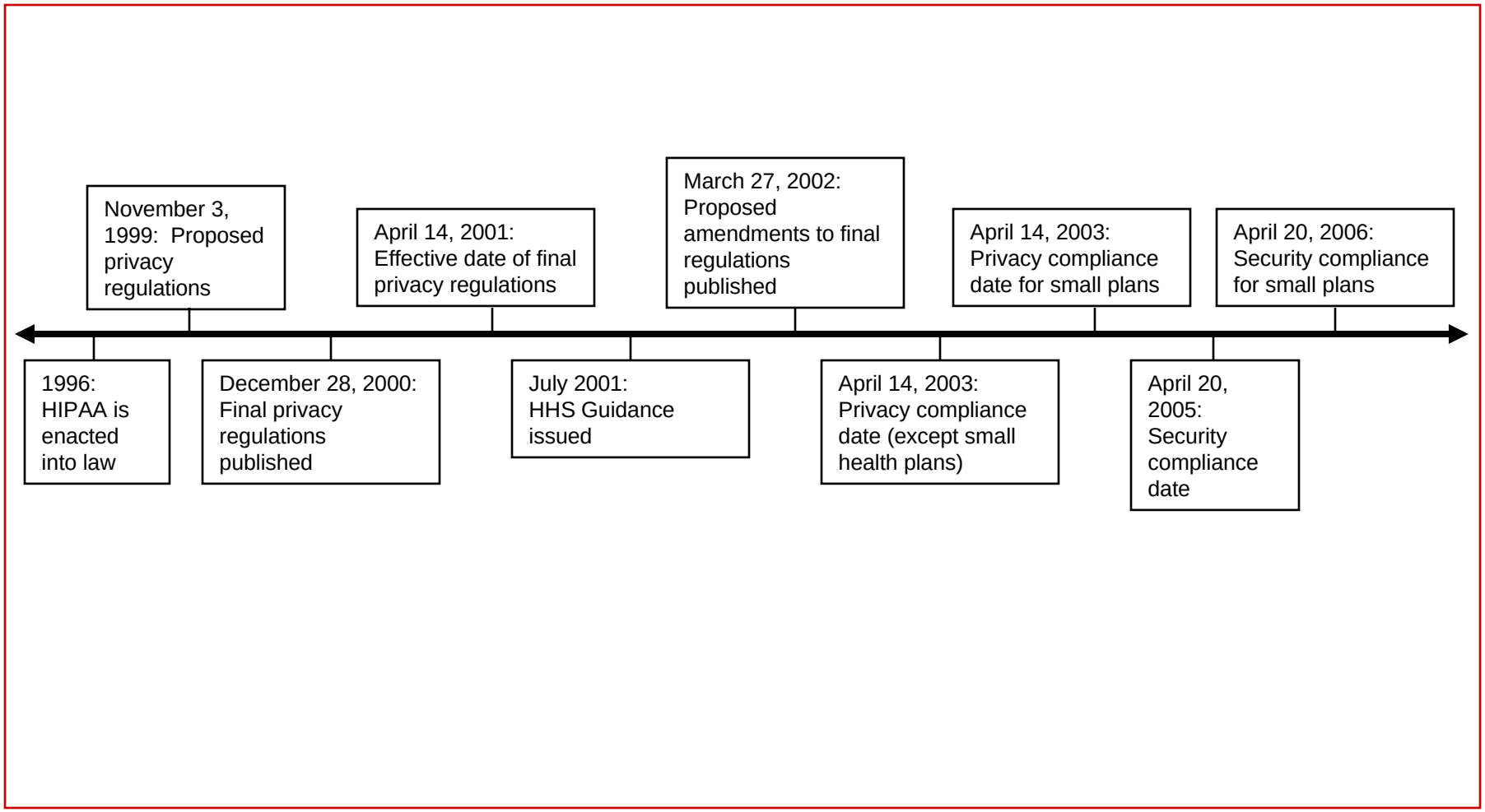
Advanced HIPAA Privacy Compliance Strategies: Those Nagging Issues That Don't Seem to Go Away

