Covered Entities and Business Associates:

An Evolving Relationship

Rebecca L. Williams, RN, JD
Partner, Chair of HEALTH/HIPAA Practice
Davis Wright Tremaine LLP
beckywilliams@dwt.com

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

No man is an Island, entire of itself ….

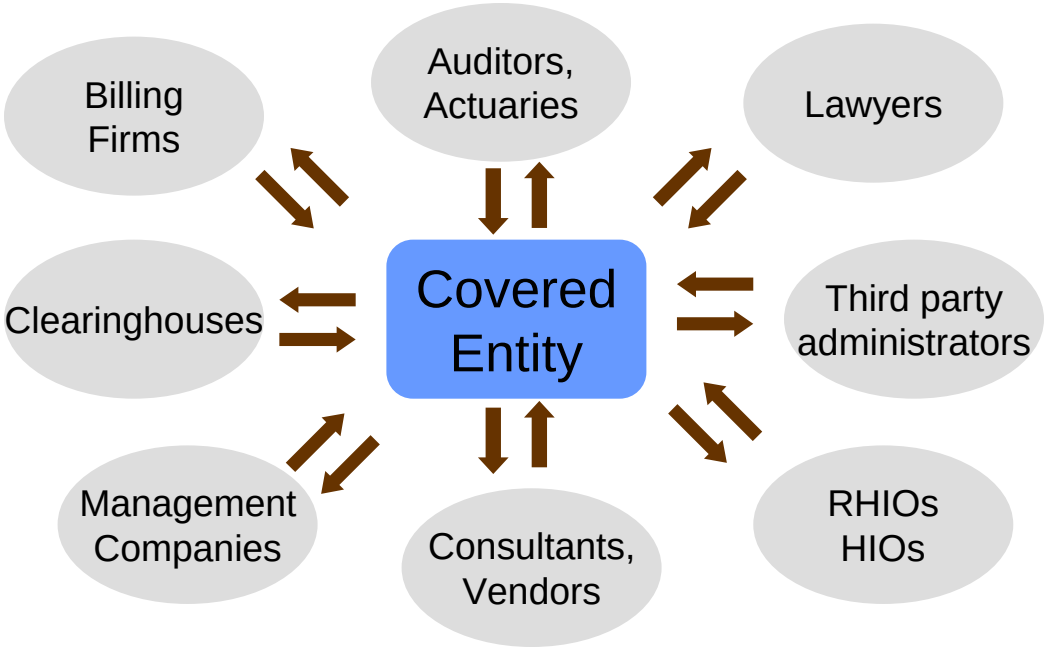
John Donne, English clergyman & poet (1572 - 1631)

No health care provider or health plan is an island either …

Davis Wright Tremaine LLP

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 PHI and IIHI
- Not: a workforce member; treating provider; plan sponsor with respect to its plan; government agency determining eligibility enrollment for public benefit plan; OHCA's covered entity
- A person is a Business Associate by meeting the definition, even if no contract is in place



A Walk Down Memory Lane . . . Before HITECH

- Only Covered Entities – not Business Associates – had direct HIPAA compliance obligations
- A Covered Entity could use a Business Associate but needed a Business Associate Contract
- Business Associate Contracts must contain HIPAA-mandated language
  - Different requirements under privacy rule and security rule
  - May have additional requirements
- Business Associate Contract = contractual obligation for some HIPAA requirements
- HITECH brought many changes

Enforcement

- Business Associates are subject to civil and criminal enforcement under HIPAA
- HHS has indicated it would NOT enforce HITECH requirements until final regulations became effective
- Not binding on Department of Justice or State Attorneys General
- In fact . . . .

