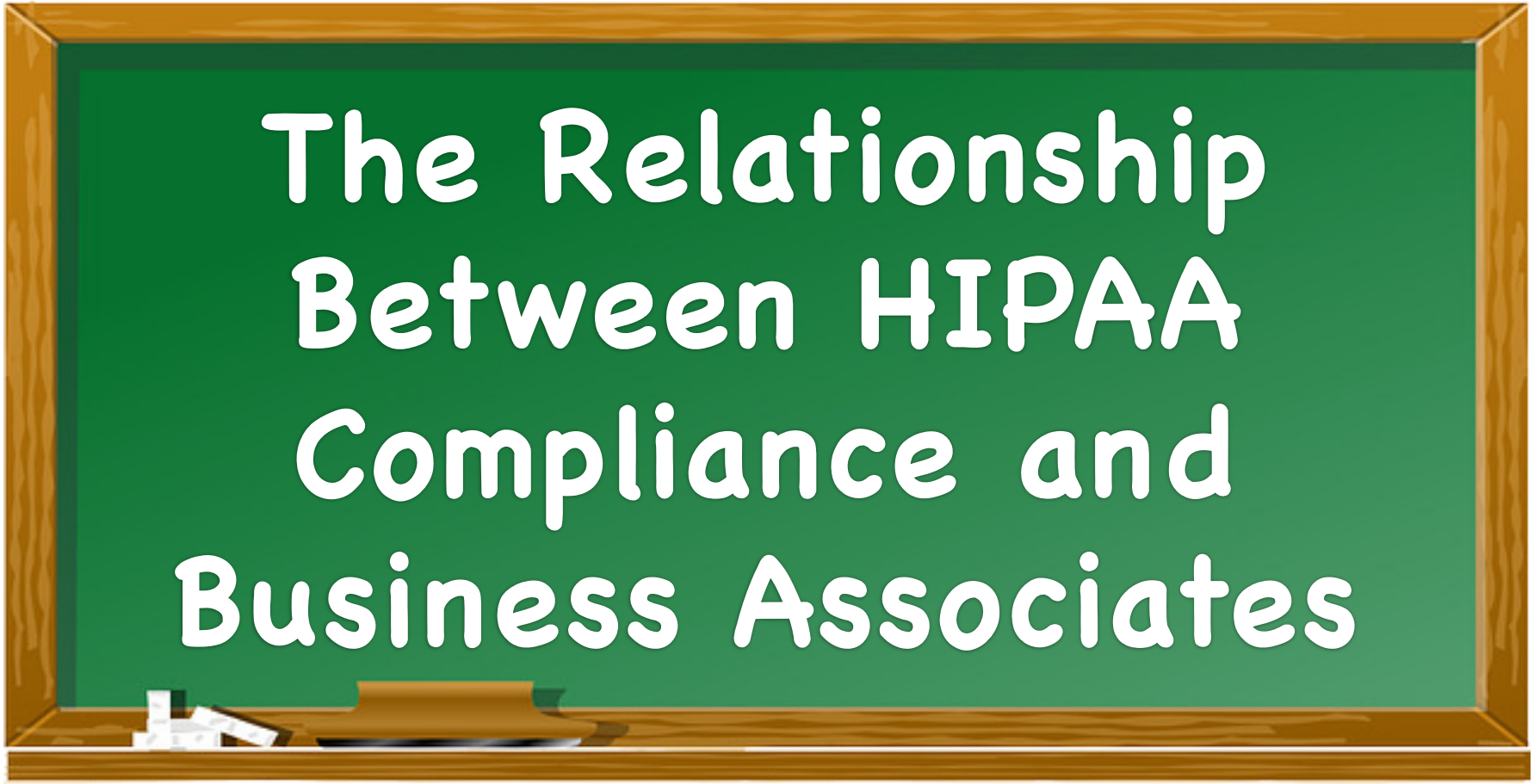

The Relationship Between HIPAA Compliance and Business Associates

HHS Wall of Shame

	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
0	Carson Valley Medical Center	NV	Healthcare Provider	11388	04/04/2017	Unauthorized Access/Disclosure	Email
0	Ashland Women's Health	KY	Healthcare Provider	19727	04/04/2017	Hacking/IT Incident	Network Server
0	Memorial Healthcare	MI	Healthcare Provider	685	04/03/2017	Unauthorized Access/Disclosure	Other
0	Apex EDI, Inc.	UT	Business Associate	1132	03/31/2017	Hacking/IT Incident	Network Server
0	Skin Cancer Specialists, P.C.	GA	Healthcare Provider	3366	03/31/2017	Hacking/IT Incident	Network Server
0	Women's Care of Somerset	KY	Healthcare Provider	1806	03/31/2017	Unauthorized Access/Disclosure	Email
0	ABCD Pediatrics, P.A.	TX	Healthcare Provider	55447	03/26/2017	Hacking/IT Incident	Network Server
0	Lane Community College Health Clinic	OR	Healthcare Provider	1911	03/25/2017	Hacking/IT Incident	Laptop
0	Washington University School of Medicine	MO	Healthcare Provider	80270	03/25/2017	Hacking/IT Incident	Email
0	WellSpan Health	PA	Health Plan	732	03/23/2017	Unauthorized Access/Disclosure	Paper/Films
