Business Associates:

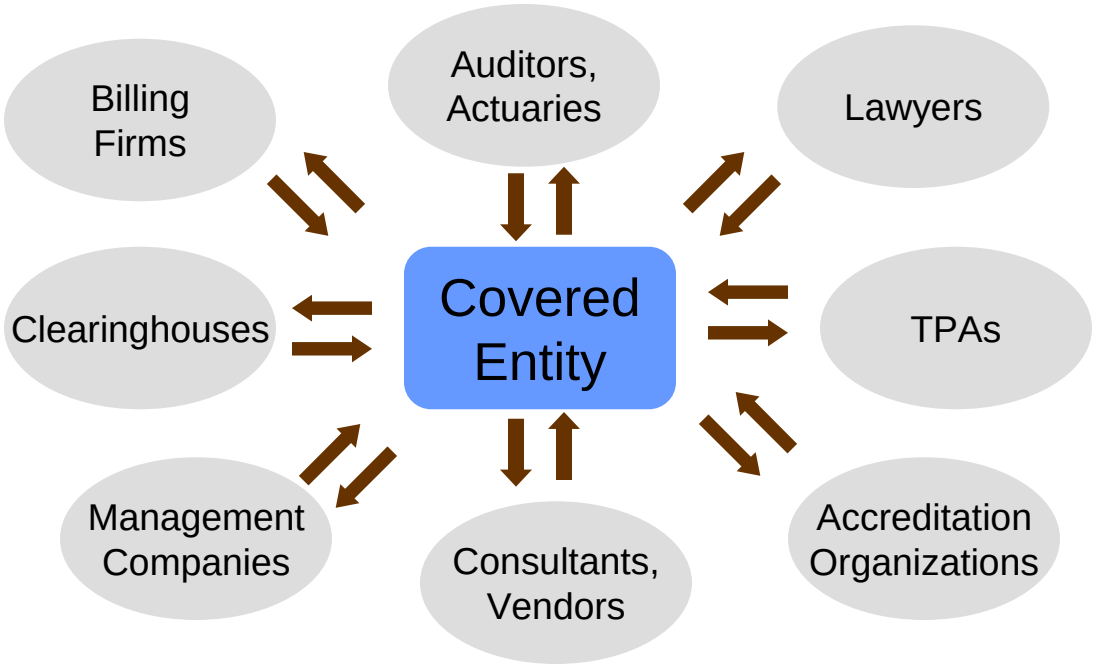
HITECH Changes You Need to Know

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 information, or otherwise covered by HIPAA
  - Performs certain identified services involving PHI



Business Associates

- Existing Law: Business associates have not been directly regulated by HIPAA
  - Instead Covered Entities were required to enter into business associate contracts with their business associates
  - Way to backdoor some of the HIPAA requirements

Clarification of Status for Certain Business Associates

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

Davis Wright Tremaine LLP

Data Breach Notification

- Business associate must notify its covered entity
- Upon discovery
- Of a breach unsecured PHI
- Notification without unreasonable delay but not later than 60 days
- Notification, to the extent possible, to include:
  - Identification of individuals affected
  - Other available information that CE must provide
- BAs need policies/procedures/plan to respond
- CEs need to decide what requirements to put in place for their BAs

Direct Compliance with Security Rule

- Business associates are required to directly comply with certain provisions under the HIPAA security rule:
  - Administrative standards
  - Physical standards
  - Technical standards and
  - Policy, procedures, and documentation requirements
- As if they were covered entities
- Need to engage in security compliance process beginning with risk analysis and risk management

Privacy Requirements

- 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
- Business associates should revisit existing processes relating to privacy requirements under business associate contracts

Privacy Requirements: “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:
  - Take steps to cure breach and, if unsuccessful
  - Terminate arrangement or
  - Report to HHS
- How far does this extend?

Davis Wright Tremaine LLP

Other Privacy and Security Requirements

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

What Does this Mean for Business Associate Contracts?

- Current options:
  - Amend existing contracts
  - Written notification/reminder/assurance of compliance with HITECH obligations
  - Do nothing
- Prepare for future:
  - Amend templates
  - Good opportunity to revisit approach
- Be ready to respond

Davis Wright Tremaine LLP

Expanded Accounting of Disclosures

- Existing Law: No TPO in accounting
- HITECH: If CE uses/maintains an EHR -
  - Right to accounting of TPO through EHR
  - For previous 3 years (as opposed to 6 years)
- Affected by rulemaking (coming soon)
- Compliance Date:
  - January 1, 2011
  - Reprieve for existing EHRs (as of 1/1/09): January 1, 2014
- Business Associates will need to know whether expanded accounting applies

Access to PHI

- Existing Law: Individual has a right to access/receive a copy of medical record
- HITECH: If CE uses/maintains an EHR-
  - Right to electronic copy of records
  - Right to direct CE to transmit electronic copy to another entity or person
- May affect business associate's obligations

Individually Requested Privacy Restrictions

- Existing Law: Individual has right to request privacy restrictions but binding on CE only if CE agrees
- HITECH: No disclosure to health plans for self-pay services if so requested by individual
- May have business associate implications

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 business associate contract

Minimum Necessary

- Use, disclose, request Limited Data Sets to the extent practicable
- If not practicable, minimum necessary
- HHS guidance

Davis Wright Tremaine LLP

No Sale of PHI

- Existing Law: No prohibition on being paid for PHI as long as the disclosure is otherwise permitted
- HITECH: Prohibits a covered entity or business associate from directly or indirectly receiving remuneration in exchange for any PHI without a valid authorization from the individual that includes a specification of whether the PHI is subject to sale for re-disclosure

No Sale of PHI

- Exceptions:
  - Public health activities
  - Research – with price reflecting costs for preparation and transmittal
  - Treatment of the individual, subject to any regulation
  - 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 otherwise determined by HHS

New Enforcement Approaches

- Clarifies/expands liability for criminal violations
- Increased civil penalties
- Harmed individuals to receive percentage of CMP
- State Attorney Generals may bring civil actions
- Continuation of OCR corrective action plans
- Audits

New Penalties

- Tier A (if offender did not know, and by exercising reasonable diligence would not have known, that he or she violated the law): $100 for each violation, up to $25,000 for identical violations
- Tier B (if the violation was due to reasonable cause and not willful neglect): $1,000 for each violation, up to $100,000 for identical violations
- Tier C (if the violation was due to willful neglect but was corrected): $10,000 for each violation, up to $250,000 per year
- Tier D (if the violation was due to willful neglect and was not corrected): $50,000, up to $1,500,000 per year