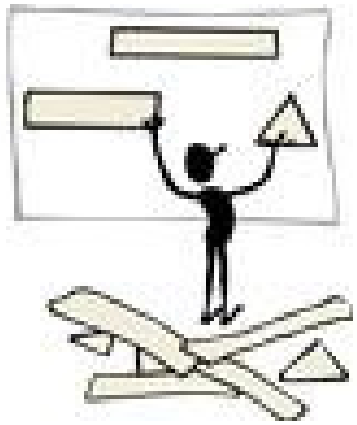
Business Associates:

HITECH Changes You Need to Know

Rebecca L. Williams, RN, JD
Partner, Co-chair of HIT/HIPAA Practice
Davis Wright Tremaine LLP
beckywilliams@dwt.com

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

Big Changes



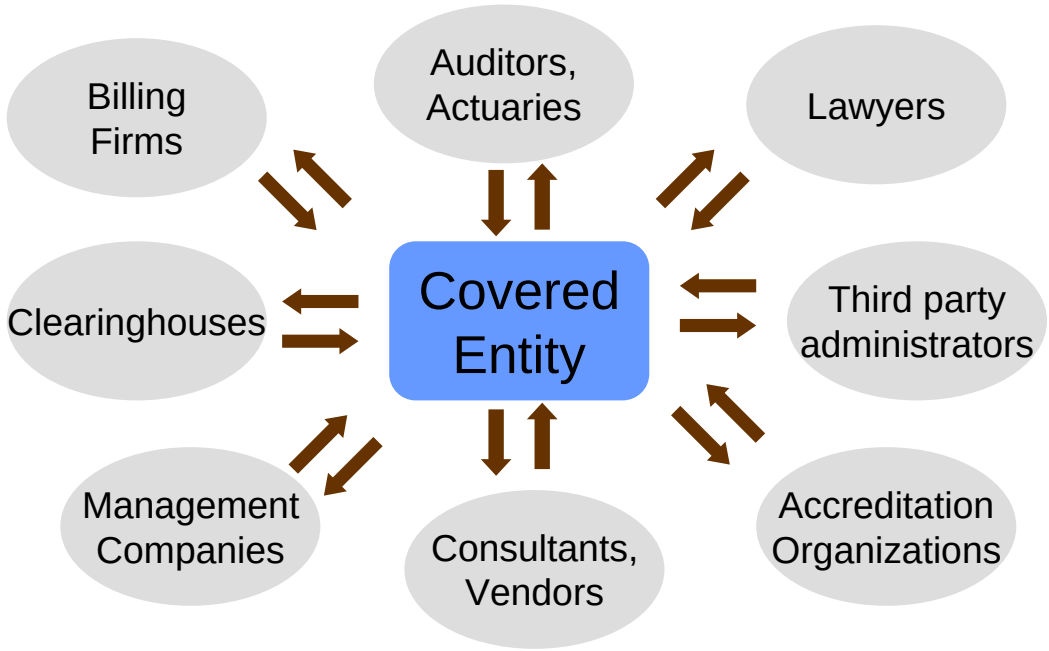
- Requirements from
  - HIPAA
  - Health Information Technology for Economic & Clinical Health Act (HITECH)
  - Interim final breach notification regulations
  - Proposed Rule modifying HIPAA under HITECH (published July 14, 2010)
- Resulting in
  - More responsibilities
  - Direct liability
  - Likely expansion of those included as Business Associates
  - New contract considerations

General Approach

- Covered Entity may permit a Business Associate to create, receive, maintain, or transmit protected health information (PHI)
- Only with "satisfactory assurances" ─ Business Associate Contracts ─ from Business Associate to appropriately protect PHI
- Business Associate Contracts must comply with HIPAA requirements
  - Different requirements under privacy and security rule
  - May have additional language
- Under original HIPAA:
  - Business Associates were not directly regulated by HIPAA
  - Business Associate Contract = way to backdoor some of the HIPAA requirements

Who Is a Business Associate?