0	Specialty Dental Partners of Philadelphia, PLLC - DBA Rich Orthodontics	PA	Healthcare Provider	960	03/23/2017	Theft	Desktop Computer, Laptop
0	Hospice of North Central Ohio	OH	Healthcare Provider	1051	03/23/2017	Unauthorized Access/Disclosure	Other
0	Urology Austin, PLLC	TX	Healthcare Provider	279663	03/22/2017	Hacking/IT Incident	Network Server
0	UNC Health Care	NC	Healthcare Provider	1298	03/20/2017	Unauthorized Access/Disclosure	Paper/Films
0	Highland Rivers Community Service Board	GA	Healthcare Provider	967	03/20/2017	Unauthorized Access/Disclosure	Paper/Films
0	Rocky Mountain Health Maintenance Organization, Inc.	CO	Health Plan	1320	03/17/2017	Unauthorized Access/Disclosure	Paper/Films

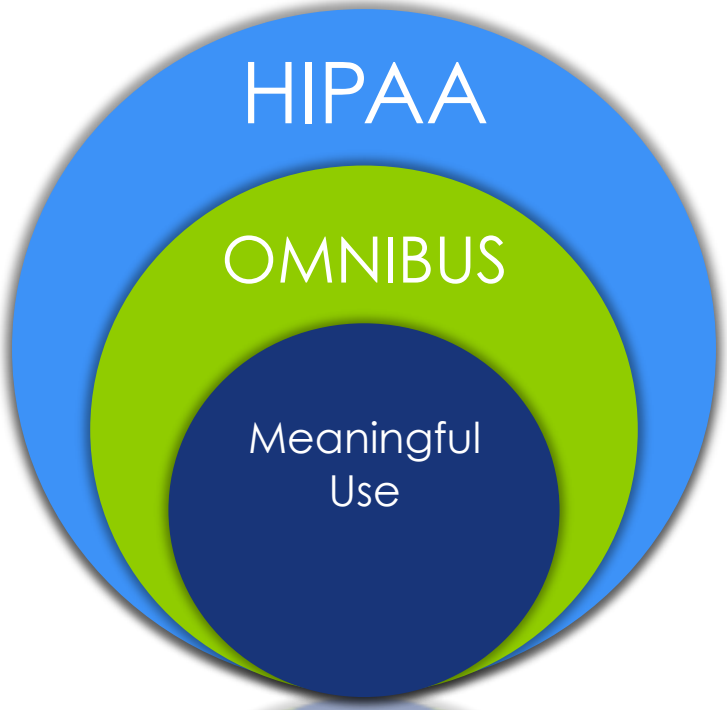
20%

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

What is HIPAA Compliance and what is NOT

- **Compliance vs. Security**
  - Fines vs. Risk
- **HIPAA/HITECH**
  - Protect patient confidentiality while furthering innovation and patient care
  - Privacy Rule and Security Rule
- **Omnibus**
  - Business Associates must be HIPAA compliant
  - Covered Entities must have BAAs
    - Conduct Due Diligence
  - Breach Notification Rule
- **Meaningful Use**
  - Accelerate adoption of EHR (electronic Health records)



What Information Does HIPAA Protect?

