



Significant Risk of Harm

Coping with Breaches, Enforcement,
and Other Fallout under HITECH's
Breach Reporting and Enforcement
Rules

Edward Shay
Post & Schell, PC
October 25, 2011



The Premise

- Breach notification is transformational.
 - Unprecedented transparency
 - Convergence with enhanced enforcement
 - Triggers other HIPAA requirements
 - Changing business relationships
 - Changing how entities comply
 - Driving litigation



The life cycle of a breach

- A routine breach
 - Mass General resolution agreement
 - Workforce member commuting on public transit leaves behind paper billing records of 66 individuals and scheduling records of 192 others.
 - Names, addresses, DOBs, MRNs, diagnosis, insurance
 - No SSNs or driver license numbers (DLN)
 - No evidence any further use or disclosure
 - Outcome: the mundane becomes the expensive



The life cycle of a breach

- What is a "Breach?"
- Key elements
 - Acquisition, access, use, or disclosure
 - Unsecured PHI
 - Not permitted by Privacy Rule
 - Compromises security or privacy of the PHI



The life cycle of a breach

- Management of the incident/breach
 - “Discovery” of the incident/breach
 - Rule out exceptions (e.g., unintentional good faith, one time use, inability to retain)
 - Assess significant risk of harm
 - Assuming breach—give notifications
 - To individuals
 - To Secretary
 - Documentation, documentation, documentation



The life cycle of a breach

- The rest of HIPAA (Privacy, Security, Enforcement Rules) applies
 - A “breach” is an acknowledged privacy violation
 - Duty to mitigate (including known harm of BA’s violation)
 - Sanctions as appropriate (documentation)
 - Accounting for unauthorized disclosures (documentation)
 - Review of “safeguards”—policies, physical/technological security of records, access controls



The life cycle of a breach

- Assume records/PHI were on thumb drive as EPHI—Security Rule issues
 - “Breach” would be a “security incident”
 - Duty to follow security incident procedure
 - Document and report incidents/responses
 - Implications for security management process
 - Policies and procedures, risk analysis, sanctions, review IS activity



The life cycle of a breach

- The challenge of timely correction
 - To avoid penalties, Enforcement Rule requires correction within first 30 days “of such knowledge” of the failure to comply
 - In an EPHI “breach,” CE/BA will have knowledge of “security incident” and privacy violation at time of breach “discovery”
 - 30 days to correct is first ½ of 60 days to notify



The life cycle of a breach

- A “breach” under post-HITECH enforcement means:
 - Reported/admitted violation in the new “no fault” environment
 - For breaches with 500+ individuals, OCR always conducts a compliance audit
 - OCR now likely to investigate smaller breaches, conduct proactive audits
 - HITECH penalties escalate with culpability
 - Consider Cignet Health on failure to cooperate



The life cycle of a breach

- Lessons
 - Breach management does not occur in a silo
 - A breach implicates multiple HIPAA provisions and related requirements
 - Every breach has two clocks to beat, and correction runs faster than notification
 - Documentation is critical



Assessing Risk of Harm

- A breach must involve a “significant risk of financial, reputational or other harm”
- Requires a good faith judgment
- Made by business associate or covered entity
- Must include various relevant factors
- Must document basis for determination



Assessing Risk of Harm

- Three illustrative incidents
 - Laptop stolen from pulmonary lab with 800 patient names, age, height, weight, date of admit, date of study and test result for COPD and asthma. No SSN or DLN
 - Flash drive 2,800 patients unencrypted name, MRN, test ordered, test result, test date, testing location. No SSN or DLN
 - Documents including name, DOB, address, date of service, some SSNs found in home of former employee of BA arrested on unrelated ID theft charges



Assessing Risk of Harm

- Factors to consider
 - Types and amount of information
 - Name and fact of services not harmful
 - Type of service may be harmful
 - Perception of information drives “reputation”
 - Who used/to whom disclosed
 - Another covered entity subject to rules?



