Arnall Golden Gregory LLP

Client Alert

Contact Attorney Regarding This Matter:

H. Carol Saul
404.873.8694 - direct
404.873.8695 - fax
carol.saul@agg.com

OCR HIPAA Audit Update

The Department of Health and Human Services (HHS), Office of Civil Rights (OCR), awarded a $9.2 million contract to KPMG LLP on June 10, signaling the start of OCR's proactive and intensified Health Insurance Portability and Accountability Act (HIPAA) audit process. Historically, most OCR auditing has been reactive, in response to complaints of violations of the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information, or Security Rule, which sets national standards for the security of electronic, protected health information. Section 13,411 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, however, mandates that HHS conduct periodic, proactive audits to determine compliance.

Earlier this year, HHS awarded two contracts to technology consulting firm Booz Allen Hamilton:

1. To outline potential audit methodologies; and
2. To identify potential audit targets.

To date, neither report has been made publicly available. Similarly, little has been disclosed about KPMG's audit plans, although it is charged with designing the audit protocol as well as conducting the audits. Most of what is known has been gleaned from the OCR Award Notice, including the following:

- Both covered entities and business associates will be audited;
- Audits will occur at least in part on-site;
- Site visits will include interviews with leadership (e.g., chief information officer, privacy officer, legal counsel, health information management or medical records administrator);
- Auditors will examine physical operations and determine whether policies and processes meet regulatory requirements;
- KPMG will submit a report to include its timeline and methodology, best practices noted, raw data collected, and recommendations for corrective action and future oversight; and
- Completion of 150 audits is anticipated by the end of 2012.

Many questions remain about the audits, including how audit targets will be selected, when audits will begin and, perhaps most importantly, whether audit results will lead to civil monetary penalties or simply be used as an educational tool.

Arnall Golden Gregory LLP
Attorneys at Law
171 17th Street NW
Suite 2100
Atlanta, GA 30363-1031
404.873.8500
www.agg.com

Susan McAndrew, OCR's deputy director for privacy, has previously given some clues regarding the possible OCR audit focus. She stated in a May 2010 presentation, discussing the mandatory audits, that the audit starting point will be making sure companies have done and documented a risk assessment, a foundational requirement of the Security Rule. She also noted that reported breaches indicate external threats are a significant issue, so that physical safeguards should be a focus. With regard to the Privacy Rule, Ms. McAndrew noted concerns regarding patient access to medical records, internal access controls and internal staff improperly accessing records, including those of celebrities and family members.

While the odds of being selected for one of the anticipated KPMG audits are slim, both covered entities and business associates should consider taking steps now to prepare. Priorities for audit readiness should include the following:

- Ensuring you have an up-to-date, documented security risk assessment; CMS offers risk assessment guidance online here;[1]
- Making sure your written policies are updated for HITECH Act changes and changes to your operations, and that your policies are being followed;
- Determining whether those likely to be interviewed are knowledgeable regarding regulatory requirements and can articulate how your organization meets those requirements, including how you address those Security Rule specifications that are "addressable" rather than "required;"
- Making sure your documentation is organized by asking question like, for example, whether you have executed business associate agreements where required and whether copies are maintained in one location; and
- Making sure all workforce members have been trained and that you have documentation to prove it.

1 www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.pdf