PHI may include any of the following:

- Names
- Addresses
- Dates of Service
- Telephone Numbers
- Fax Numbers
- Email Addresses
- Social Security Numbers
- Medical Record Numbers
- Health Plan Beneficiary Numbers

- Account Numbers
- Certificate/License Numbers
- Vehicle identifiers/Serial Numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers;
- Biometric identifiers
- Full Face Photos or Videos
- Any other unique identifying number, characteristic, or code

Compliance vs. Security

- Audits
  - Security, Privacy, and Administrative
- Gap Identification
- Remediation
- Policies & Procedures
- Employee Training & Attestation
- Business Associate Management
  - BA Agreements & Audit
- Incident Management

- Security Risk Analysis
- Penetration Testing
- Remediation
  - Vulnerability Scan
- Prevention
  - System Hardening
- Detection
  - Behavioral monitoring
  - Network Security Monitoring

Security Risk Assessment

FINES → **REPUTATION** ← RISK

Omnibus Rule

- Business Associates:
  - Direct liability by function
  - Directly liable for violations
  - Must be HIPAA Compliant (Security Rule)
    - **Technical**, **Administrative, & Physical** Safeguards
- Covered Entities:
  - Compliance with Privacy Rule
  - Must have BAAs (Business Associate Agreements)
  - Conduct **Due Diligence**
  - 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."

The HIPAA Compliance Puzzle

Importance of BAA & Complete Risk Analysis

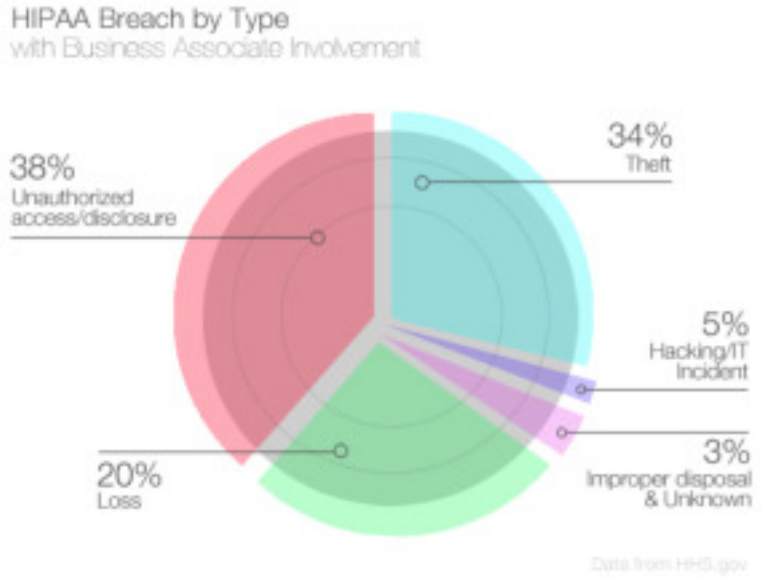
- Who: North Memorial Health Care of Minnesota
- What: **Laptop theft**, 6,497 patient records
- Why: No **BAA** with Billing firm, **failed to complete a risk analysis** to address all potential risks and vulnerabilities to ePHI
- Settlement: **$1,550,000 and CAP** (3/19/16)

*"Two major cornerstones of the HIPAA Rules were overlooked by this entity," said **Jocelyn Samuels, Director of OCR**. "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.*

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

Why You Should Worry About Business Associates

- In a recent study, **more than half** of business associates (**59%**) reported a data breach in the last two years that involved the loss or theft of patient data. More than a quarter (**29%**) experienced two breaches or more.
- Of the 345 incidents reported by HHS and listed on their site under Breaches Affecting 500 or More Individuals, 74 involved a business associate (**21%**).



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

The Need For BAAs

- Who: Raleigh Orthopaedic (North Carolina)
- What/Why: 17,300 patients affected
  - Handed over PHI to potential business partner without first executing a **business associate agreement**.
- Settlement: **$750,000 & 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," said **Jocelyn Samuels, Director of OCR**. "It is critical for entities to know to whom they are handing PHI and to obtain assurances that the information will be protected."

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/raleigh-orthopaedic-clinic-bulletin/index.html

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.