- A person who, on behalf of Covered Entity or OHCA,
  - Performs, or assists with, a function or activity or
  - Performs certain identified services
- Involving protected health information
- A person is a Business Associate if it meets the definition, even if no contract is in place



Davis Wright Tremaine LLP

Specific Inclusions as Business Associates

- Patient Safety Organizations (Proposed Rule)
- Health Information Organizations
- e-Prescribing Gateways
- Other persons that facilitate data transmissions
- PHR vendors that provide PHRs to Covered Entities
- Subcontractors of Business Associates
  - Proposed Rule
  - A dramatic change

Davis Wright Tremaine LLP

Subcontractors as Business Associates

- Definition: Person who acts on behalf of a Business Associate, other than as workforce
- Current Law: Downstream contractual obligation
- Proposed Rule: New category of Business Associate
  - Subcontractor + PHI = Business Associate
  - Viewed as closing a gap
- Business Associate would need to enter into a Business Associate Contract with its Subcontractors
- Result: Two types of "Business Associates" with different rules:
  - Direct Business Associates (contract with Covered Entities)
  - Subcontractor Business Associates (contract with other Business Associates)

Direct Liability for Business Associates

- Direct liability under HIPAA and HITECH for Business Associates
  - Civil liability
  - Criminal liability
  - Contractual liability
- Direct HIPAA liability attaches regardless of whether there is a formal contract

HITECH's Breach Notification

- Business Associate must notify its Covered Entity — and Covered Entities must make their notifications — upon "discovery" of a "breach" of "unsecured" PHI
- "Breach"
  - Unauthorized acquisition, access, use, disclosure of PHI
  - In a manner not permitted by the HIPAA Privacy Rule
  - That compromises the security or privacy of such PHI
    - Poses a significant risk of financial, reputational, or other harm to the individual
    - Fact-specific analysis (consider nature of information, recipient, mitigation)
    - De-identified information does not pose risk of harm
  - Exceptions
    - Unauthorized person would not reasonably have been able to retain the PHI
    - Certain good faith or inadvertent access by or disclosure to workforce in same organization

Breach Notification

- Timing
  - Notification without unreasonable delay but not later than 60 days after “discovery”
  - Clock starts ticking on first day it is known – or using reasonable diligence would have been known – to any workforce member or agent (per federal common law of agency) (other than person committing the breach)
  - Subject to law enforcement delay
  - Covered entities may want additional notice requirements, particularly for “agents”
- Content of Business Associate’s notification:
  - Identification of individuals affected
  - Other information that Covered Entity must provide
  - To extent possible

Breach Notification

- Business Associates
  - Need policies/procedures/plan to respond
  - Response must be without unreasonable delay
  - Want immediate internal reporting
- Covered Entities
  - Need policies/procedures/plan to respond
  - Business Associate Contracts require Business Associates to report security incidents and impermissible disclosures
  - Proposed Rule includes breaches of unsecured PHI
  - May want to add timing, particularly for “agents”
  - May want coordination of notification -- No duplicative notice
- Subcontractors
  - Need to notify the Business Associate
  - Some inconsistency between HITECH and Proposed Rule

Compliance with Security Rule

- Business Associates must directly comply with certain provisions of the HIPAA Security Rule:
  - Administrative standards
  - Physical standards
  - Technical standards and
  - Policy, procedures, and documentation requirements
- As if they were covered entities
- Proposed Rule also would apply general security obligations to Business Associates
- BA to engage in security compliance process
  - Expands safeguard requirements in BACs
  - Begins with risk analysis and risk management
  - Document

Davis Wright Tremaine LLP

Privacy: Permitted Uses and Disclosures

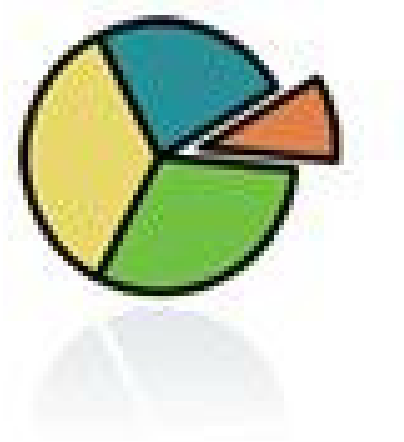
- HITECH: Business Associates may use and disclose PHI only if such use or disclosure is in compliance with each applicable requirement of the privacy provisions of their Business Associate Contracts
- Proposed Rule: Business Associates, like Covered Entities, may not use or disclose PHI except as permitted or required by the Privacy Rule and Enforcement Rule