Rebecca L. Williams, RN, JD
Partner; Co-Chair of HIT/HIPAA Practice Group
Davis Wright Tremaine LLP
Seattle, WA
beckywilliams@dwt.com

Davis Wright Tremaine LLP

HIPAA Privacy — A Timeline



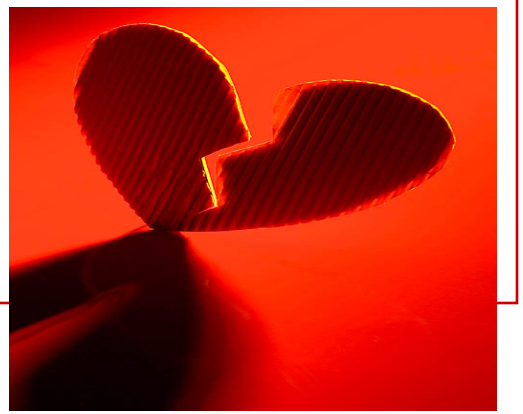
HIPAA Roulette

The Ex-Factor and Beyond

- Breaking Up is Hard to Do
- When Good Employees Go Bad

The Ex-Factor and Beyond

- Top risks for intentional misuse, improper disclosures and false accusations:
  - Ex-relationships: divorces, custody disputes, break-ups, new significant others, and so on
  - Ex-employees
  - Even ex-classmates such as high school/grade school grudges
- Other high-level risks include
  - Friends and family
  - Co-workers
  - Celebrities of one form or another



The Ex-Factor and Beyond

- Tip: When there is “history,” dig a little deeper
  - Could go either way
- Tip: Privacy Officer should be attuned to “gossip”
- Tip: Audit records of patients who may be temptations
- Tip: Revisit sanction processes, including termination
- Tip: Avoid even the appearance of impropriety

Complaint Process

Complaint Process

- When is a complaint a complaint?
- Must provide process to receive complaints
- Must document all complaints and their disposition
- Tip: Make it easy for a patient to complain
  - Written only vs. any medium
- Tip: Be aware of direct complaints that may become OCR complaints
- Tip: Pay attention to the follow-up
- Tip: Beware of promising complete confidentiality to complainant

Lost Laptop and Other Security Breaches

And other portable media and remote access issues

Lost Laptop and Other Security Breaches: It Can Happen to Your Organization

- "FBI Reports on Missing Laptops and Weapons," ***Washington Post*****,** February 2007
  - "The FBI said that 160 laptop computers were lost or stolen in less than four years, including at least 10 that contained sensitive or classified information . . . "
- "The Commerce Department has Lost 1,137 Laptop Computers Since 2001," **Associated Press,** September 2006
- **"**Computer Stolen From VA Subcontractor" ***Washington Post*****,** August 2006

Lost Laptop: Privacy Rule Requirements

- Have appropriate administrative, technical, and physical safeguards to protect the privacy of PHI
- Minimum necessary rule
- Duty to mitigate, to the extent practicable, the harmful effects of improper use or disclosure
  - Need to determine what actions, if any, will mitigate adverse effects
  - Notification may be appropriate mitigation, particularly if information includes SSN, DOB sensitive information, etc.)

Lost Laptop: Security Rule Requirements

- Ensure confidentiality, integrity and availability of ePHI
- Protect against reasonably anticipated
  - Threats to the security or integrity of ePHI
  - Mis-uses or improper disclosures of ePHI
- Assure workforce compliance
- Obtain assurances of confidentiality and security from contractors
- Risk analysis and risk management

Lost Laptop: Security Guidance

- Issued December 28, 2006
- HHS "**may rely upon this guidance** . . . in determining whether or not the actions of a covered entity are reasonable and appropriate"
- Guidance "**may be given deference in any administrative hearing** pursuant to the HIPAA enforcement rule."
- Recommends extreme caution to allow off-site use/access to PHI
- Need a "business case"

