Into the Breach: Breach Notification Requirements in the Wake of the HIPAA Omnibus Rule

The Twenty-Second National HIPAA Summit Healthcare Privacy and Security After HITECH and Health Reform

Rebecca Williams, RN, JD
Partner,
Co-Chair, Health Information Practice
Davis Wright Tremaine LLP
beckywilliams@dwt.com
(206) 757-8171

Breach Notification

- HITECH: First federal law mandating breach notification for health care industry
  - Applies to covered entities, business associates, PHR vendors, and PHR service providers
  - FTC regulates the PHR entities
  - HHS regulates covered entities and business associates
- Interim Final Breach Notification Rule (August 2009)
- Omnibus Rule (2013)

Breach Notification – Remember State Law

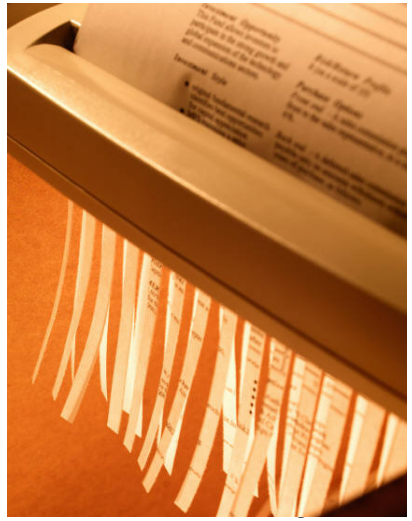
- 46 states (plus DC, Puerto Rico, and the Virgin Islands) have notification laws
- Evaluate state law as well as the Omnibus Rule requirements
  - Trigger
  - Timing
  - Content
  - Recipients

Data Breach Notification Overview

- Upon the **discovery** of a
- **Breach** of
- **Unsecured**
- **Protected health information** (PHI)
- Covered entities and business associates must make required **notifications**
- Subject to certain **exceptions**

Definition of Unsecured PHI

- Not rendered unusable, unreadable, or indecipherable to unauthorized persons
- Guidance Specifying the Technologies and Methodologies that Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals
- Encrypted or Shredded/Destroyed



Definition of Breach

- "Breach"
  - Unauthorized acquisition, access, use, disclosure
  - Of unsecured PHI
  - In a manner not permitted by the HIPAA Privacy Rule
  - That compromises the security or privacy of the PHI

Exceptions

- Unauthorized person not reasonably have been able to retain PHI
- Certain acquisition, access, or use by workforce in good faith and within scope of authority and no further impermissible uses and disclosures
- Certain inadvertent “disclosures” within the same covered entity, business associate, or organized health care arrangement and no further impermissible uses and disclosures
- ~~Limited data sets without ZIP or DOB~~

Hello Omnibus Rule Presumption

- An impermissible acquisition, access, use, or disclosure of PHI is
- **Presumed** to be a reportable breach
- UNLESS the entity demonstrates that there is a low probability that the PHI has been compromised

Risk Assessment

- **A documented risk assessment** to demonstrate a **low probability** of **compromise**
- Four mandatory factors
  - **What PHI:** Nature and extent of PHI involved
  - **Who:** The unauthorized person who used the PHI or to whom the disclosure was made
  - **Acquired:** Whether the PHI actually was acquired or viewed
  - **Mitigation:** The extent to which the risk to the PHI has been mitigated
- Other factors may be considered – Evaluation of overall probability

Risk Assessment

- Risk Assessment must be
  - Thorough
  - Completed in good faith
  - Have reasonable conclusions
  - Documented
- OCR views risk assessment as “more objective”
- Not mandatory: Discretion to provide notification without risk assessment
- Guidance promised/Guidance welcome

Goodbye Risk of Harm

- Interim final rule: "Compromise" meant poses a significant risk of financial, reputational, or other harm to the individual
- Controversial from the beginning
- Omnibus Rule: Risk of harm goes out the window
- Also the definition of compromises security or privacy of PHI