1st Business Associate Enforcement Action

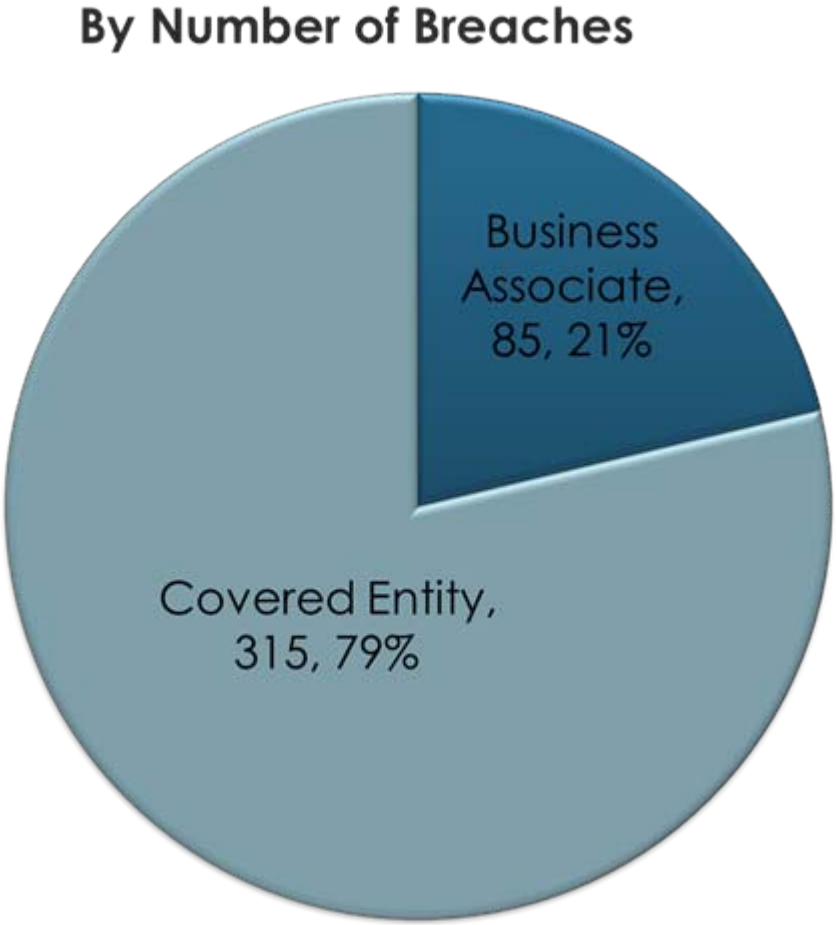
- Compliments of Minnesota AG
- Accretive Health
  - Business Associate engaged in multiple lines of business
  - Debt collecting
  - Data mining & consumer behavior modeling as part of operating hospital's revenue cycle
  - "Quality and total cost of care" initiative – payor incentives to cut patient costs
- Stolen: Laptop from backseat of rental car

Enforcement Against Business Associate

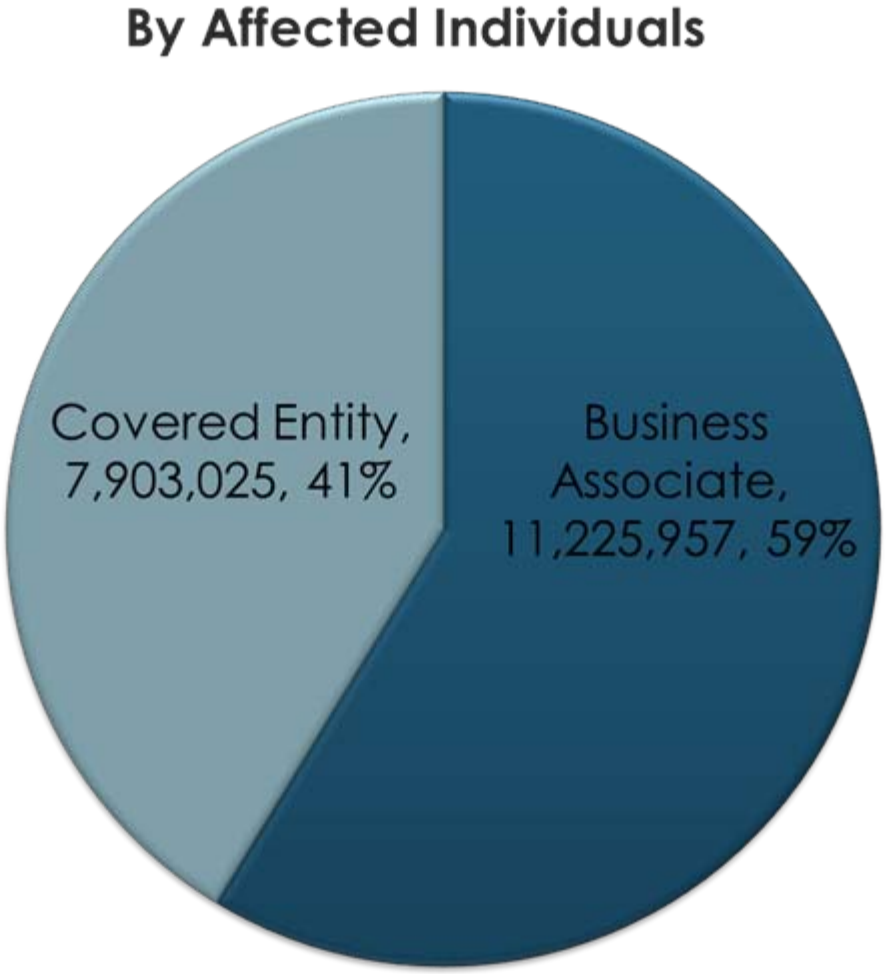
- ~ 25,000 patients affected/information included
  - Medical score (likelihood of admission/frailty)
  - Dollar amount “allowed” to provider
  - Itemization of 22 conditions (e.g., bipolar disease, high BP)
  - Demographic information including SSN
- Alleged HIPAA violations – (Policies, training)
- Alleged deceptive & fraudulent practices
  - Failure to affirmatively disclose to patients the amount of collected PHI
  - Masking its identity