Lost Laptop: Security Guidance

- Give "significant emphasis and attention" to:
  - Risk analysis and risk management strategies
  - Policies and procedures for safeguarding ePHI (derived from the risk analysis and management)
  - Security awareness and training
- Policies and procedures, no matter how well designed, will not be effective unless a workforce receives appropriate training

Lost Laptop: Applying the Guidance

- Tip: Revisit risk analysis
  - Should the employee have had the laptop outside the organization? Is there a "business case"?
  - Did all that information need to be on the laptop?
- Tip: Revisit policies and procedures
  - Balance the practical needs with the privacy and security objectives
  - Plan the response to a breach, including
    - Appointment of point-person, spokesperson and team
    - Investigation approach
    - Be knowledgeable about legal requirements/best practices
    - Decision-making process for specific response

Lost Laptop: Training

- Tip: Take the opportunity for training workforce/encouraging workforce awareness
  - Focused training on directly affected personnel
  - Generalized training for other workforce
  - Training needs to be relevant and tailored
- Tip: facilitate workforce reporting of suspicions and making suggestions
- When it comes to privacy and security compliance, workforce
  - Biggest threat
  - Greatest resource

Lost Laptop: Sanctions

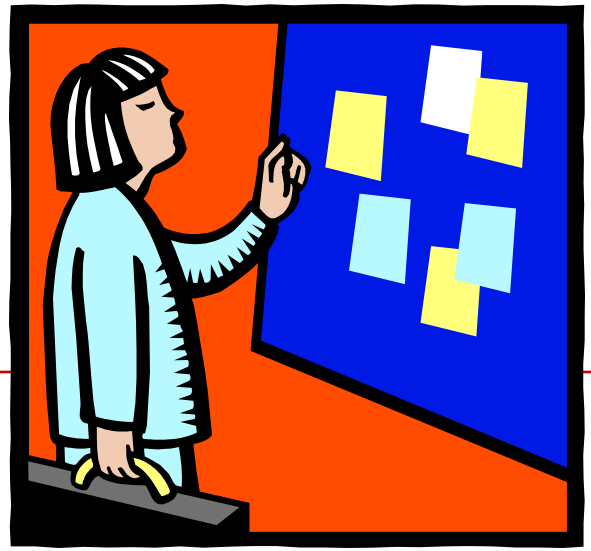
- Did any workforce act or fail to act in a manner that should result in sanctions?
  - Up to any including termination
  - Sanctions to be consistently applied
- May prove helpful when dealing with oversight and enforcement agencies
- Tip: Involve HR
- Tip: Ensure Employee Handbook is consistent with HIPAA requirements

Consumer Breach Notification

When do you have to report yourself?

Consumer Breach Notification

- HIPAA has no specific notification requirement but
  - Covered entities have a duty to mitigate
  - Accounting of disclosure for breaches (that are not incidental disclosures)
- Many state laws mandate notification
  - Notification triggers
  - Content requirements
- Beware: No good deed goes unpunished
  - Good citizens
  - Bad PR, class actions, etc.