Privacy: Required Uses and Disclosures

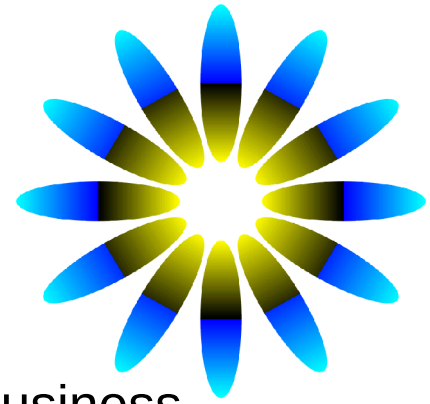
- To HHS for investigation of Business Associate's compliance
- To Covered Entity, individual, or individual's designee to respond to request for electronic copy of individual's PHI

Minimum Necessary

- Proposed application to Business Associates
  - Business Associates may use, disclose, or request
  - Only the minimum PHI
  - Necessary to accomplish the intended purpose
- Solicited public comment on guidance



Expanded Accounting of Disclosures



- Existing Law: No TPO in accounting
- HITECH: If Covered Entity uses an EHR
  - Right to accounting of TPO through EHR
  - For previous 3 years
- Covered Entity may either:
  - Provide accounting of Covered Entity's and Business Associate's disclosures or
  - Provide accounting of Covered Entity's disclosures and a list of its Business Associates
- Listed Business Associate to provide accounting of its disclosures, if requested
- May want to address accounting in Business Associate Contract
- Compliance Date:
  - January 1, 2011 (or date of EHR implementation)
  - Reprieve for existing EHRs: January 1, 2014

No Sale of PHI

- HITECH: Prohibits a Covered Entity or Business Associate from directly or indirectly receiving remuneration in exchange for any PHI
- Unless individual authorization –
  - HITECH requires specification of whether PHI is subject to sale for re-disclosure
  - Not so required under Proposed Rule

No Sale of PHI

- Exceptions:
  - Public health activities
  - Limited data sets (proposed)
  - Research (with limits)
  - Treatment of the individual
  - Payment (proposed)
  - Sale, transfer, merger, or consolidation
  - *Payment to Business Associate for its services (modified by Proposed Rule)*
  - Provision to an individual with a copy of his/her record
  - Disclosures required by law (proposed)
  - Disclosures permitted by Privacy Rule (proposed)
  - As determined by HHS

Business Associate Contract – Required Privacy Language

- Establish permitted uses and 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 to report breaches (proposed)
- Ensure any Subcontractors (that access PHI) agree to the same requirements that apply to Business Associate
  - In the form of Business Associate Contract (proposed)
- Facilitate PHI access

Business Associate Contract – Required Privacy Language

- Facilitate PHI amendment
- Provide information for accountings of disclosure
- If Business Associate is carrying out a Covered Entity obligation under the Privacy Rule, Business Associate must comply with the Privacy Rule
- Make internal practices, books, and records available to Secretary to determine Covered Entity's HIPAA compliance
- On termination of contract, return/destroy PHI, if feasible, or extend protections

Business Associate Contract – Required Security Language

- Comply with applicable Security Rule requirements
- Ensure Subcontractors agree to safeguard ePHI
  - Including to comply with applicable requirements of Security Rule (proposed)
  - Entering into Business Associate Contract (proposed)
- Report any security incident
  - Including breaches of unsecured PHI (proposed)

Liability for Others

- Existing Rule: Covered Entity is liable if it knows of a pattern or practice by Business Associate that is a material breach of Business Associate Contract unless Covered Entity:
  - Takes steps to cure breach and, if unsuccessful
  - Terminates arrangement, if feasible, or
  - Reports to HHS

- HITECH: Business Associate is liable if it knows of a pattern or practice of Covered Entity that is a material breach of Business Associate Contract (unless cure, terminate, or report)

Liability for Others

- Proposed Rule:
  - Makes Covered Entity liable for acts of Business Associates that are agents
  - Makes Business Associate liable if it knows of a pattern or practice by its Subcontractor that is a material breach of Business Associate Contract unless Business Associate takes steps to cure breach or terminate contract
  - Removes reporting to HHS as an alternative

Transition Provisions for Business Associate Contracts

- Proposed transition provision to grandfather existing Business Associate Contracts and existing Subcontractor agreements that
  - Comply with the then-current HIPAA requirements
  - Have not been amended or modified

HITECH Enforcement Approaches

- Business Associates are subject to civil and criminal enforcement under HIPAA
- Clarifies/expands liability for criminal violations
- Increased civil penalties
- Harmed individuals may receive percentage of Civil Money Penalties
- State Attorneys General may bring civil actions
- Continuation of OCR corrective action plans
- Audits mandated