FOULSTON SIEFKIN LLP

ATTORNEYS AT LAW

WWW.FOULSTON.COM
WICHITA TOPEKA OVERLAND PARK

HEALTH CARE LAW
FOULSTON SIEFKIN ISSUE ALERT

HIPAA AUDITS ARE HERE:
CAN YOU SATISFY THE AUDITOR OF YOUR COMPLIANCE?

DECEMBER 6, 2011

by Brooke Bennett Aziere
baziere@foulston.com
316.291.9768

THE MOVEMENT TO AUDIT HIPAA COMPLIANCE continues to expand. In 2007, the Office of E-Health Standards and Services posted a sample document request list for on-site HIPAA security audits and CMS established a yearlong contract with PricewaterhouseCoopers to conduct security audits. Now four years later, the Office for Civil Rights (OCR) has continued and expanded its auditing efforts by posting, on November 8, a first glimpse at the details associated with its formal HIPAA Privacy and Security Rules audit program. KPMG, LLP (KPMG), the auditor, began the compliance audits in November, subjecting some providers to an unparalleled level of inquiry.

Audit Program

The audit program is a three-step process. The first step was KPMG's development of the audit protocols. It is unknown whether OCR will make the protocols public.

The second step is an initial group of twenty audits. The initial audit group will be limited to covered entities; no business associates will be selected. Upon completion of the initial group, OCR and KPMG will revisit the protocols and make any necessary revisions before completing the remaining 130 audits no later than December 31, 2012, the third step in the process.

Audit Notification Letter

Covered entities that are selected by OCR will be notified by letter. OCR provides a sample notification letter on its website at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/index.html. Covered entities will be expected to produce all of the requested documentation within ten business days of receiving the letter.

Site Visit

Each audit will include a site visit. The site visit will be completed after KPMG receives and reviews documentation produced by the covered entity in response to the notification letter. OCR anticipates that KPMG will give each entity thirty to ninety days' notice before the site visit. The length of the site visit will vary depending upon the complexity and size of the organization, as well as the auditor's need to access the entity's "key personnel" and "observe processes and operations to help determine compliance." It is worth noting that OCR does not define key personnel or provide any further guidance on how site visits will work. OCR estimates that most site visits will take between three and ten business days.

CONTINUED ON PAGE 2

Report

After the site visit, KPMG will create a draft report and share this report with the entity. The entity will have ten business days to review the report and provide written feedback to the auditor. KPMG will provide a final audit report no later than thirty days after the entity's response and submit it to OCR.

Possible Enforcement Activities

Upon receipt of the auditor's report, OCR will review the final report and use the aggregated results of the audits to gain a better understanding of HIPAA privacy and security compliance in the real world. Although OCR has been somewhat coy on whether the results of audits will lead to enforcement activities, it has certainly left that door open.

Best Practices

OCR also indicates that "best practices" that are gleaned from the audits will be shared with covered entities and business associates. Findings posted by OCR will not contain information that would identify the audited entity.

Take-Away

The take-way from OCR's explanation is three-fold. First, at least initially, the audits will be used to discover weaknesses in HIPAA privacy and security compliance that may be shared by a multitude of covered entities. OCR will identify best practices to address those identified weaknesses. However, entities should beware that OCR has indicated that serious acts of non-compliance discovered during the audit could lead to enforcement action. Second, OCR reminds entities that they are obligated to provide KPMG with their "full cooperation and support" during the audit process. Third, although a covered entity's chance of being selected for an initial audit is relatively small, it should not ignore the fact that the auditor is on the loose. Entities need to make sure their HIPAA privacy and security policies are fully implemented and up-to-date, so they will be able to respond within the relatively short time frames.

For Further Information

If you have questions or want more information, you should contact your legal counsel to ensure compliance with the new HIPAA audit program. If you do not have regular counsel, Foulston Siefkin LLP would welcome the opportunity to work with you to specifically meet your business needs. Brooke Bennett Aziere and Marta Fisher Linenberger are available to assist you. Brooke Bennett Aziere can be reached at 316.291.9768 or **baziere@foulston.com** and Marta Fisher Linenberger can be reached at 785-233-3600 or **mlinenberger@foulston.com.** If you are looking for general health care counsel you may contact Scott Palecki at (316) 291-9578 or **spalecki@foulston.com**.

Foulston Siefkin's health care lawyers maintain a high level of expertise regarding federal and state regulations affecting the health care industry. The firm devotes significant resources to ensure our attorneys remain up-to-date on daily developments. At the same time, the relationship of our health care law practice group with Foulston Siefkin's other practice groups, including the taxation, general business, labor and employment, and commercial litigation groups, enhances our ability to consider all of the legal ramifications of any situation or strategy. For more information on the firm, please visit our website at **www.foulston.com**.

####