Practices
- Copies of agreements with Business Associates or Business Associate subcontractors

- Procedures for evaluating Business Associates or Business Associate subcontractors prior to entering into a Business Associate Agreement
- Procedures for responding to improper disclosure of PHI
- Procedure for determining whether PHI disclosure constitutes a breach
- Policies and Procedures for responding to breaches
- Breach reporting process

In addition to the above, entities being audited can count on the auditors drilling down in the areas favored by OCR investigators such as:

- Documentation of workforce training upon acceptance of job duties and on an annual basis
- Most current Risk Analysis
- Documentation of incidents, results, mitigation, and employee discipline
- Disaster contingency plans

OCR is also emphasizing the importance of upper management and Board members familiarity and involvement with HIPAA compliance so it will not be surprising if the auditors insist on interviewing any of the following and inquiring about what they view as their role in ensuring HIPAA compliance:

- One or more members of the Board of Directors
- President, CEO or Administrator of the entity
- HIPAA Compliance Officer
- Lead Systems Manager
- Computer Hardware Specialists
- HR Representative
- Incident Response Team Leader

For 2012, OCR has mandated that the HIPAA auditors conduct 150 audits so the odds of being selected are low. However, now is the time to get prepared for your HIPAA audit. If you prepare for a HIPAA audit you put your organization in the best position to prevent the improper disclosure of PHI and will be prepared should you be chosen for an audit. Further, the more prepared you are and the more compliant you are the less the likelihood of having civil money penalties assessed against your organization should you come under review.