



Office for Civil Rights Launches HIPAA Compliance Audits

By Arthur Yermash, Esq.

In November 2011, The Department of Health and Human Services' Office for Civil Rights (OCR) announced a new effort to audit covered entity and business associate compliance under Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act (HIPAA and HITECH are jointly referred to as HIPAA).

As authorized and required under HIPAA, OCR will begin conducting HIPAA compliance audits at covered entities and business associates in order to uncover risks or vulnerabilities in the privacy and security rules under HIPAA. OCR is expected to perform 150 audits by the end of 2012. The Audit Program is primarily intended to improve OCR's understanding of compliance efforts with particular aspects of the Standards, to determine what types of technical assistance should be developed and to determine what types of corrective actions are being developed. OCR will share best practices identified during the Pilot Audit Program and issue guidance on common compliance challenges, but it will not publish a list of the audited covered entities or any findings of an audit that could identify an audited entity.

The OCR has engaged a private contractor, accounting firm KPMG LLP, to conduct the audits. Entities that are being audited will be required to respond to KPMG document requests within 10 business days of receipt and will likely have 30 to 90 days' notice of the on-site visit by KPMG. The on-site visit will last three to 10 business days depending on the complexity of the organization. KPMG will provide its draft report to the audited entity for review and comment, give the entity 10 business days for that review and then submit its final report to OCR.

Under Section 13411, any covered entity or business associate is eligible to be audited. For the pilot program, however, only covered entities will be targeted. OCR states that it will use a selection of a broad range of covered entities in order to ensure its auditing protocols are put to the test across a wide variety of scenarios. Specifically, OCR cites "covered individual and organizational providers of health services, health plans of all sizes and functions, and health care clearinghouses" as potential targets for the pilot. According to OCR's audit protocols, the goal is to complete each audit within 180 days from the date the notification letter is sent.

CLIENT ADVISORY

2011



Even though business associates are excluded from direct consideration for the pilot, it is possible that a target's business associate could be indirectly implicated in a pilot audit. HIPAA requires that all Business Associates comply with and be directly subject to the rules and regulations promulgated under HIPAA. HIPAA requires that Business Associate agree to such obligations pursuant to contracts between the covered entity and the Business Associate (known as Business Associate Agreements).

While the pilot-program will only select a very small percentage of covered entities to be audited, it is representative of OCR's stepped up efforts to enforce and ensure compliance. Accordingly, it would be prudent for covered entities, as well as Business Associates to revisit their HIPAA/HITECH compliance policies and procedures and ensure that they have completed and documented at least one security risk assessment consistent with the HIPAA security standards.



Clients who have any further questions or concerns about the information contained in this Advisory should not hesitate to contact us.

Joseph N. Campolo, Esq.
631.738.9100 x 301
jcampolo@cmmllp.com

Arthur Yermash, Esq.
631.738.9100 x 304
ayermash@cmmllp.com

ATTORNEY ADVERTISING: This publication may be considered "advertising material" under the rules of professional conduct governing attorneys in New York State. This advisory is for guidance only and not intended to be a substitute for specific legal advice. Prior results do not guarantee similar outcomes.