Davis Wright Tremaine LLP

Large Breaches



Large Breaches



Davis Wright Tremaine LLP

HITECH's Breach Notification

- Upon the "discovery" of a
- "Breach" of
- "Unsecured" PHI
- Business associates must make required notifications to covered entities
- Covered entities must make their notification requirements

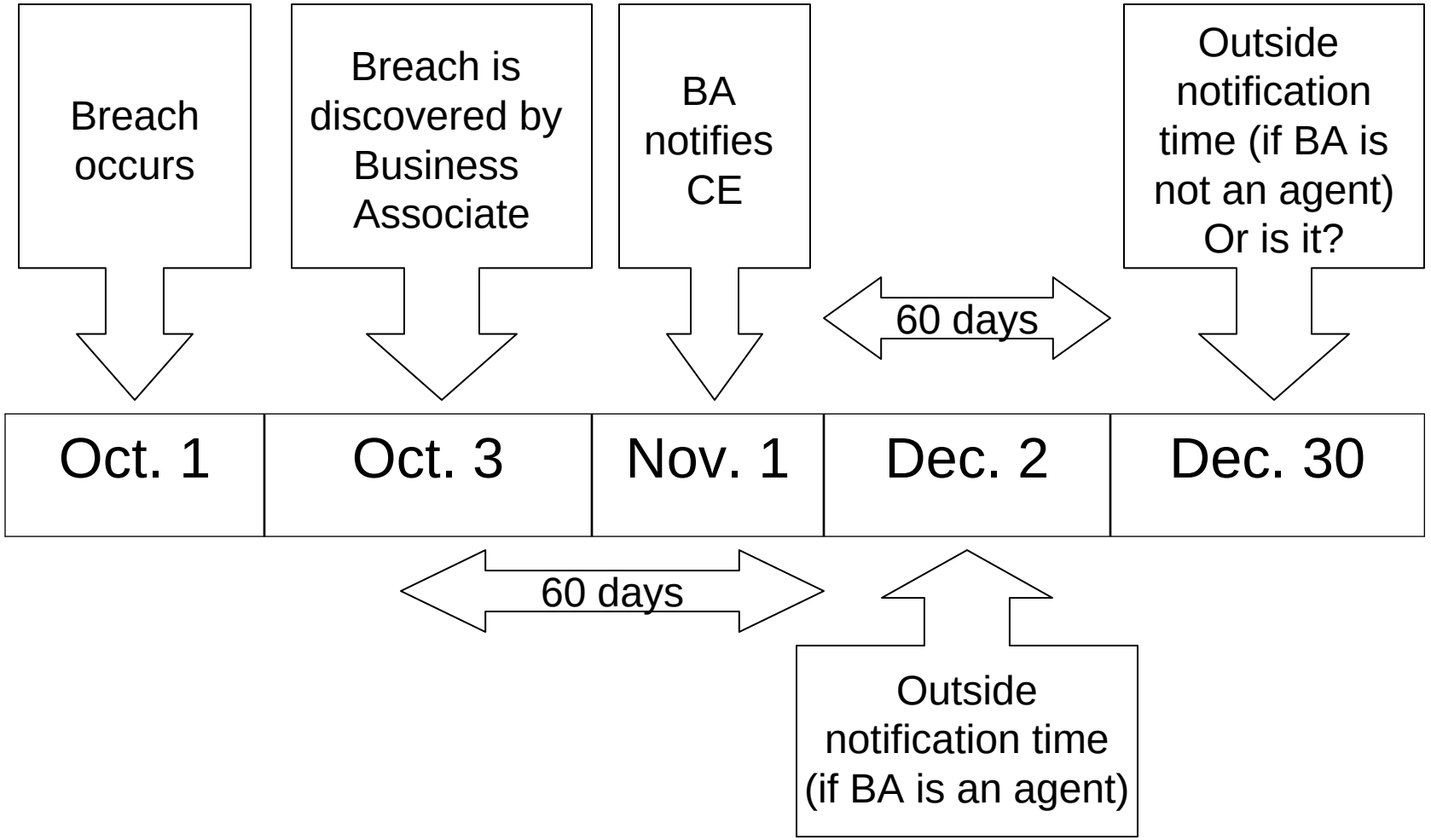
HITECH's Breach Notification

- "Breach"
  - Unauthorized acquisition, access, use, disclosure of PHI
  - In a manner not permitted by the Privacy Rule
  - That poses a significant risk of financial, reputational, or other harm to the individual
    - Fact-specific analysis
    - Consider nature of information, recipient, mitigation
- Should Covered Entities leave the determination up to the Business Associate?

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 should 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

Examples of Timing



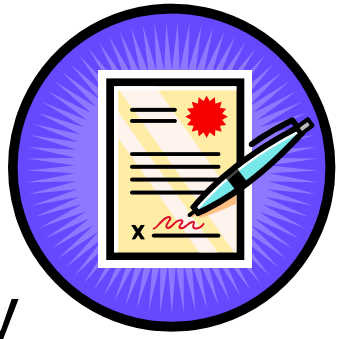
Davis Wright Tremaine LLP

HITECH Security

- Business Associates must directly comply with certain provisions of the HIPAA Security Rule:
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards and
  - Policy, procedures, and documentation requirements
- As if they were covered entities
- Proposed Rule: include general security obligations
- BA to engage in security compliance process
  - Begins with risk analysis and risk management
  - Document
- Covered entities may want tighter security requirements/audit rights

Davis Wright Tremaine LLP

HITECH Privacy



- Different HITECH approach for privacy
  - Business Associates may use and disclose PHI only if the use or disclosure is
