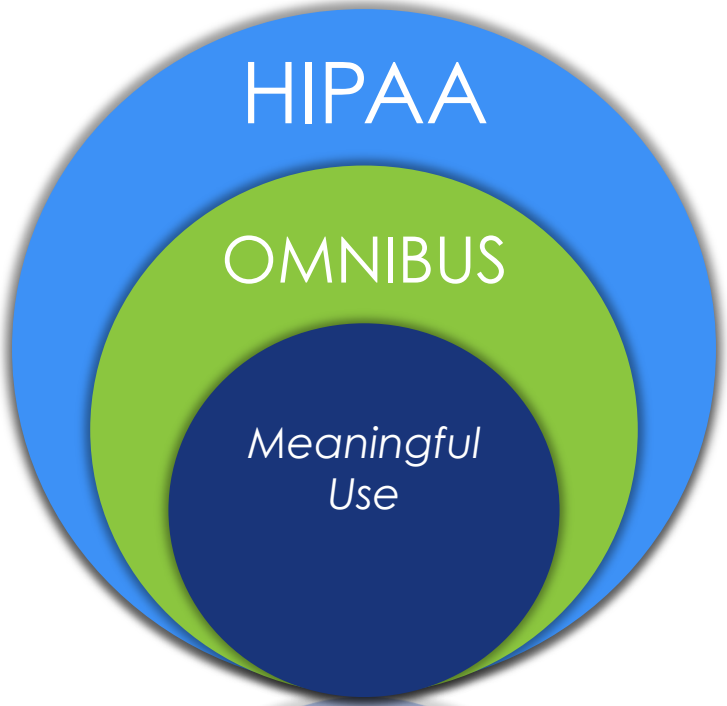
The Relationship Between HIPAA Compliance and Business Associates

What is HIPAA?

- **HIPAA / HITECH**
  - Protect patient confidentiality while furthering innovation and patient care
- **Omnibus** (September 2013)
  - Business Associates must protect PHI
- **Meaningful Use**
  - Accelerate adoption of EHR (electronic Health records)
- **Compliance vs. Security**
  - Fines vs. Risk



The HIPAA Compliance Puzzle

What are your responsibilities?

- Have an up-to-date BAA (Business Associate Agreement)
- Confirm the Business Associate:
  - Uses the information only for the purposes for which it was engaged for
  - Will safeguard the information from misuse
  - Help the covered entity comply with some of the covered entity's duties under the Privacy Rule.

What the Omnibus Rule changed for Business Associates

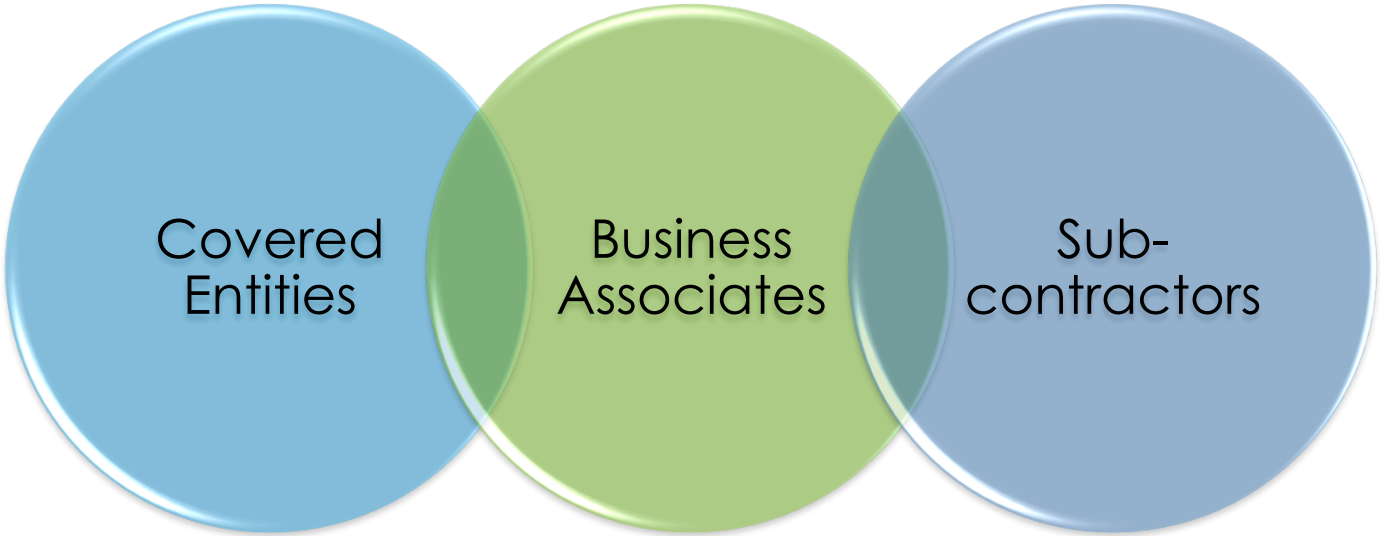
- Direct liability by function
  - Directly liable for violations
- Compliance with Security Rule
  - **Technical** Safeguards
  - **Administrative** Safeguards
  - **Physical** Safeguards
- Compliance with Privacy Rule
  - For the CE
- Contracting with subcontractors
  - BA liability flows to all subcontractors