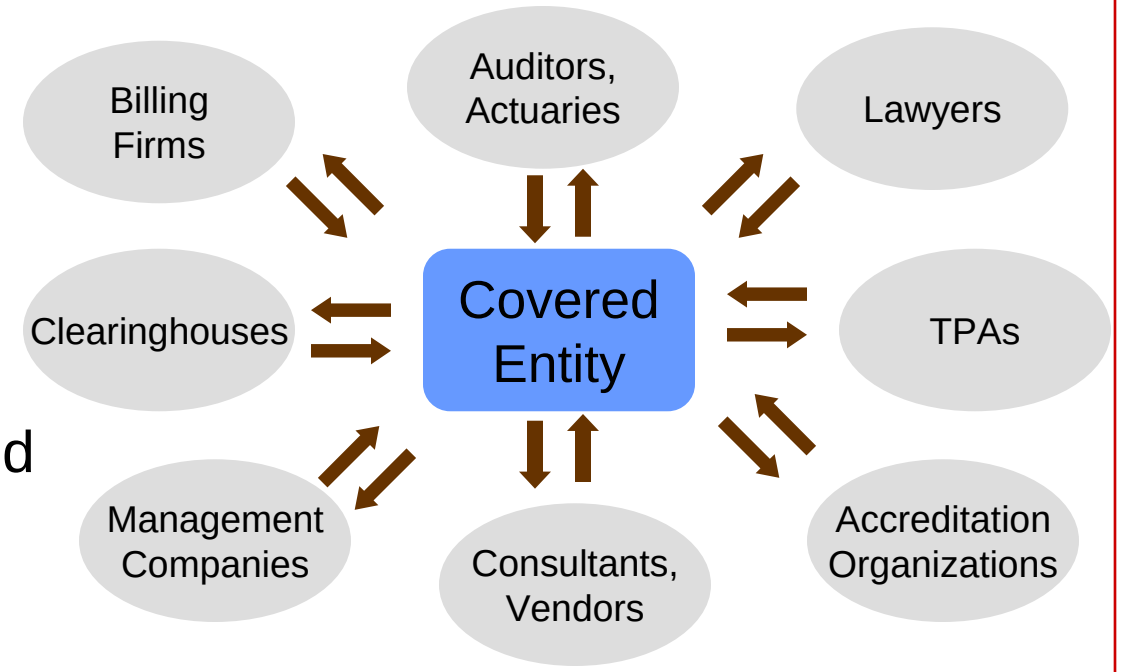


Business Associates

Continues to be a top area of confusion/frustration

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 PHI or
    - Otherwise covered by HIPAA
  - Performs certain identified services



Who Are Business Associates?

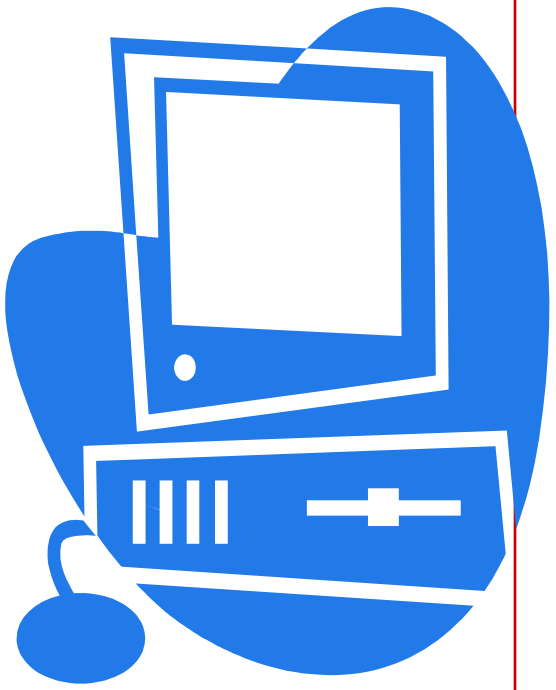
- Medical device company . . . Probably not
- Research sponsor . . . Usually not
- Record storage/destruction . . . Depends
- Accreditation organizations . . . Yes
- Lawyers . . . Definitely maybe
- Software vendor . . . Maybe
- Central EHR repository . . . Probably
- Provider participants in RHIO . . . Probably not

What Must Be in a Business Associate Contract — Privacy Rule

- Use and disclose information only as authorized in the contract
  - No further uses and disclosures
  - Not to exceed what the covered entity may do
- Implement appropriate safeguards
- Report unauthorized disclosures to covered entity
- Facilitate covered entity's access, amendment and accounting of disclosures obligations
- Allow HHS access to determine CE's compliance
- Return/destroy protected health information upon termination of arrangement, if feasible
  - If not feasible, extend BAC protections
- Ensure agents and subcontractors comply
- Authorize termination by covered entity

What Must Be in a Business Associate Contract — Security Rule

- Implement administrative, physical and technical safeguards that reasonably and appropriately protect the
  - Confidentiality,
  - Integrity and
  - Availability
  - Of *electronic* protected health information
- Ensure any agent implements reasonable and appropriate safeguards
- Report any security incident
- Authorize termination if the covered entity determines business associate has breached



