March 2nd, 2012

THE GROUP BENEFIT NEWS BULLETIN

HIPAA Privacy Audits Pilot Program – Is Your Plan Compliant?

Pursuant to the American Recovery and Reinvestment Act and Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, periodic audits must be supplied by Health & Human Services (HHS) to ensure compliance with the Health Insurance Portability and Accountability Act's (HIPAA) Privacy and Security Rules, and Breach Notification standards. The Office for Civil Rights (OCR) within HHS began the pilot phase in November 2011 and it will last until December 2012. The pilot involves 150 covered entities, including both insured and self-insured group health plans.

Under this compliance-centric arena, plan sponsors are encouraged more than ever to seek counsel and review their compliance program making certain to include::

- Updated HIPAA Security Risk Assessment – Plan sponsors without a periodic HIPAA security risk assessment since their initial assessment in 2004-2005 are long overdue, particularly if they have adopted any new systems, technologies or websites with interactive features
- Current policies and procedures consistent with actual privacy and security practices.
- Updated Privacy Policy Manuals
- Updated HITECH-compliant Business Associates Agreements
- Updated HITECH-compliant Breach Notification and Log Policies – Covered entities and business associates are required to comply with breach notification provisions that took effect under HITECH. In the instance of a breach of unsecured Protected Health Information (PHI), covered entities must notify affected individuals and the HHS Secretary. When large-scale breaches (any breach affecting more than 500 people) occur, the media must also be informed. Common causes of large-scale breaches are theft or loss of paper records or electronic media (laptops, desktop computers, smart phones, flash drives, network servers, etc.), unauthorized access or use of PHI, human or technological error (misdirected email, mail, etc.) and improper disposal of paper records.

There has been no announcement regarding selection criteria for the pilot phase audit candidates, other than stating they will be of varying types and sizes to give a broad assessment of a complex and diverse health care industry. Speculation is that complaints or media reports regarding privacy or security breaches could be potential "red flags" to drive selection. OCR will consider all covered entities, covered providers of health services, health plans of all sizes and functions, and health care clearinghouses for audit eligibility.

Accounting firm, KPMG LLP, has been contracted to conduct the audits. Once an entity has been chosen for an audit, they will receive a documents request from KPMG. Upon receipt of the documents request, entities should contact legal counsel immediately as they are expected to provide the documentation within 10 business days of the request receipt. OCR expects to notify the entity 30 to 90 days in advance of an on-site visit, which will usually last between 3 and 10 business days, depending on the complexity of the organization. Upon completion, KPMG will provide the entity with a draft report, and they will have 10 business days to review and provide written comments back to the auditor. The auditor will complete a final audit report within 30 business days after the response period and submit it to OCR.

Following the audit, OCR will review final reports to analyze the HIPAA compliance efforts of the entities audited. This analysis will be used to determine different types of technical assistance to be developed and the most effective corrective actions. If serious compliance problems are uncovered during an audit, OCR may initiate a compliance review to address the problem. OCR will not be releasing any publications clearly identifying any audited entities.

***Note: See the attached OCR Sample Letter that an audit candidate might receive upon selection.**

As always, TBPG will continue to monitor all updates and keep you informed of any pertinent information. If you have any questions, please contact your TBPG representative.

DEPARTMENT OF HEALTH AND HUMAN SERVICES **OFFICE OF THE SECRETARY**

Voice – (202) 619-0403 TDD – (202) 619-2357 FAX – (202) 619-3818
http://www.hhs.gov/ocr

Office for Civil Rights
200 Independence Ave., SW; RM 509F
Washington, DC 20201

Date
Name of Entity
Address of Entity
Point of Contact of Entity

Dear Covered Entity:

The Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS) has responsibility for administration and enforcement of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules (45 CFR Part 160 and Part 164 Subparts C and E). These rules are designed to provide important health information privacy and security protections and rights for individuals. The OCR is committed to developing and enforcing strong health information privacy protections that do not impede access to quality health care.

The American Recovery and Reinvestment Act of 2009 (ARRA) requires HHS to audit covered entity and business associate compliance with the HIPAA privacy and security standards. To effectively implement this statutory mandate, OCR has engaged the services of a professional public accounting firm (KPMG LLP) to conduct performance audits, using generally accepted government auditing standards. You are receiving this letter because OCR has selected [Name of entity] to be the subject of an audit.

These audits are a new facet of the OCR health information privacy and security compliance program. Audits present an opportunity to examine mechanisms for compliance, identify best practices and discover risks and vulnerabilities that may not have come to light through OCR's established complaint investigations and compliance reviews. OCR will broadly share best practices gleaned through the audit process and guidance targeted to observed compliance challenges. OCR will assess whether to open a separate compliance review in cases where an audit indicates serious compliance issues.

Request for Information and Points of Contact

In the attached letter, KPMG LLP requests certain information be provided by you in order to facilitate the audit process. Additionally, they provide contact information for the audit firm personnel responsible for conducting the audit. Please recognize that KPMG LLP is requesting and reviewing these documents solely as a contractor to OCR and on its behalf and pursuant to its audit authority. This letter serves to notify you that the audit shall begin within the next 30 to 90 calendar days from the date of this letter. The results of the audit firm's work, including your management's written response to any reportable findings will be presented in a final report to OCR.

We expect you to provide KPMG LLP your full cooperation and support and remind you of your cooperation obligations under the HIPAA Enforcement Rule.

Sincerely,

Leon Rodriguez
Director
Office for Civil Rights, DHHS