"I heard the new HIPAA Omnibus Rules are a whole lot tougher on business associates."

Important Definitions

- **Covered Entity (CE)**: Health care providers, health plans, health care clearinghouses who electronically transmit any Protected Health Information (PHI)
- **Business Associate (BA)**: Any individual or organization that creates, receives, maintains or transmits PHI on behalf of a Covered Entity (CE)
- **Subcontractor**: Create, receive, maintain or transmit PHI on behalf of a BA

HIPAA Overlap



Some Covered Entities are also Business Associates.

Business Associate Agreements

Agreement between the CE and BA to govern the BA's creation, use, maintenance and disclosure of PHI.

- Must comply with HIPAA Security
- Must help a CE satisfy Privacy Rules
- BAAs have **ALWAYS** been required by HIPAA
- After Omnibus – Require **reciprocal monitoring** by the BA & CE
- Subcontractors of BAs are treated as BAs as well

Required before a CE contracts with a third party individual or vendor (subcontractor) to perform activities or functions which will involve the use or disclosure of PHI

Business Associate Liability

Business associates are directly liable for:

1. Impermissible uses and disclosures
2. Failure to provide breach notification to the CE
3. Failure to provide access to a copy of ePHI to either the CE the individual, or the individual's designee
4. Failure to disclose PHI where required by the HHS to investigate or determine the BA's HIPAA compliance
5. Failure to follow Minimum Necessary standard when using or disclosing
6. Failure to provide an accounting of disclosures

Security AND Privacy Rule

- **Who**: **Insurance** company, Triple-S (Puerto Rico)
- **What/Why**: Widespread non-compliance
  - Failure to implement **Administrative**, **Privacy**, and **Technical** safeguards
  - Lack of appropriate **Business Associate Agreements**
  - Failure to conduct **accurate/thorough Risk Analysis**
- **Settlement**: **$3.5 Million & CAP** (11/30/15)

*"This case sends an important message for HIPAA Covered Entities not only about compliance with the requirements of the **Security Rule**, including risk analysis, but compliance with the requirements of the **Privacy Rule**, including those addressing **business associate agreements** and the minimum necessary use of protected health information."* **- Jocelyn Samuels, Director of OCR**

http://www.hhs.gov/about/news/2015/11/30/triple-s-management-corporation-settles-hhs-charges.html

Business Associates Must Comply

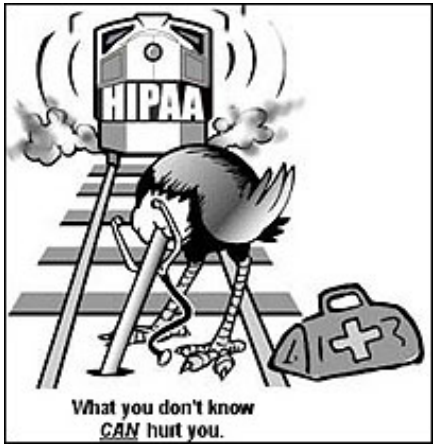
- **Who**: **Business Associate** (Catholic Health Care Services of the Archdiocese of Philadelphia)
- **What**: **iPhone theft**, 412 patient records
- **Why**: Did not complete **thorough risk analysis**, failed to implement appropriate security measures. Did not have **policies in place**.
- **Settlement**: **$650,000 and CAP** (3/19/16)

*"**Business associates must implement** the protections of the **HIPAA Security Rule** for the electronic protected health information they create, receive, maintain or transmit from covered entities. This includes an enterprise-wide risk analysis and corresponding risk management plan, which are cornerstones of the HIPAA Security Rule."*
- Jocelyn Samuels, Director of OCR

http://healthitsecurity.com/news/business-associate-agrees-to-650k-ocr-hipaa-settlement

When is a BAA Not Needed?

