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

Details Emerge About Looming OCR HIPAA Audits

The Health Information Technology for Economic and Clinical Health (HITECH) Act mandated that the Department of Health and Human Services (HHS) conduct proactive audits of covered entities' and business associates' compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. In June, HHS' Office of Civil Rights (OCR), which is charged with HIPAA enforcement responsibility, awarded a contract to U.S. audit, tax and advisory services firm KPMG to assist in designing and carrying out those audits. The contract award discloses that OCR anticipates 150 such audits will be conducted by the end of 2012.

While a number of questions about the OCR audit process have not been answered, OCR's Deputy Director for Health Information Privacy Susan McAndrew, in a webinar hosted by the International Association of Privacy Professionals last week, shared new details, including the following:

- OCR regards the audit process as a separate function from enforcement, in part because the statutory language mandating the proactive audits is not within the statute's enforcement provisions.
- Despite the foregoing, where audits uncover instances of serious noncompliance, referrals may be made to investigatory units and compliance reviews may be triggered, with the potential for a corrective action plans, resolution agreements and civil monetary penalties.
- The audit process will attempt to identify both vulnerabilities to be addressed and best practices, and will endeavor to provide positive feedback.
- Audit targets will be objectively selected based upon general risk categories (size and type of entity), not based on those who have experienced an actual breach or other violation of law.
- Due to the relative difficulty in identifying the universe of business associates, the audits will initially focus on covered entities rather than their business associates. (HHS estimates, based upon a business census conducted by the Small Business Administration, that there are more than 700,000 HIPAA-covered entities, so the odds of being audited are extremely low.)

Arnall Golden Gregory LLP
Attorneys at Law

171 17th Street NW
Suite 2100
Atlanta, GA 30363-1031
404.873.8500

2001 Pennsylvania Avenue NW
Suite 250
Washington DC 20006
202.677.4030

www.agg.com

- Audit protocols will be scalable to the size and operations of the entity.
- Audit subjects will be given advanced notice of the audit and likely will receive requests for documents prior to an onsite audit.
- Audit subjects will be given an opportunity to comment before findings are made final, and will be required to report back regarding recommended remedial action.
- OCR plans to make audit findings public, but only in an aggregate format, so that identified vulnerabilities will not be linked to a particular audit subject.
- Regarding timing, OCR anticipates a two- to four-month development phase, followed by a test phase in late 2011, with the majority of the audits being conducted throughout 2012.

OCR has not yet stated whether its audit protocols will be made public. It also is not known whether OCR audits will continue beyond 2012, when HITECH Act funding will no longer be available. However, it should be noted that OCR is permitted to retain the dollars it collects through enforcement, and those dollars could be a funding source for audits beyond 2012.