HIPAA Business Associates

Outside auditors are business associates! This means that you and/or your company is required to safeguard protected health information in the same manner as your clients - healthcare providers. Each of your clients, as covered entities, should initiate a business associate agreement with you, but if they don't, then you should send them a signed agreement that meets the HIPAA requirements.

A ***covered entity*** is a health plan, a health care clearinghouse, or a health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.

A **b*usiness associate*** is any individual or entity that creates, maintains, processes, or transmits protected health information on the behalf of a covered entity but is not part of the workforce of that covered entity.

A Business Associate Agreement is a contract between the covered entity and the business associate that holds the business associate to the HIPAA Security Rule guidelines. As business associates, you are required to hold your subcontractors (business associates of business associates) to the same standards, preferably with a signed agreement.

What are the safeguards HIPAA requires business associates to implement to protect health information?

Administrative Safeguards - Actions, policies and procedures security to protect electronic protected health information and to manage the conduct to the workforce in relation to protecting healthcare information. Administrative safeguards are over half of all required safeguards and include staff training, incident response, contingency plan, business associate agreement, workforce security, and much, much more.

Technical Safeguards - Access and audit controls, integrity, person/entity authentication, and transmission security.

Physical Safeguards - facility access controls, workstation use and security, device and media controls.

Your HIPAA compliance begins with written policies and procedures (administrative controls). Next is a security analysis to determine risks and help develop appropriate controls.

One of the most recent enforcement proceedings cost an oncology group $750,000. A laptop bag holding an employee's computer and unencrypted backup media was stolen from the employee's automobile. It contained names, addresses, dates of birth, Social Security Numbers, insurance information and clinical information of about 55,000 patients. This covered entity was found in widespread non-compliance with the HIPAA rule, including the lack of a security risk analysis and written policy concerning removal of hardware and media containing ePHI.

The Office for Civil Rights is the enforcement agency for HIPAA rules. No business associates were included in the first round of "routine inspections," but they will be included when round two gets underway.

The HIPAA website, www.hhs.gov/ocr/privacy/hipaa has a lot of information, including a sample Business Associate Agreement.

DoctorsManagement has a customizable HIPAA Omnibus Manual. While primarily geared toward covered entities, it can be used by business associates as well. This

manual and other tools may be ordered on the DoctorsManagement website: *www.doctors-management.com*

This Week's Tip Provided By:

Ann Bachman, BS MT(ASCP), CLC(AMT)
Ann serves as Partner and Director of Regulatory Compliance for our parent company, DoctorsManagement LLC