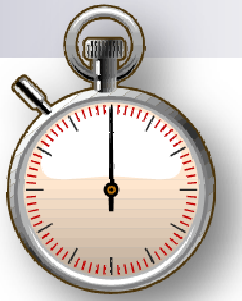
Timing of Notice

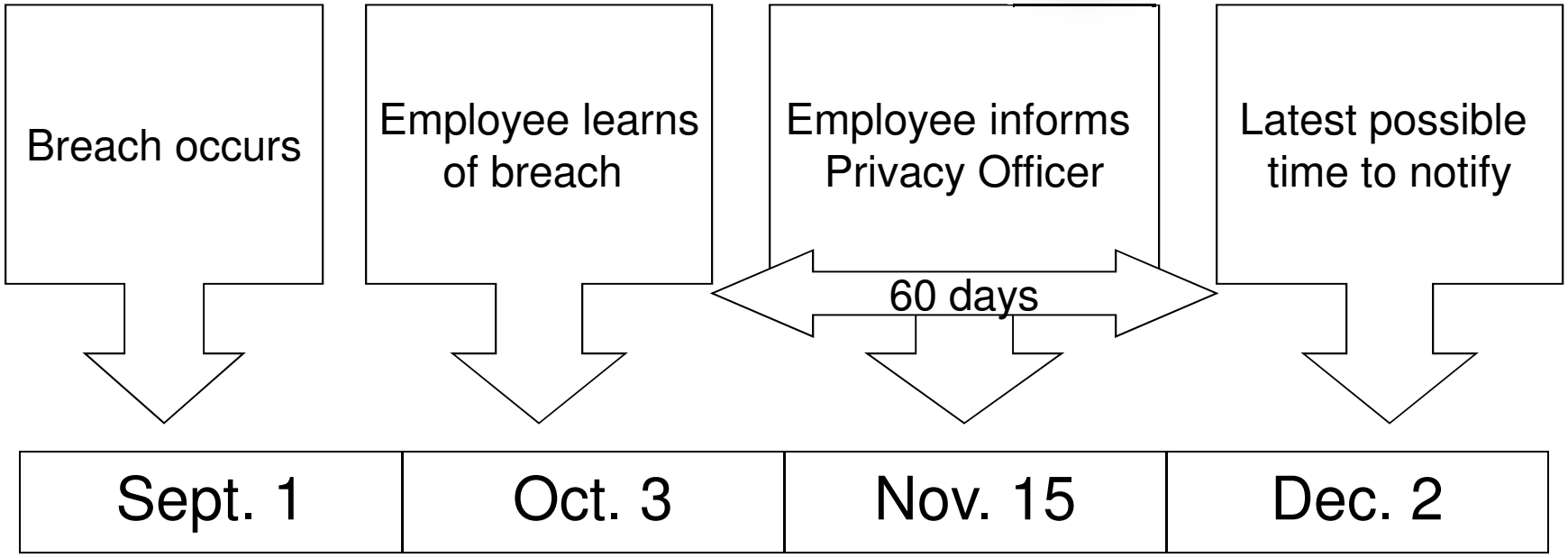
- Notification must be made "**without unreasonable delay**"
  - No more than 60 days after "discovery"
  - Subject to law enforcement delay

Discovery

- "Discovery" of a breach occurs when:
  - Entity has actual knowledge of a breach including through workforce member or agent (but not person committing the breach) or
  - Using reasonable diligence, entity would have known of the breach
- Agency is based on federal common law