Business Associate Contracts

- Tip: Contract management system
  - Revisit from time to time
- Tip: Do not forget the security requirements
  - When ePHI is involved, the privacy version is not enough
- Tip: In Health Information Exchange environment, the same BAC rules apply
  - Identify HIE participants, what information is accessed for what purpose
  - Determine role of each participant (e.g., business associates, providers, plans)
  - Use business associate contracts as applicable

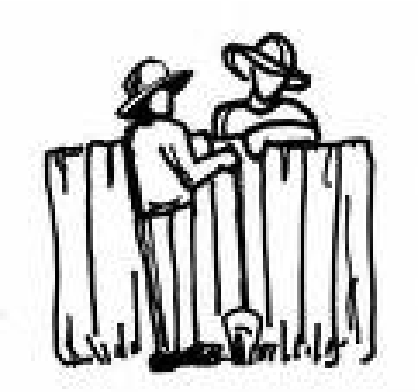
The Forgotten and Easily Confused Health Plan

The Forgotten and Easily Confused Health Plan

- Covered providers have employee benefit plans that likely are covered entities
- Treated as a separate entity
- Verify compliance efforts
  - Don’t forget FSAs and EAPs
- Compliance for privacy and security is required for all health plans

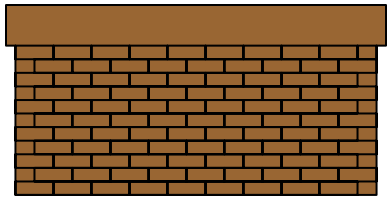
The Forgotten and Easily Confused Health Plan: Firewalls

- Health plan information must be used and maintained separately from employer functions
- Plan document amendments
  - Specify individuals allowed access for plan functions
  - Impose protections on information in hands of employer
- Authorization
- If hands-off PHI, Employer may receive only enrollment/disenrollment and summary plan information



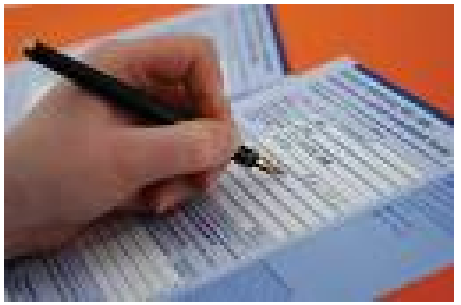
The Forgotten and Easily Confused Health Plan: Firewalls

- Confusion over what hat is being worn
  - Plan function v. Employer function
  - TPA
  - Employee Health
- Tip: Identify and segregate plan and employer functions
  - Need firewalls
  - Lines get blurred so plan ahead and verify when uncertain
- Tip: Need to educate relevant staff



The Forgotten and Easily Confused Health Plan: Misdirected Communications

- System problems sending communications, such as EOBs to the wrong person
- Failure to update
  - Divorces
  - Moves
  - Adult children
- Failure to respect alternate communication requests or promises of additional privacy protections



Access by Employees to Own/Family Records

Access by Employees to Own/Family Records

- HIPAA grants a right of access to an individual's own records
  - Some information is excluded
  - HIPAA allows for a process to respond to requests
- Employees of many providers access their own records and/or records of family members
- Slippery slopes
  - Information not subject to mandatory access
  - Records of children when they reach age to consent to certain services
  - Spouses records
- Tip: Revisit policy on subject
  - Often very political

Enforcement

A change in the status quo?

Enforcement: The Enforcement Rule

- Final Rule
  - Published: February 16, 2006
  - Effective date: March 16, 2006
- Uniform civil enforcement approach for all administrative simplification – DOJ remains responsible for criminal enforcement
- Signal for change in enforcement?
  - Continuing commitment to cooperation and assistance
  - HHS discretion continues
  - Mandates civil money penalties where a violation is found

Enforcement: Increased Activity

- Recent convictions – DOJ
  - *U.S. v. Machado & Ferrer* (Jan '07)
  - Defendants have not been covered entities
- Civil enforcement – CMS
  - 2 corrective action plans against plans
  - Violations of transaction and code set standards
- Audit - OIG

Questions