SEYFARTH SHAW LLP
ATTORNEYS

One Minute Memo®

Are Your HIPAA Policies in Place?

HIPAA Audits Underway - Prototcols Posted

The U.S. Department of Health and Human Services, Office of Civil Rights (OCR) enforces the privacy and security rules set forth in the Health Insurance Portability and Accountability Act, as amended (HIPAA). In 2011, OCR instituted a pilot audit program whereby OCR began analyzing the HIPAA processes, controls and policies in place for selected covered entities, but not business associates. Having started pilot audits last November, on June 26, 2012, OCR posted the protocol(s) it will use to conduct future audits, which will eventually be expanded to include business associates. (You can access their website and view these protocols by clicking *here*.)

The protocols list the performance criteria on which OCR will focus and the audit procedures OCR will enlist when auditing a covered entity's compliance with the *security rules*, the *breach notification rules*, and the *privacy rules*. The audit procedures consist of OCR both interviewing management and members of the workforce, and obtaining and reviewing HIPAA privacy and security documents.

HIPAA Security Breach Results in $1,700,000 Penalty Settlement

In addition to auditing covered entities for compliance with HIPAA, OCR investigates breach reports submitted to OCR by covered entities and business associates, as required by law. The Alaska Department of Health and Social Services (DHSS) submitted a breach report to OCR, which triggered an investigation. DHSS reported that a portable electronic storage device possibly containing electronic-PHI had been stolen from a vehicle of a DHSS employee. After investigating, OCR determined that DHSS did not have adequate policies and procedures in place to safeguard PHI. DHSS recently agreed to pay $1,700,000 to settle the potential violations of the HIPAA security rules. As part of the settlement, DHSS also agreed to comply with a "Corrective Action Plan" whereby DHSS was required to develop and distribute written security policies, obtain certification from all employees who have access to e-PHI that they have read and understand the policies, update the security policies at least annually, train all employees who have access to e-PHI at least annually on the security policies, and obtain certification from all trained employees that they have received training.

More HIPAA Guidance Coming

In early June, OCR indicated that it was "extremely close" to publishing a final omnibus HIPAA rule which was expected to include a final breach notification rule, a final enforcement rule, a final rule implementing changes to the privacy and security standards, and a final rule modifying HIPAA's privacy rule in accordance with the Genetic Information and Discrimination Act. The omnibus rule was sent to the White House Office of Management and Budget (OMB) on March 26, 2012 for review, and the review process usually takes 90 days. Nevertheless, and despite that OCR intends to implement a permanent audit program by December, the OMB announced on June 22, 2012 that it is extending its review of the omnibus rule to an unspecified date in the future.

To Do List

Notwithstanding the delay in issuing the final omnibus HIPAA rules, in light of OCR's significant enforcement actions, plan sponsors should:

- Ensure they have in place HIPAA privacy and security policies, a privacy notice, and business associate agreements with each of their business associates.
- Ensure all employees who have access to PHI are trained on the plan's privacy policies and that all employees who have access to e-PHI are trained on the plan's security policies.

By: *Joy Sellstrom*

Joy Sellstrom is senior counsel in Seyfarth's Chicago office. If you would like further information or help in implementing a HIPAA compliance program, please contact your Seyfarth Shaw LLP attorney or Joy Sellstrom at *jsellstrom@seyfarth.com*.