Examples of Timing

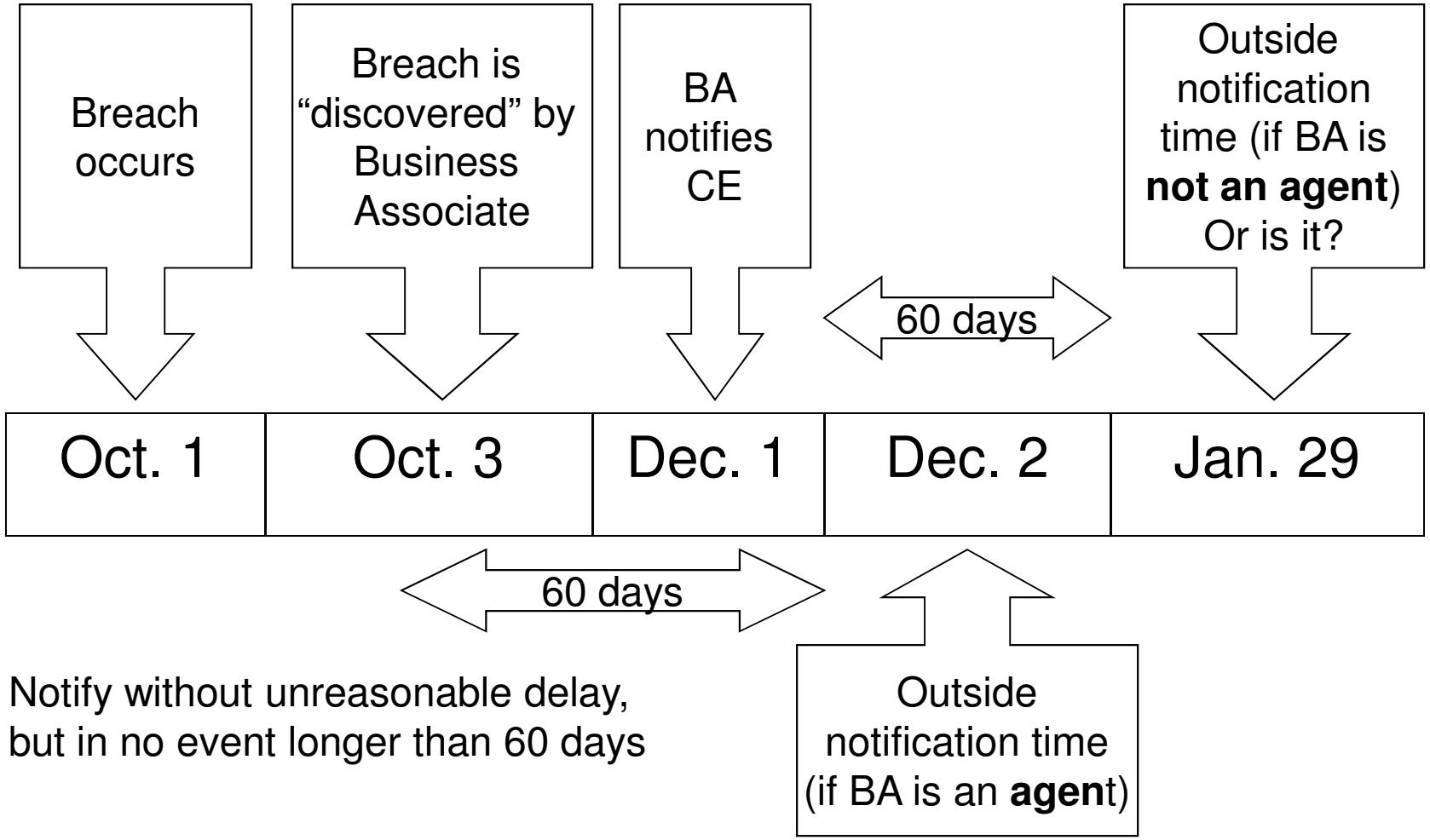




But remember without unreasonable delay

Caveat: Discovery. Clock starts when entity learns of – or using reasonable diligence should have learned of – the breach. Should the covered entity have learned of the breach earlier?

Timing with Business Associate



Caveat: When should the Business Associate/Covered Entity have learned of the breach?

Contents of Notice to Individuals

- Notices must contain:
  - Brief description of what occurred
  - Description of types of unsecured PHI involved (e.g., name, SSN, DOB, address) but not the actual PHI
  - Steps individuals should take to protect themselves
  - Brief description of what covered entity is doing to investigate the breach, mitigate damage, and protect against further breaches
  - Contact information for questions

