eALERT

INCompliance

July 6, 2012

Despite What GAO Says — OCR has a Plan

HIPAA Audit Protocols and OCR's Plan for Future HIPAA Audits

On Friday June 22, 2012, the Government Accountability Officer (GAO) issued a report to Congress containing a review of the guidance and oversight of health privacy and security by the Department of Health and Human Services (HHS).

The report noted the current Health Insurance Portability and Accountability Act (HIPAA) audits conducted by the Office of Civil Rights (OCR) but criticized HHS for not having future audit plans. The report found:

> *HHS was also required by law to implement periodic compliance audits of covered entities' compliance with HHS privacy and security requirements; however, while it has initiated a pilot program for conducting such audits, it does not have plans for establishing a sustained audit capability. According to OCR officials, the office has completed 20 audits and plans to complete 95 more by the end of December 2012, but it has not established plans for continuing the audit program after the completion of the pilots or for auditing covered entities' business associates. Without a plan for establishing an ongoing audit capability, OCR will have limited assurance that covered entities and business associates are complying with requirements for protecting the privacy and security of individuals' personal health information.*

But at the American Health Lawyers Association (AHLA) annual meeting on Monday June 25, 2012, David Mayer from OCR stated that this is no longer correct. Mr. Mayer stated that OCR "will have HIPAA audits for next several years at least" with at least same scope of current initial audits.

Covered entities should continue to be prepared for a possible audit. On June 26, 2012, OCR posted the audit program protocol on its website.

The audit program protocol contains the requirements to be assessed through the HIPAA audits. The audit program protocol covers:

- Privacy Rule requirements for (1) notice of privacy practices for PHI, (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative

requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures;

- Security Rule requirements for administrative, physical, and technical safeguards; and

- Requirements for the Breach Notification Rule.

However, OCR notes that the combination of these multiple requirements may vary based on the type of covered entity selected for review.

On the website, OCR has listed the audit procedures for each requirement. Additional background on the HIPAA audits and procedure used by OCR is available here.

This E-Mail Alert was prepared by Allen Killworth (akillworth@incomplianceconsulting.com). Please contact us at: info@incomplianceconsulting.com for more information. This and previous E-Mail Alerts may be accessed here.