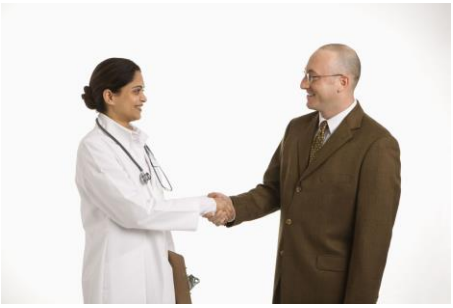
HIPAA Business Associate Management – 2016 update



In 2016,

- A hospital was fined $ 2.7 million for storing patient data with a cloud service without having a Business Associate Agreement in place.
- Another hospital was penalized $ 1.55 million, and a medical practice was fined $ 750,000, for sharing Protected Health Information (PHI) with a vendor without having a signed Business Associate Agreement.
- A Business Associate was fined $ 650,000 for losing just 412 patient records.
- A health care provider was fined $ 400,000 sharing data with the health system of which it was a member, in the absence of an updated Business Associate Agreement.

"HIPAA's obligation on covered entities to obtain business associate agreements is more than a mere check-the-box paperwork exercise," said Jocelyn Samuels, Director of the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR). "It is critical for entities to know to whom they are handing PHI and to obtain assurances that the information will be protected."

Also in 2016, for the first time Business Associates are being audited by the federal government, if one of their Covered Entity clients was selected for an audit. If the Business Associate fails, this can have a negative impact on their client.

HISTORY

Since 2003, HIPAA Covered Entities and Business Associates have been required to sign Business Associate Agreements. The HIPAA Omnibus Final Rule announced in January, 2013, increased the liability for Business Associates; required them to implement HIPAA compliance programs, expanded the definition of Business Associates; and requires Business Associates to be responsible for the compliance of their Subcontractors.

Covered Entities and Business Associates must work with each other to protect health information. Covered Entities must identify all of their Business Associates and sign agreements. Business Associates must identify all of their Subcontractors and sign agreements. Subcontractors must identify their Subcontractors and sign agreements. Everyone down the line from the patient is responsible for complying with HIPAA and protecting patient data. This chain can be long and involve multiple layers.

A Covered Entity can provide services to another Covered Entity, creating a Business Associate relationship between the two Covered Entities. Sometimes a parent organization acts as a Business Associate to a member organization, depending on the structure of the organizations.

DEFINITIONS

Covered Entity

A health provider that electronically bills Medicare or insurance companies, or a payer (Medicare, Medicaid, Private Insurance Company, or Self-Insurer). Covered Entities are allowed to share Protected Health Information between themselves for the purposes of Treatment, Payment, and Operations. In certain circumstances Covered Entities can be Business Associates.

Business Associate

A person or entity that comes in contact with patient data while performing services for a Covered Entity. Under the new HIPAA Omnibus Final Rule data centers, online backup companies, and Cloud Services providers are considered Business Associates if they store data—even if they do not, or cannot, access it. A Covered Entity becomes a Business Associate of another Covered Entity when the services it is providing is not related to the shared treatment of a patient. Examples we have dealt with include a hospital providing after-hours phone answering services to local medical providers, and a parent organization of a national charity that provides shared IT services to local chapters.

Subcontractor

A person or entity that comes in contact with patient data while performing services for a Business Associate. Under the new HIPAA Omnibus Final Rule data centers, online backup companies, and Cloud Services providers are considered Subcontractors of Business Associates if they store data—even if they do not, or cannot, access it.

PRIVACY CHAIN OF TRUST

PATIENT → COVERED ENTITY → BUSINESS ASSOCIATE → SUBCONTRACTOR 1 → SUBCONTRACTOR 2
PATIENT → DOCTOR → IT MANAGED SERVICE PROVIDER → ONLINE BACKUP PROVIDER → DATA CENTER(S)

Conduit

An organization that simply moves health care information and cannot access it, such as the Postal Service, UPS, Fedex, and Internet Service Providers (that do not offer storage or backup services.) These organizations are not Business Associates and do not require a BA Agreement.

BUSINESS ASSOCIATE EXAMPLES

- IT companies that support health care providers
- Electronic Health Record (EHR) system providers
- Data centers, online backup companies, Cloud service providers, even if they do not access data, or if data is encrypted
- Collections companies
- Shredding companies
- Insurance agents
- A CPA firm whose accounting services to a health care provider involve access to protected health information.
- An attorney whose legal services to a health plan or provider 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.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan's pharmacist network.

SUBCONTRACTOR EXAMPLES

- Any person or entity providing services to a Business Associate that requires access to PHI
- Data centers, online backup companies, Cloud service providers, providing services to a Business Associate, even if they do not access data

AGREEMENTS

Business Associate Agreement

A written agreement that Business Associates sign with Covered Entities, containing, at a minimum, specific terminology requiring that the Business Associate will access patient data only for specific purposes; will keep the data confidential; will comply with HIPAA; and will ensure the compliance of any Subcontractors with which they work. BA Agreements are contracts between two entities, and can come from either party.

Subcontractor Business Associate Agreement

A written agreement that Business Associates sign with Business Associates, containing, at a minimum, specific terminology requiring that the Business Associate will access patient data only for specific purposes; will keep the data confidential; will comply with HIPAA; and will ensure the compliance of any Subcontractors with which they work. Subcontractor BA Agreements are contracts between two entities, and can come from either party. Subcontractors do not have to sign BA Agreements with Covered Entities, although some Covered Entities require this.

REPORTING REQUIREMENTS

Covered Entities must report data breaches to affected patients and to the US Dept. of Health & Human Services (HHS) Office for Civil Rights (OCR). Breaches of over 500 records must be reported within 60 days (5 days in California.) Breaches of fewer than 500 records must be reported annually. Patients must be notified immediately.

Business Associates must report data breaches to Covered Entities, not to patients or OCR, in enough time for the Covered Entities to comply with reporting deadlines.

Subcontractors must report data breaches to Business Associates, not to patients or OCR, in enough time for the Covered Entities to comply with reporting deadlines.

QUESTIONS…

- **COVERED ENTITIES SHOULD ASK VENDORS THAT MAINTAIN OR MAY COME IN CONTACT WITH PHI**
- **BUSINESS ASSOCIATES SHOULD ASK SUBCONTRACTORS THAT MAINTAIN OR MAY COME IN CONTACT WITH PHI**
  1. Do you acknowledge that your organization provides services that qualify you as a HIPAA Business Associate?
  2. Will your organization sign HIPAA Business Associate Agreements with us before the enforcement deadline of 9/23/2013?
  3. Has your organization implement HIPAA-specific policies and procedures, and complete a HIPAA risk analysis and workforce training?
  4. Will your organization submit to a 3rd party audit of your HIPAA compliance efforts?

If you believe your vendor is a Business Associate, but they will not sign a BA Agreement or agree to HIPAA compliance, any PHI you share with them is a data breach—a violation of the law that must be reported up the line from Subcontractors to Business Associates to Covered Entities to Patients and the Federal Government. You should switch to another vendor prior to the enforcement deadline.

RESOURCES

Business Associates http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html
Business Associate Agreements (revised 1/25/2013) http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
Business Associate Frequently Asked Questions http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/index.html

Semel Consulting works with Covered Entities, Business Associates, and Subcontractors to properly manage HIPAA compliance.

SEMEL CONSULTING
www.semelconsulting.com