  - In compliance with each applicable requirement of the privacy provisions of their Business Associate Contracts
- Other challenges, such as accountings of disclosures

HITECH: No Sale of PHI

- Prohibits direct or indirect remuneration to Covered Entity or Business Associate for PHI
- Exceptions:
  - Authorization (specified content)
  - Public health activities
  - Limited data sets (proposed)
  - Research (with limits)
  - Treatment
  - Payment (proposed)
  - Sale, transfer, merger, or consolidation
  - *Payment to Business Associate for its services (proposed)*
  - 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

HITECH: Specific Inclusions as Business Associates

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

Proposed Rule: 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: 2 tiers of "Business Associates"
  - Direct Business Associates (contract with Covered Entities)
  - Subcontractor Business Associates (contract with other Business Associates)

Around the Next Corner

- Final Omnibus Rule
- Likely result to Covered Entities & Business Associates:
  - Amend all existing Business Associate Contracts – even if contracts were amended with HITECH
  - Revise Business Associate Contract templates
  - Update HIPAA policies and procedures
- For Business Associates and (possibly) Subcontractors:
  - Risk analysis/risk management
  - Implement appropriate security measures
  - Policies and procedures: security, breach notification, privacy

For more information

Rebecca L. Williams, R.N., J.D.

Davis Wright Tremaine LLP
DEFINING SUCCESS TOGETHER

beckywilliams@dwt.com

206.757.8171

Davis Wright Tremaine LLP