

New HIPAA Requirements: Omnibus Regulatory Changes 1.25.2013

By Charles James, Jr.

HIPAA has been with us for many years now. We all know that HIPAA was born in the interest of administrative simplification, of which little has happened! We will leave the regulatory history of HIPAA for another time and focus on the changes that are going into effect on September 23, 2013. There are several components.

For Covered Entities, there are several revisions to notices of privacy practice that need to be distributed to patients. These revisions to be included are specific statements regarding the use or disclosure of psychotherapy notes, PHI for marketing, sale of PHI, fundraising, genetic information, among others which must be communicated to patients. Therefore, HIPAA notices of privacy practices will need to be updated and distributed to patients.

Another major change is that Business Associates are now subject to the same requirements and penalties as Covered Entities. According to HHS, a Business Associate "is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. Your billing company or Rural Health Clinic consultants are definitely Business Associates. Some HHS examples of Business Associates are:

- A third party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involve access to protected health info.
- An attorney whose legal services to a health plan involve access to protected health information.
- A consultant that performs utilization reviews for a hospital.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html>

Business Associates must comply with HIPAA physical and security safeguards and issue breach notifications as if they were covered entities. Covered Entities are liable for the actions IF their Business Associates are determined 'agents' of the Covered Entity. Audits of Business Associates are to begin after the September 23rd deadline. All Business Associate agreements will have to be updated with new language and re-signed with the appropriate parties.

Enforcement and penalties of HIPAA breaches have also been increased. For example, the penalty for a violation due to reasonable cause has been increased from \$100 per violation and a \$25,000 maximum to \$1,000 per violation and a \$100,000 maximum...per violation! Enforcement through increased HIPAA audits of Covered Entities and Business Associates is expected.

The biggest action item is the Security Risk Assessment. A security risk assessment must be performed by September 23rd, 2013. The risk assessments "should identify and document potential threats and vulnerabilities, assess current security measures, determine the likelihood of the threat occurring, determine the potential impact of threat occurrence, determine the level of risk, and identify security measures..." (CMS Basics of Risk Analysis and Risk Management).

The bottom line is that more changes to HIPAA compliance are in our immediate future. It is imperative that your practice has reviewed and implemented the required physical and security safeguards now being required. Your HIPAA policies must be reviewed, updated, and communicated to staff as well. There are many tools available for HIPAA risk assessments, compliance and education - many from vendors who will be at our fall conference. A HIPAA education session is on the agenda at the upcoming conference in Indianapolis in October. In the meantime - you likely have HIPAA homework! We hope to see you in Indy!

Charles James, Jr.

MBA, North American Healthcare Management Services
Board Member, NARHC