Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

The Basics of Business Associates

Rebecca L. Williams, RN, JD
Co-Chair, Health Information Practice
beckywilliams@dwt.com
(206) 757-8171

Who Is a Business Associate?

- Three-prong definition plus exceptions
- First Prong
  - Creates, receives, maintains, or transmits protected health information (PHI)
  - On behalf of a covered entity
- New definition of business associate

Who Is a Business Associate?

- Second Prong
  - Provides certain identified services
  - Involving PHI
  - Examples: legal, actuarial, accounting, consulting
  - Slight tweak from Omnibus Rule

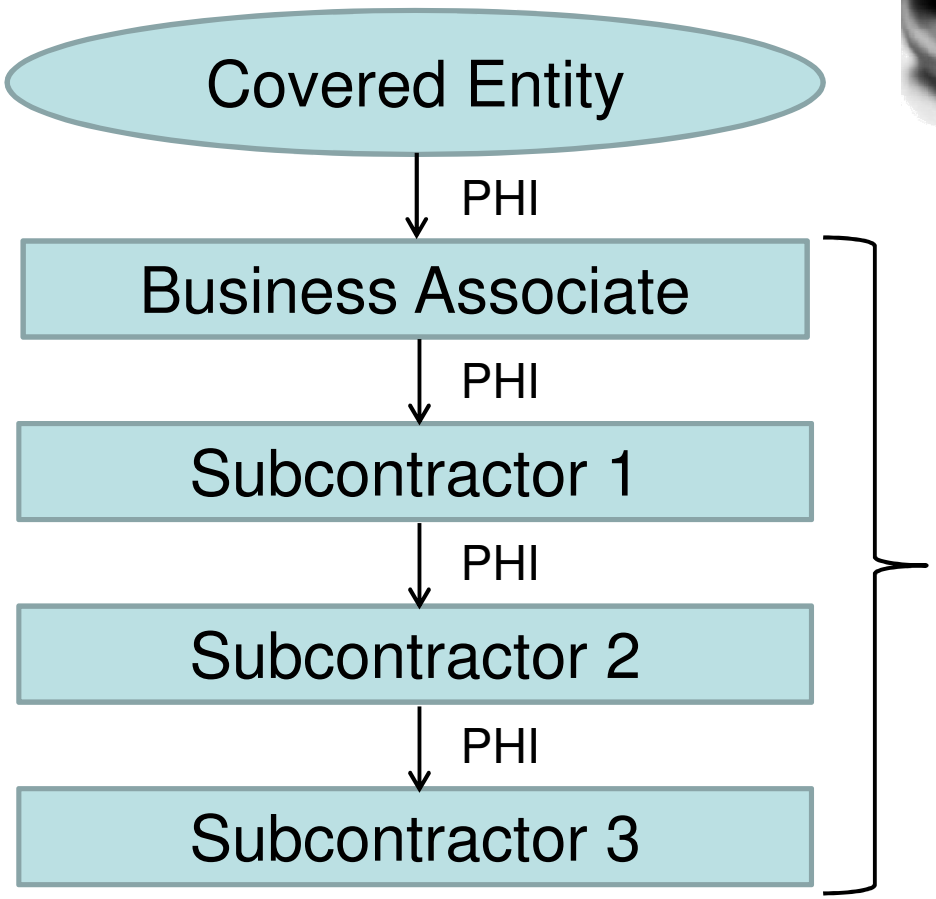
Who Is a Business Associate?

- Third Prong
- “Business associate" specifically includes
  - Health Information Organization
  - e-Prescribing Gateway
  - Other provider of data transmission services that requires access to PHI
  - Offerer of PHR on behalf of covered entities
  - Subcontractor

Welcome to the HIPAA Party, Subcontractors!

- Subcontractor + PHI = Business Associate
- Subcontractor = person to whom a business associate delegates a function, activity, or service and who is not workforce

All the Way Down the Chain



All Business Associates

Who Isn't a Business Associate?

