New Mandates for Health Infosec

Bill Pankey, Tunitas Group

HIPAA2 and HIPAA^2

SF ISACA Health Professionals Day
July 21, 2010

ISACA®
Serving IT Governance Professionals
San Francisco Chapter

Agenda

HITECH Security Mandates

- Upgrades to the HIPAA security standard
  - Treatment of business associates
  - Reporting of security breaches
  - Enhanced enforcement
- EHR security standards
  - HIPAA applied to EHR
  - Certification
- Challenges

HIPAA2? Or HIPAA^2?

HITECH HIPAA upgrades have a ‘more of the same’ quality

- No rehabilitation of HIPAA standards, but
- New obligations and liability

HHS promotes HIPAA as the framework for EHR security standards

- HIPAA applied to her

However, HITECH introduces a new HIPAA problem set requiring qualitatively different level of effort

HITCH Shifts the Focus

<u>Administrative</u> simplification -> security standards mandated by HIPPA

- Protection required to secure *reimbursement* related transactions
- Clinical information is secondary
    - ie, still no claims attachment rule

Automation of <u>clinical workflow</u> -> security requirements (explicit & implicit) of HITECH

- Protection required to secure *clinical* transactions involving practitioners
- Clinical information is primary

Change in Risk Calibration

Reimbursement transactions

- High value for timeliness
  - Dependent authorization decisions
    “care delayed is care denied”
  - Mandatory reporting, billing windows
  - Obvious economic value (for providers) in timely completion
  - Expediency prevails (many examples)
- Low value for accuracy
  - Transactions are readily rescinded / corrected / adjusted

Changes Risk Calibration

Clinical transactions

- Low value for timeliness
  - Practitioners are trained to act upon available information
  - Much of health info is dated with relatively little immediacy
  - Typically have the option of re-doing important studies
- High value for accuracy
  - Absolute practitioner liability for the care delivered. Historically, ‘bad data’ is not an effective defense
  - Once the procedure \ treatment delivered, cannot be simply ‘revoked’

Differing Information Values

Example:

1996 HIPAA Law mandated electronic signature standard to ensure authenticity of reimbursement transactions

- CMS refusal to act. Expediency trumps strong practitioner accountability for statements made in support of healthcare claims.

EHR Standards (by inclusion) require use of electronic signature to support mandated eRx, CPOE

- Practitoner's historical role as a control for the appropriateness of medical treatments

HIPAA2 Part

Business Associate problem and ‘fix’

Handling of security incidents

Enhanced penalties

1. Business Associates under HIPAA

Business associates are not subjects of the 1996 Public Law 104-191, i.e. not a plan, provider or healthcare clearinghouse

- *but* receive, process, maintain or disclose significant quantity of health information on behalf of covered entities

Security rule ‘workaround’

- require CE diligence as part of risk assessment activity
- require covered entities to obtain assurances that BA will *appropriately protect* the shared PHI
    - Allow (but not require) CE to terminate contract for material breach of privacy and security provisions of contract

Business Associate Problem

HIPAA’s BA provisions exacerbated the ‘rule interpretation’ problem

- Covered entity needed to communicate its understanding of requirements to BA
  - Interpretation necessarily idiosyncratic
    - §164.306(b) flexibility of approach
  - the CE’s circumstances? the BA’s circumstances?
- but requirements should also calibrated relative to the risk that the BA’s activities and environment created for the information

Result: M covered entity clients each provide the business associate with a different specification of the HIPAA requirement

Business Associate Example

Example, Health plan BA that routinely receives and processes healthcare claims related to appx. 25M members.

Multiple CE clients required 1 or more of the following:

1. Submission of the BA’s risk assessment and “HIPAA compliance” self-evaluation
2. Certification of compliance with the CE’s security policy
3. Certification of SOX compliance
4. Satisfactory SAS-70
5. Satisfactory 3rd party ‘HIPAA security’ audit
6. Risk assessment by covered entity staff
7. Accreditation by industry quality organization (NCQA; URAC)
8. Implementation of specific technical security measures
9. Implementation of specific security procedures

Consequence

Inefficient diligence process

- Exacerbates the CE’s risk assessment issue w/ 10s or 100s of BA
- Evaluates the ‘same risk’ from perspective of multiple frameworks & methodologies

Unrealistic & inefficient security requirements

⇒ Business associate treats the HIPAA requirement as a customer relationship management problem

- Agree to whatever necessary to ‘make the deal’
- *Finesse* the requirements of individual clients

HITECH Solution

1. Require, as a matter of Federal law, that business associates comply with HIPAA security rule
   - HHS enforcement; penalties for non-compliance

2. Subject the BA to Federal penalty should it use or disclose PH in a manner not permitted by its contracts with covered entities.

3. Remove covered entity's liability exception for the willful failures of business associates
   - CE must continue to apply diligence to business associates and in the case of agents, oversight.