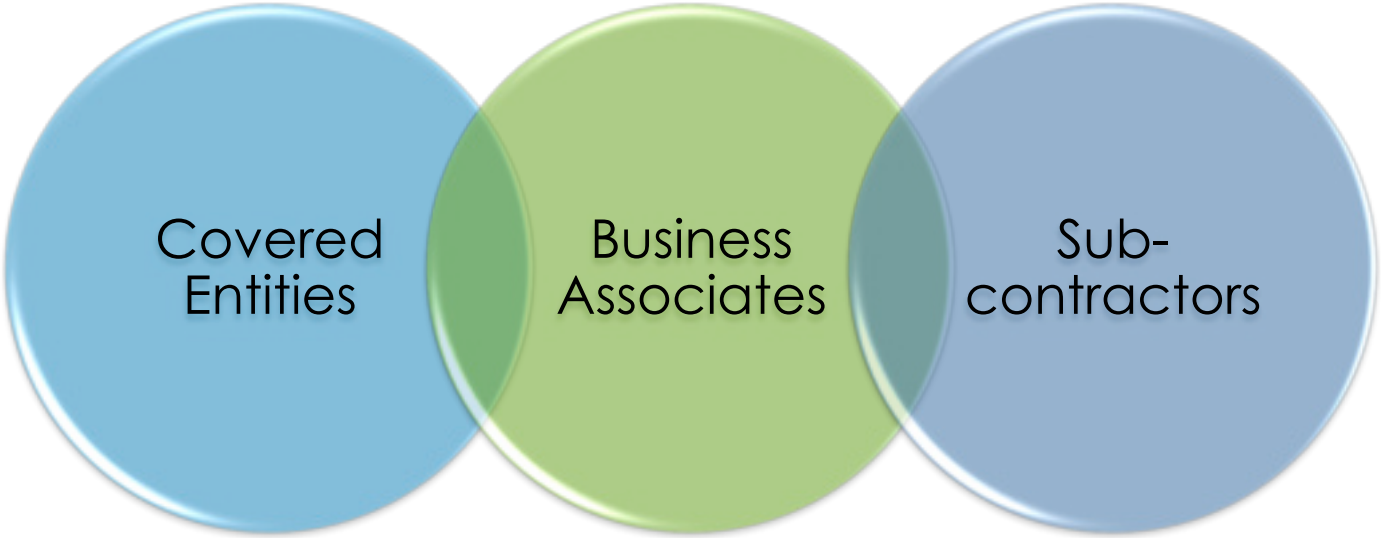
Important Definitions

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

First Business Associate Penalty

- Who: Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS), **IT services for nursing facilities**
- What: **iPhone theft** (412 PHI)
- Why: Device was **unencrypted** and **not password protected**;
  - **Lack of policies & procedures** for removal of PHI devices
  - Lack of policies & procedures to address **incidents**
  - **No risk analysis or risk management plan**
- Settlement: **$650,000 & CAP** (6/29/16)

*"**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," said Office for Civil Rights (OCR) Director Jocelyn Samuels. "This includes an **enterprise-wide risk analysis** and corresponding risk management plan, which are the cornerstones of the HIPAA Security Rule."*

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

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

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

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 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?

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

Data Transmission Services

Data Transmission Services

- Business associates include health information organizations and e-prescribing gateways.
- To qualify as a business associate, the data transmission service must have "routine" access to the PHI it is transmitting.
- The "conduit exception" – if an entity is simply acting as a pass-through with no routine access, not a business associate.
  - Examples include telephone company, UPS and courier services.

The HIPAA Compliance Puzzle

Compliancy Group

We simplify compliance so you can confidently focus on your business.

The Guard

- Total HIPAA compliance Solution
- Simple
- Cost-Effective
- **Achieve, Illustrate and Maintain™** methodology
  - No Audits failed, ever!
- Compliance Support
  - Compliance Coaches
  - HIPAA Hotline, Email, chat or call
  - Breach Support
  - Audit Support
- Seal of Compliance
  - Verification and Validation of your HIPAA compliance

Questions? Need Help with Compliance?

Marc Haskelson
President & CEO
855-854-4722 Ext 507
Marc@compliancygroup.com

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