- Health care providers (for treatment)
- Plan sponsors (for plan sponsor activities after plan amendments and certifications)
- Financial institutions (such as for cashing checks or conducting funds transfer)
- Onsite contractors (when treated as workforce)
- "Conduits" that transport/transmit PHI but do not access PHI other than on a random or infrequent basis to support transport or as required by law

What to Do About Business Associates?

- Must obtain "satisfactory assurances"
  - Covered Entity → Business Associate
  - Business Associate → Subcontractor Business Associate
- Generally as a business associate contract
- Must meet minimum content requirements of
  - Privacy Rule – applies to all PHI
  - Security Rule – applies to the ePHI
- May contain additional requirements
- Sample on HHS website – Use with caution

Business Associate Contract — Required Privacy Language

- Establish permitted/required uses & disclosures of PHI
- Not use or further disclose PHI other than in accordance with the contract or as required by law
- Use appropriate safeguards
- Report any impermissible use or disclosure, including breach
- Ensure any Subcontractors (who access PHI) agree to the same requirements that apply to Business Associate
- Facilitate access, amendment, and accounting of disclosures
- Comply with the Privacy Rule if carrying out a Covered Entity's HIPAA obligations
- Make internal records available to Secretary to determine Covered Entity's HIPAA compliance
- On termination, return/destroy PHI, if feasible, or extend protections

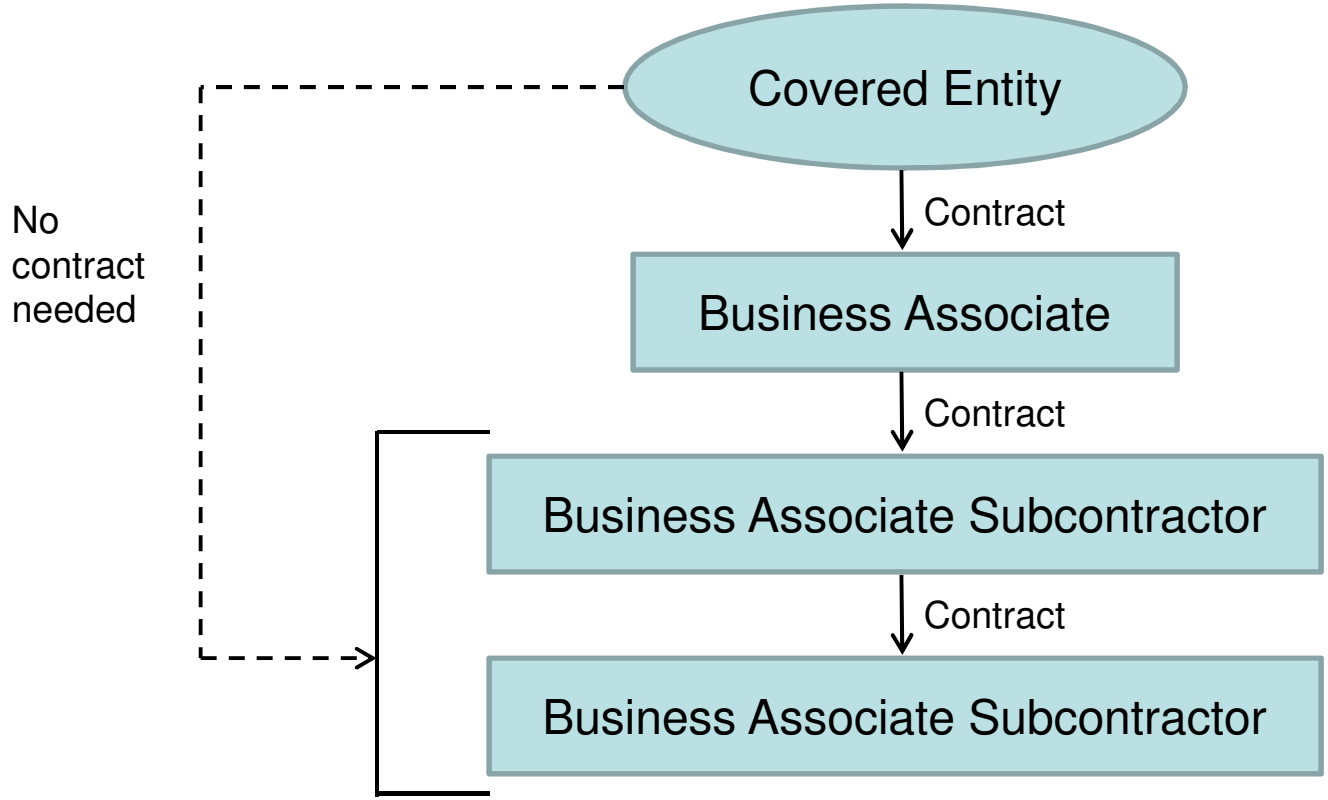
Business Associate Contract – Required Security Language