- **Treatment**
  - PHI being disclosed to a healthcare provider for treatment purposes (e.g., primary/referring physician, contract physicians or specialists, contract nursing staff, contract rehab staff, ambulance, home health, dentist).
- **Payment**
  - PHI being disclosed to a health plan for payment purposes, or to a health plan sponsor with respect to disclosures by a group health plan.
- **Operations**
  - PHI being disclosed for the purpose of health care operations. (Administrative and managerial activities, such as business planning, resolving complaints, and complying with HIPAA.)



BA Definition Made Easy

(**Person/Organization**) who…
On behalf of such (**Covered Entity/Business Associate**)…
Creates, receives, maintains, or transmits protected health information …

The Question To Ask Yourself

What is (**company X**) doing with my PHI….
that otherwise I would need to do myself?

Is an offsite transcription service a Business Associate?

No

Incorrect

Yes

Correct

Is a contracted office cleaning company a Business Associate?

No

Correct

Yes

Incorrect

Correct

What is (company X) doing with my PHI…. that otherwise I would need to do myself?

Is a document storage company a Business Associate?

No

Incorrect

Yes

Correct

What is (company X) doing with my PHI…. that otherwise I would need to do myself?

Correct

Is a Security Guard service a Business Associate?

No

Correct

Yes

Incorrect

Correct

What is (company X) doing with my PHI…. that otherwise I would need to do myself?

Is Your Billing Firm a Business Associate?

No

Incorrect

Yes

Correct

What is (company X) doing with my PHI…. that otherwise I would need to do myself?

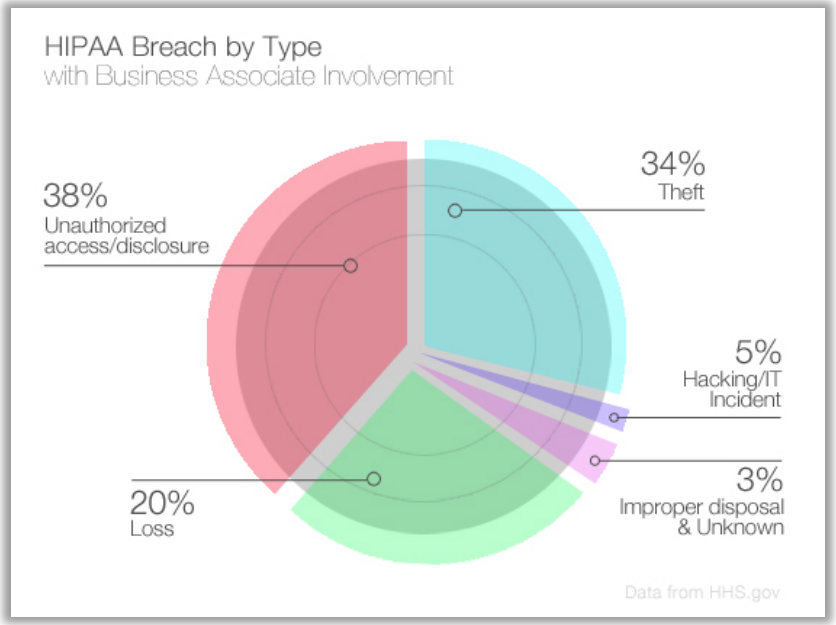
Correct

Examples of Business Associates

- IT Support and Software Vendors
- IT Equipment Vendors
- Leasing firms
- Telephone CPE Vendors
  - Depends on Conduit
- Shredding Vendors
- Data Centers
- Cloud Computing Providers
- EHR/EMR Providers
- Answering Services for Medical Offices
- Medical Billing Services
- Medical Transcriptions Services
- Medical Collection Agencies
- Temporary Employment Agencies
- Healthcare Equipment Companies
- Document Storage Companies
- Accounting Firm
- Law Firm
- Consulting Firm
- Software Vendor

Why You Should Worry About Business Associates

- **> 59%** of BAs reported a data breach in the last two years that involved the loss or theft of patient data.
- **> 29%** experienced two breaches or more.



Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data conducted by Ponemon Institute
http://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf

HHS Breach Portal AKA "Wall of Shame"

Breach Report Results

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
BioReference Laboratories, Inc	NJ	Healthcare Provider	3563	04/08/2016	Unauthorized Access/Disclosure	Other
Virtua Medical Group	NJ	Healthcare Provider	1654	03/11/2016	Unauthorized Access/Disclosure	Network Server, Other
G&S Medical Associates, LLC	NJ	Healthcare Provider	3000	01/14/2016	Hacking/IT Incident	Desktop Computer
Horizon Healthcare Services, Inc., doing business as Horizon Blue Cross Blue Shield of New Jersey, and its affiliates	NJ	Health Plan	1173	09/24/2015	Unauthorized Access/Disclosure	Other
Jersey City Medical Center	NJ	Healthcare Provider	1447	04/17/2015	Unauthorized Access/Disclosure	Email
MD Manage (Vcarve LLC)	NJ	Business Associate	35357	10/22/2014	Unauthorized Access/Disclosure	Network Server
Vcarve LLC d/b/a MD Manage	NJ	Business Associate	585	10/06/2014	Unauthorized Access/Disclosure	Network Server
Jersey City Medical Center - Barnabas Health	NJ	Healthcare Provider	36400	08/07/2014	Loss	Other
Sutherland Healthcare Solutions, Inc.	NJ	Business Associate	342197	05/22/2014	Theft	Email, Laptop
Options Counseling Center	NJ	Healthcare Provider	2828	05/09/2014	Theft, Unauthorized Access/Disclosure	Paper/Films
Inspira Health Network Inc.	NJ	Healthcare Provider	1411	02/21/2014	Theft	Desktop Computer
Horizon Healthcare Services, Inc., doing business as Horizon Blue Cross Blue Shield of New Jersey, and its affiliates	NJ	Business Associate	839711	01/03/2014	Theft	Laptop

20% **Involved Business Associates**

Based on HHS Breach Portal: Breaches Affecting 500 or More Individuals, "Type of Breach" https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

The NEED for BAAs

- **Who**: Raleigh Orthopedic (North Carolina)
- **What**: **Breach report**, 17,300 patient records
- **Why**: Handed over x-rays and associated PHI to potential business partner without first executing a **business associate agreement**.
- **Settlement**: **$750,000 and CAP** (4/20/16)

*"HIPAA's obligation on covered entities to obtain **business associate agreements** is more than a mere check-the-box paperwork exercise. It is **critical for entities to know to whom they are handing PHI** and to obtain assurances that the information will be protected."* **- Jocelyn Samuels, Director of OCR**

http://www.hhs.gov/about/news/2016/03/16/155-million-settlement-underscores-importance-executing-hipaa-business-associate-agreements.html

Importance of BAA & Complete Risk Analysis

- **Who**: North Memorial Health Care of Minnesota
- **What**: **Laptop theft**, 6,497 patient records
- **Why**: No **BAA** with Billing firm, **failed to complete a risk analysis** to address all potential risks and vulnerabilities to ePHI
- **Settlement**: **$1,550,000 and CAP** (3/19/16)

*"Two major cornerstones of the HIPAA Rules were overlooked by this entity. Organizations must have in place compliant **Business Associate Agreements** as well as an **accurate and thorough risk analysis** that addresses their enterprise-wide IT infrastructure.* **- Jocelyn Samuels, Director of OCR**

http://www.hhs.gov/about/news/2016/03/16/155-million-settlement-underscores-importance-executing-hipaa-business-associate-agreements.html

The HIPAA Compliance Puzzle

Compliance Questions?

For more information, contact:

855 85 HIPAA
(855-854-4722)
www.CompliancyGroup.com
info@compliancygroup.com

Marc Haskelson
855.854.4722 ext 507
marc@compliancygroup.com