Assessing Risk of Harm

- Factors to consider
 - PHI format - verbal, paper, electronic
 - Immediate remedial steps (e.g., recovering before accessed/used or agreement not to access/use)
 - Type/nature of PHI (limited data set/data use agreement versus cancer, mental health, substance abuse, SSN, account number)



Assessing Risk of Harm

- Lessons and observations
 - In illustrative breaches, pulmonary lab and BA went unreported but thumb drive was reported. Where would you stand?
 - Risk of harm analysis has been controversial
 - Was it Congressional intent?
 - Final breach rule may drop risk of harm analysis



Discovery and investigation of a breach

- Incident starts the clock
 - Discovery = 1st day where have actual knowledge of breach, including when by using reasonable diligence would have known
 - "Prompt investigation"
 - Information needed for notice
 - Problem of false bottom and false negative finding
- Actual knowledge and "reasonable diligence" means
 - "Business care and prudence" expected of one "seeking to satisfy a legal requirement"



Discovery and investigation of a breach

- Knowledge imputed to covered entity from agents
 - Follows federal common law of agency
- Knowledge not imputed from independent contractors
- Affirmative duty to train workforce and agents
- Importance of clarity with business associates—before, during, after breach



Discovery and investigation of a breach

- Lessons
 - Not all BAs are independent contractors
 - Training is critical—SOPs
 - Need for rapid response process, designated people, timeline
 - State law may be more stringent
 - Again—watch related HIPAA duties



Notifications

- Written notice of a breach must be given to:
 - Affected individuals
 - Secretary
 - Covered entity by business associate
 - Sometimes the media
- Notice must be timely and adequate



Notifications

- To individuals
 - Timing—not later than 60 days
 - Content
 - What occurred and when
 - Types of PHI
 - Steps to protect individuals
 - What is being done to investigate, mitigate
 - Covered Entity contact information



Notifications

- To Individuals
 - Substitute notice (if outdated/no contact info)
 - Web site posting, newspaper, 800 number (if 10+ individuals)
 - Documentation requirements
 - Large breach media notice
 - 500 or more
 - Without unreasonable delay
 - Content same as individual



Notifications

- To the Secretary
 - Large breach notice given at time of individual notice
 - Fewer than 500
 - Not later than 3/1 of following year
 - On HHS web site
 - Content specified in dialog boxes



Notifications

- Notifications under state law
 - To State Attorneys General
 - Questions on long arm reach
 - Expect requests for payment or production of plans
 - Timing of notification may be much shorter
 - California in five business days



Notifications

- Lessons
 - Unprecedented transparency
 - OCR sees everything
 - State AGs come knocking
 - Free lunch for the media on a slow news day
 - Enterprise embarrassment
 - Admitting to potential harm
 - Trigger for litigation
 - With affected individuals
 - With business associates



The Laptop Problem

- Unencrypted laptops containing PHI remain the Achilles heel of HIM security
- 112 of 265 large breaches reported to OCR involved laptops (68) and other portable media (44)
- Unencrypted laptops are a huge enterprise risk



The Laptop Problem

- Converging factors heighten risk
 - 2006, CMS issued industry guidance on remote access and laptops
 - Covered entities should be “extremely cautious” in allowing offsite use/access to EPHI and then only where “great rigor” has been taken to assure effective policies and training
 - Laptop vulnerability has continued unabated
 - Encryption solutions less costly each year
 - OCR investigates all large breaches



The Laptop Problem

- Considerations
 - Encryption of data at rest “addressable” under the Security Rule
 - “Addressable” does not mean “optional”
 - Requires risk assessment
 - Requires documentation of why not “reasonable and appropriate” to implement
 - Requires implementing an alternative



The Laptop Problem

- Lessons
 - HITECH penalty scheme makes the culpability of inaction very risky
 - Looks a lot more like “willful neglect” than “reasonable cause”
 - Willful neglect = carelessness, reckless indifference
 - Reasonable cause = circumstances beyond one’s control where ordinary business care and prudence used
 - It is more effective to change the technology than the behavior of your workforce
 - It is time to encrypt if at all feasible

Breaches and HITECH Enforcement

- The breach notification rules
 - Require self disclosure/reporting
 - Invite investigation by OCR
- HITECH's enforcement IFR
 - Introduces "strict liability" unless violations are corrected w/in 30 days
 - Tiers of penalties
 - Tiers of culpability