- Comply with the applicable provisions of the Security Rule
- Ensure Subcontractors agree to comply with the applicable provisions of the Security Rule
- Report any security incident, including a breach

Business Associate Contract – Other Language

- BAAs are contracts subject to negotiation
- Other provisions permissible
  - Subcontracting with permission/notice/due diligence; off-shore prohibition
  - Timing, especially for agents
  - Indemnification
  - Limitations on damages
  - Insurance
  - Audit / Ongoing monitoring
  - Third party beneficiaries
  - Interpretation

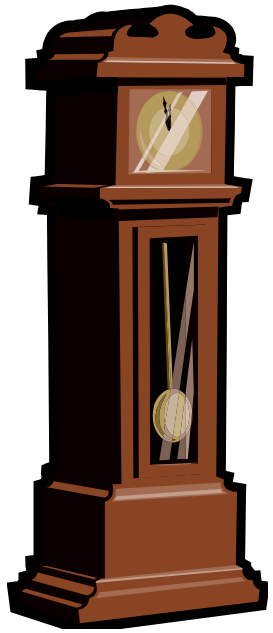
Business Associate Contracting: Who Contracts with Whom?



*** Each contract in the chain must be at least as restrictive as the contract above it.**

Grandfathering Provision

- Existing contract (as of 1/25/13) that meets HIPAA Privacy and Security Rule requirements
- Not renewed or modified between effective date (3/26/13) and compliance date (9/23/13)
- May have up to an additional year to comply (until 9/22/14)
- Still must comply with HIPAA requirements



What Does This Mean for Business Associate?

- Directly required by HIPAA (penalties for noncompliance) including:
  - Breach Notification Rule
  - Security Rule
  - Appropriate uses & disclosures of PHI
- Required by business associate contract (only breach of contract for noncompliance) including:
  - Reporting impermissible uses & disclosures; security incidents
  - Return or destroy PHI at termination
- Not required (unless delegated by Covered Entity)
- Potential best practice

Business Associate Obligations

- HIPAA liability attaches to business associates even in the absence of a business associate contract

Who Is Liable?

- Business Associates and Covered Entities are liable for acts of agents within scope of agency
  - Workforce
  - Agents who are business associates, regardless of whether BA contract is in place
- Who is an agent?
  - Subject to the Federal common law on agency
  - Authority to control the business associate's conduct in the course of its performance? Authority to provide interim instructions or directions?

Action Items for Covered Entities

- Business associate contracts
  - Identify and re-verify business associates and agents
  - Revise business associate contract templates
  - Determine plan for amending/renegotiating existing BAAs

Action Items for Business Associates

- Breach Notification Rule compliance
  - Implement breach/security incident response system
  - Policies/procedures and training
- Security Rule compliance
  - Don't forget risk analysis!
  - Policies/procedures and training

- Privacy Rule: Consider policies/procedures/training
  - Specific Privacy Rule requirements
  - Consider most stringent BAA

Questions

For more information…

Rebecca L. Williams, JD, RN

Davis Wright Tremaine LLP

beckywilliams@dwt.com
206.757.8171