Business Associates:

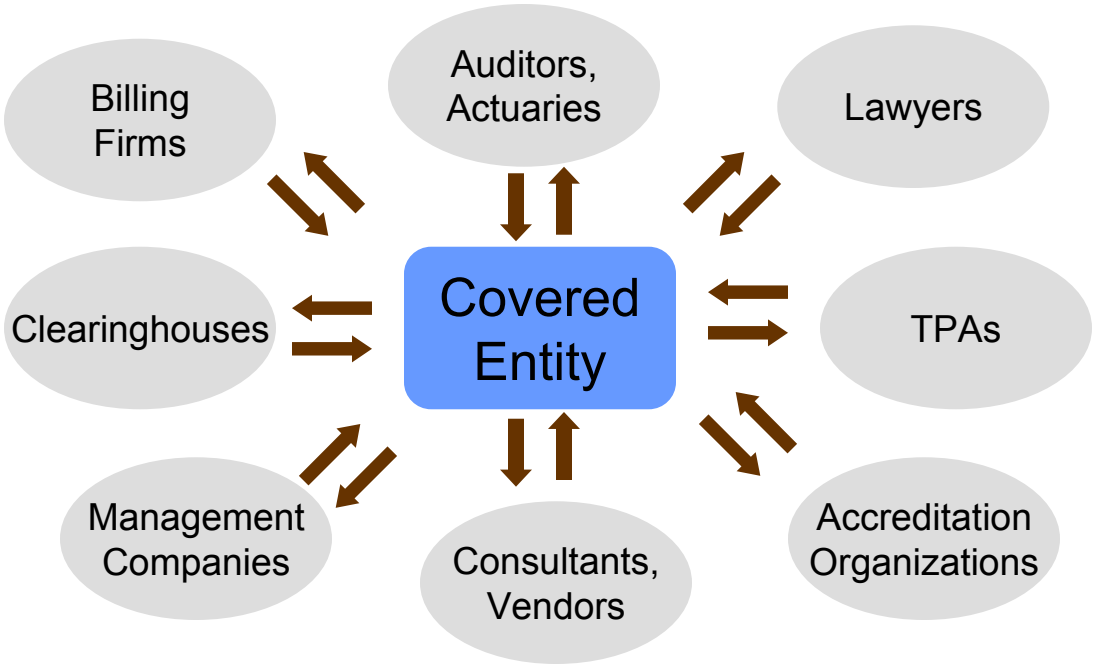
HITECH Changes You Need to Know

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

Who Is a Business Associate?

- A person who, on behalf of a covered entity or OHCA
  - Performs or assists with a function or activity involving individually identifiable health information
  - Performs certain identified services involving individually identifiable health information



Davis Wright Tremaine LLP

Clarification of Status for Certain Business Associates

- HITECH: Clarification of business associate status
  - HIEs
  - RHIOs
  - e-Prescribing Gateways
  - PHR vendors that provide PHRs to covered entities
- No change to definition

Business Associates

- Previous Law: Business associates have not been directly regulated by HIPAA
  - Instead, covered entities are required to enter into business associate contracts with their business associates
  - HIPAA mandates certain contract content
  - Different requirements under privacy and security rule
  - Way to backdoor some of the HIPAA requirements

HITECH's Breach Notification

- Business associate must notify its covered entity — and covered entities must make certain 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)
  - May want additional notice requirements for "agents"
  - Subject to law enforcement delay
- Content of notification by BA, to extent possible:
  - Identification of individuals affected
  - Other available information that CE must provide

Breach Notification

- BAs need policies/procedures/plan to respond
  - Response must be without unreasonable delay
  - Want immediate internal reporting
  - Timing for agents?
  - What about subcontractors?
- CEs need to decide whether to:
  - Require/acknowledge/expand notification in BAC
  - Timing requirements, particularly for “agents”
  - Coordination of notification -- No duplicative notice
- Not intended to interfere with current BA-CE relationship

Davis Wright Tremaine LLP

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
- BA to engage in security compliance process
  - Expands safeguard requirements in BACs
  - Begins with risk analysis and risk management
  - Document
- CEs may want to have BA acknowledge its security obligations

Privacy Requirements

- Business associates may use & disclose PHI
  - Only if such use or disclosure
  - Is in compliance with
  - Each applicable requirement of the
  - Privacy provisions of their BACs
- Business associates should revisit existing privacy processes under BACs

Privacy “Snitch” Rule

- Business associate is not in compliance with privacy provisions of its business associate contract
- If BA knows of a pattern of activity or practice of CE
- That constitutes a material breach of CE’s material obligation under the BAC
- Unless the business associate:
  - Takes steps to cure breach and, if unsuccessful
  - Terminates arrangement, if feasible, or
  - Reports to HHS
- Covered entities have similar requirements
- Some uncertainty how far this goes

Davis Wright Tremaine LLP

Other Privacy and Security Requirements

- Other HITECH privacy and security requirements that apply to CEs "shall be incorporated into the business associate agreement"
- Differing interpretations
  - Application of law?
  - Requirement to amend business associate contracts?
- Waiting for HHS guidance

What Does this Mean for Contracts?

- Current options:
  - Amend existing contracts
  - Written notification/reminder/assurance of compliance
  - Do nothing
- Prepare for future:
  - Amend templates
  - Good opportunity to revisit approach
- Be ready to respond
  - To differing approaches
  - To government guidance

Expanded Accounting of Disclosures

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

Davis Wright Tremaine LLP

Marketing

- Existing Law: Exceptions to “marketing” (treatment, care coordination, part of plan of benefits, etc.)
- HITECH: Exceptions do not apply if CE receives direct or indirect payment for communication unless the communication is:
  - Regarding a drug currently prescribed for the recipient and payment is “reasonable in amount”
  - Made by the CE pursuant to a valid authorization
  - Made by a BA, on behalf of the CE, and such communication is consistent with the applicable BAC
- Particular impact on BAs involved with marketing

No Sale of PHI

- HITECH: Prohibits a CE or BA from directly or indirectly receiving remuneration in exchange for any PHI
- Unless individual authorization – must specify whether PHI is subject to sale for re-disclosure
- Exceptions:
  - Public health activities
  - Research (with limits)
  - Treatment of the individual
  - Sale, transfer, merger, or consolidation
  - *Payment to business associate for its BA services*
  - Provision to an individual with a copy of his/her record
  - As determined by HHS

Other HITECH Requirements

- Minimum necessary
- Access to PHI if CE maintains an EHR
  - HITECH right to electronic copy of records
  - HITECH right to direct CE to transmit electronic copy to another entity or person
- Right to request additional privacy protections
  - CEs must comply with a request not to disclose to health plans for self-pay services
- May have business associate implications

New 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