Breaches and HITECH Enforcement

<u>Culpability</u>	<u>Amounts by tier</u>	<u>Cal. Yr. same violation max</u>
Did Not Know	\$100-\$50,000	\$1,500,000
Reasonable Cause	\$1,000-\$50,000	\$1,500,000
Willful Neglect-Corrected	\$10,000-\$50,000	\$1,500,000
Willful Neglect-Not corrected	\$50,000	\$1,500,000



Breaches and HITECH Enforcement

- Each tier encapsulates a standard of conduct
 - Did not know: “Reasonable diligence”—*business care and prudence* of person seeking to satisfy a legal requirement
 - “Reasonable cause”—exercise of *business care and prudence*; circumstances beyond control
 - “Willful neglect”—intentional failure, reckless indifference, carelessness → no affirmative defense, so penalties a certainty



Breaches and HITECH Enforcement

- “Business care and prudence” is key phrase in first two culpability tiers
- “Business care and prudence” taken from tax case law on failure to timely file
- Were you capable of exercising ordinary business care?
- Will look at contemporaneous actions



Breaches and HITECH Enforcement

- Amounts vary within each tier of penalty by factors in 160.408
 - Physical/financial harm (conceded by definition)
 - History of same issue (OCR can data mine your reports)
 - Ignored available guidance (mobile devices)



Breaches and HITECH Enforcement

- Other HITECH enforcement developments
 - Penalties apply to covered entities and business associates (lawyers included)
 - State Attorneys General may enforce
 - Criminal penalties now apply to workforce members who use/disclose PHI "without authorization"
 - Safe harbor for violations corrected in 30 days (assuming no willful neglect)



Breaches and HITECH Enforcement

- Lessons
 - Cignet shows OCR will enforce
 - HealthNet shows State AGs will act
 - Zhou shows that criminal charges apply
 - OCR seeking more resources, recently chastised
 - The bell tolls for us—you cannot win this game—except by prompt correction



Litigation and the Collateral Effects of Breach Notification

- Breach notification under HITECH has upended the old ways of HIPAA
 - Business associate agreements now on steroids
 - Covered entities are suing business associates
 - Individuals are suing covered entities
 - Covered entities are firing and employees are suing employers
 - State attorneys general are enforcing
 - DOJ is enforcing



Litigation and the Collateral Effects of Breach Notification

- Business Associate Agreements
 - Disputes over timing of notifications
 - Incident versus breach
 - Independent contractor versus agent
 - State law versus federal rules
 - Indemnification issues
 - Cyber-insurance issues
 - Service delineation/use, disclosure issues
 - Not provided is not authorized and a breach



Litigation and the Collateral Effects of Breach Notification

- Covered entities are suing business associates
 - Is the Monarch Fire Protection litigation the future?
 - HIPAA/HITECH standards emerging through
 - Claims for breach of contract
 - Misappropriation of trade secrets/proprietary information
 - Tort claims with HIPAA standard of care



Litigation and the Collateral Effects of Breach Notification

- Individuals suing covered entities
 - Large breaches lead to class action
 - Some based on state laws
 - Some based on common law claims
 - Claims hard to prove
 - Damages harder to prove
 - State AGs and DOJ are active
 - HealthNet targeted by multiple states
 - DOJ/FBI arrest the curious Dr. Zhou



Litigation and the Collateral Effects of Breach Notification

- Covered entities are terminating workforce and agents for HIPAA violations and getting sued
 - Widespread abuse of access to EHRs and misuse of PHI leads to terminations
 - Litigation on wrongful termination, discrimination and breach of contract
 - Unifying theme is HIPAA is a pretext, or HIPAA policies are selectively applied



Litigation and the Collateral Effects of Breach Notification

- Lessons
 - Notification and reporting foster unprecedented transparency
 - Transparency is driving accountability in all core HIPAA relationships
 - Accountability is placing a premium on preparedness, documentation, compliance and mitigation
 - There is no way back



Questions

Edward F. Shay
eshay@postschell.com
(215) 587-1151