Breach Notification

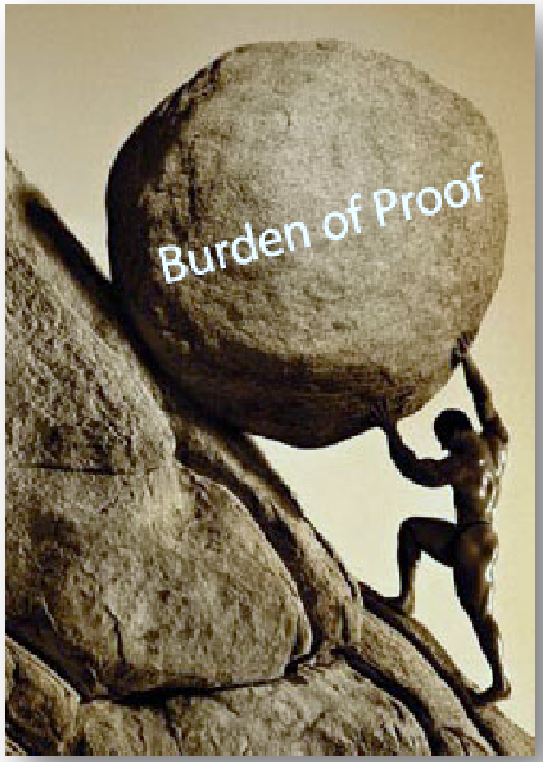
- Covered entity to notify affected individuals
  - Written notice
  - Substitute notice
- Covered entity to notify HHS
  - Timing depends on size of the breach
  - 500 or more = contemporaneous notification
  - Small breaches (<500) = annual notification
    - **Within 60 days of the end of the calendar year in which the breach was discovered (not occurred)**
    - **Considering less burdensome submission**
- Covered entity may have to notify media if more than 500 residents in a State affected
- Business associate to notify covered entity

Administrative Requirements

- Policies and procedures*
  - Recent settlement for failure to have policies even though notification was made
- Training*
- Complaints
- Sanctions
- Refraining from intimidating or retaliatory acts
- No waiver of rights

We Keep the Burden of Proof

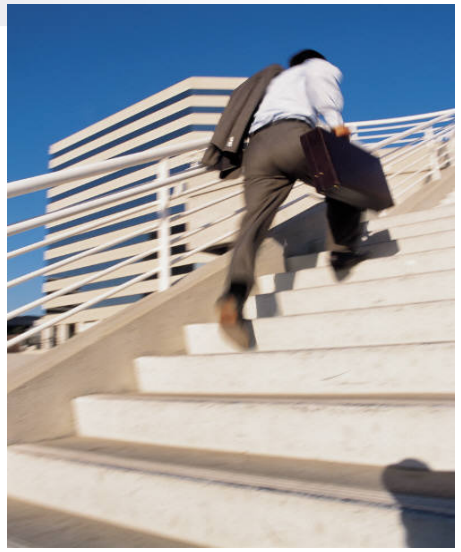
- Burden of proof is on the covered entity and business associate
- Documentation is crucial



How Does HHS Respond?

- Large breaches
  - Wall of Shame
  - Usually open a compliance review
- Even small breaches can lead to review and settlements
- Notification has resulted in settlements, e.g.
  - Massachusetts Eye & Ear
  - Blue Cross Blue Shield of Tennessee
  - Alaska Medicaid
  - Hospice of Northern Idaho
  - Idaho State University
  - Affinity Health Plan
  - Adult & Pediatric Dermatology, PC

Practical Steps



- Revise (or do) breach notification policies and procedures
- Risk analysis – revisit (or do)
- Pay special attention to portable media and personal devices
  - OCR/ONC guidance on mobile devices
- Revisit (or do) incident response plan
- Prepare incident response team

Practical Steps

- Train entire workforce
  - Avoidance
  - Alert to potential breaches
  - Response to breach
- Be ready to respond to news media attention – have designated spokesperson
- Consider tightening business associate contracts, particularly for agents

Practical Steps

- Make the most of the "Secured PHI" safe harbor
  - Encryption!
  - Verify document destruction
- Try to prevent breaches in first place
- Audit access to PHI and enforce policies

Questions??

Rebecca Williams, RN, JD
Partner,
Co-Chair, Health Information Practice
Davis Wright Tremaine LLP
beckywilliams@dwt.com
(206) 757-8171

21160681_1