HITECH Solution

Probably good for PHI protection

- Greater regulatory scope
- Increased CE liability

↑ BAs must maintain HIPAA mandated documentation

- Standard basis for CE diligence?

2. Incident Response

HIPAA requires incident response procedures

- 'incidents' very broadly defined
  - “known or suspected” ... “attempted or successful use, disclosure, modification, interference”
- mitigate harmful effects of known incidents
- document
- BA’s have to report to CE

Most CE’s and BA have been unwilling to put in place the substantial resources to perform required investigations of “suspected attempt”

- Substantial pressure to discount network & system anomalies
- BAs seek finesse in reporting

State Breach Notice Laws

Belief that notifying subjects of a breach mitigates the potential for subsequent financial fraud, identity theft

- ‘monitor your credit report’

California’s breach notification law (SB1386)

- Includes requirement to notify in case of inappropriate disclosure of personal health information. Only state to do so (as of 2009)

National players concerned about ‘patchwork’ of state law

HITECH Required Notices

Notice to information subjects (patients, plan members) required where there is a breach that poses *significant risk of financial, reputational or other harm to the individual*

Breach defined broadly as acquisition, access, use or disclosure

- Access means capability to read, write, modify, transmit PHI or otherwise sue system resources.

HITECH Notice Requirements

Notice must

- be timely (no more than 60 days past discovery)
- provide details of breach (what happenned; date of breach; date of discovery)
- identify information involved in breach
- recommend action subjects should take to protect themselves from further harm
- describe what is be done to investigate the breach, mitigate harm to subjects and prevent future breaches

Breaches involving more than 500 individuals must be reported to HHS, local media

Risk Assessment

HIPAA required risk assessment provides a basis for determination of the level of harm to individuals

- No presumption of harm to individuals

- "Harm" must be specific (measureable, tangible)
  - Mere embarassment is not 'harm'
- Some 'harms' may be completely mitigated
  - eg., rollback \ correct data errors

Enumerate potential harms, assess capability to mitigate, and conditional likelihood of occurance

- Maintain documentation
- Burden of proof lies with the experiencing the breach

Further Considerations

- Business associates must report breaches to CE

  CE must notify affected individuals

- *Per regulation*, encryption eliminates the potential for harm.
  - Appropriately encrypted data is deemed 'secure'
    - breaches are not possible?

3. HIPAA toothlessness

Enforcement has been *complaint* driven

- HHS generally seeks voluntary ‘corrective action”
  - 16K complaints => 11K corrective action plans;
5K no violations
450 referrals to DOJ for possible criminal prosecution
- No imposed civil monetary penalties
  - Providence, $100k ‘administrative fee’
  - ☼ CVS , $2.5M settlement w/ HHS & FTC
- Consequences of 2008 CMS audits unknown

Enforcement under HITECH

HHS must conduct a formal review of a complaint where there is indication of willful neglect.

HHS must conduct compliance review once it is aware of facts indicating violations due to willful neglect (no complaint needed).

HHS must impose civil penalty for violations due to willful neglect.

Civil Penalties under HITECH

Tier	Description	Fine per Violation	Allowable Imposed per Year
A	Offender did not realize he or she violated the Act and would have acted differently had he or she known	$100	$25,000
B	Violations due to reasonable cause, but not willful neglect	$1,000	$100,000
C	Violations due to willful neglect that were ultimately corrected	$10,000	$250,000
D	Violations due to willful neglect that were not corrected	$50,000	$1,500,000

Standards for EHR

HITECH directs HHS to develop a Federal Health IT Strategic Plan, that includes “objectives, milestones, metrics” with respect to ensuring:

- Privacy and security protections for electronic exchange of individual health information
- Appropriate authorization
- Authentication of healh information
- Encryption

Standards for EHR

HITECH directs HHS to develop a Federal Health IT Strategic Plan, that includes “objectives, milestones, metrics” with respect to ensuring:

- Privacy and security protections for electronic exchange of individual health information
- Appropriate authorization
- Authentication of healh information
- Encryption

Strategy supported by voluntary certification of health information technology

- Establishes EHR security standards

Certification Criteria

HIPAA used as the framework for EHR security criteria. Specific standards and criteria for:

- Access control
- Emergency access
- Automatic log off
- Auditing
- Integrity
- Authentication (local and network)
- Encryption
- Accounting of disclosures

Functionally tested through independent certification program.

- NIST accredits certification bodies.

Challenges

- HITECH mandates specific EHR use cases:
  - Patient's electronic access to health information
    - Authentication of individual requesting data?
    - Ensure appropriate patient identity?
    - Allow patient ability to control access (ie delegate)
  - Cross enterprise information sharing
    - Authorization
    - Role standardization (structual?or functional?)
    - Access control policy
    - Emergency access