Legal Alert: Are You Ready for a HIPAA Audit?: OCR's HIPAA Audit Program is Underway

12/12/2011

***Executive Summary*:** The U.S. Department of Health and Human Services' Office for Civil Rights (OCR) recently launched a pilot audit program as part of its HIPAA enforcement efforts. OCR intends to audit a range of HIPAA-covered entities and plans to use resulting audit reports to determine what types of technical assistance should be developed and what types of corrective action are most effective. Audits conducted during the pilot phase will conclude by December 2012. In addition to the audit program, OCR will continue to accept HIPAA-related complaints from individuals.

Every covered entity and business associate is eligible for an audit, including employers who are plan sponsors of a group health plan. OCR will audit as wide a range of types and sizes of covered entities as possible during the initial pilot. OCR has stated that business associates would be included in future audits.

When a covered entity is selected for an audit, OCR will notify the covered entity in writing. OCR expects covered entities and business associates who are the subject of the audit to provide requested information within 10 business days of the request for information. Such information will include, at minimum, documentation of their privacy and security compliance efforts (e.g. policies, forms, notices, training materials, etc.). Additionally, OCR will conduct on-site visits, interviewing key personnel and observing the covered entity's operations for compliance.

Common HIPAA Issues Requiring Corrective Action

In 2010, OCR received over 8,000 HIPAA-related complaints. OCR identified the following top five HIPAA-compliance issues in 2010:

• Impermissible Uses & Disclosures

• Improper Safeguards

• Access to PHI

• Providing the Minimum Necessary PHI

• Notice Obligations

In the employment context, HIPAA violations can occur when a supervisor

accesses, examines, and discloses an employee's medical records without employee authorization.

Types of Corrective Action

Covered entities who experience a HIPAA breach must, among other things, provide notice to affected individuals and take steps to mitigate the harm and prevent further breaches. To correct HIPAA violations, OCR has, among other actions, required covered entities to install computer monitor privacy screens to prevent impermissible disclosures, implement or correct computer program features, enter into a business associate agreement, train staff, and counsel employees who violate HIPAA policies.

Potential Penalties

The American Recovery and Reinvestment Act of 2009 (ARRA) increased civil monetary penalties for HIPAA violations. The Act establishes tiers of penalties based upon whether a covered entity knew of the HIPAA breach, whether the breach was due to willful neglect, and whether proper corrections were made. The tiers of penalties are as follows:

• $100/violation not to exceed $25,000/calendar year.

• $1,000/violation not to exceed $100,000/calendar year.

• $10,000/violation not to exceed $250,000/calendar year.

• $50,000/violation not to exceed $1,5000,000/calendar year.

In February 2011, HHS imposed its first civil money penalty, in the amount of $4.3 million, for violations of the HIPAA Privacy Rule. In that particular case, OCR found that the covered entity, a health care provider, violated 41 individuals' rights by denying them access to their medical records. Further, the covered entity failed to cooperate with OCR investigators.

Preparing for Possible Audits & Everyday Compliance

The pilot audit program represents OCR's increased enforcement efforts to ensure HIPAA compliance. For covered entities that have developed and updated their HIPAA procedures and related training programs, little additional preparation may be required. However, for many other covered entities, this is a good time to revisit their current HIPAA policies and procedures for compliance with privacy and security standards.

Ford & Harrison has worked with all types of covered entities on implementing and updating their HIPAA policies. Our firm can also assist with training and compliance materials.

If you have any questions regarding this Alert, or would like additional details concerning HIPAA compliance, you can contact the author of this Alert, Isabella Lee, ilee@fordharrison.com, any member of Ford & Harrison's Employee Benefits practice group, or the Ford & Harrison attorney with whom you usually work.