Navigating the Interface Between the HIPAA Privacy and Security Rules

Presented by:

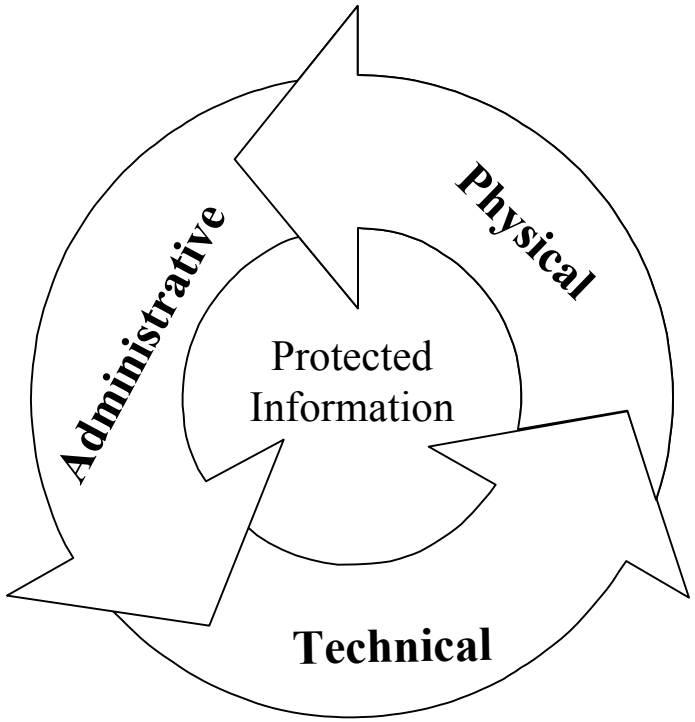
McDermott, Will & Emery

Michael L. Blau, Esq
28 State Street
Boston, MA 02109
617-535-4010
mblau@mwe.com

Marilyn Lamar, Esq.
227 W. Monroe Street
Chicago, IL 60606
312-984-7586
mlamar@mwe.com

Introduction

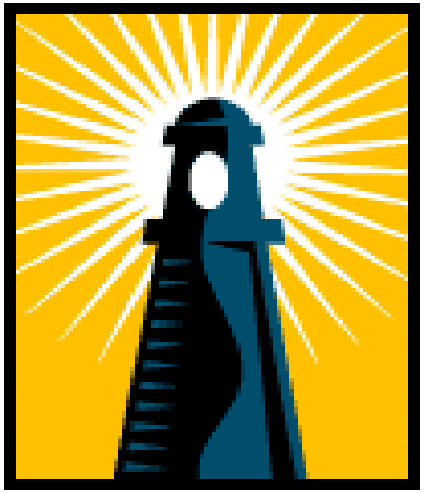
Security in Service of Privacy



- Guards the confidentiality, integrity and availability of health information

Introduction (cont.)

- Similarities between the HIPAA Privacy and Security Rules
  - Intended to be compatible
  - Both protect confidentiality of electronic PHI ("ePHI")
  - Both provide workforce access controls and protections
  - Both require business associate contracts with vendors



Introduction (cont.)

- Similarities between the HIPAA Privacy and Security Rules
  - Both require written compliance policies and procedures
  - Similar sanction and mitigation requirements
  - Same approach to Affiliated Covered Entities (ACEs) and hybrids
  - Coordinated compliance infrastructure

Introduction (cont.)

- Differences between the HIPAA Privacy and Security Rules
  - Scope--electronic PHI vs. PHI
  - Standards for workforce access – not focused on minimum necessary
  - No exceptions for incidental uses and disclosures
  - Broader audit trail advisable – not limited to responding to patient request for accounting

Introduction (cont.)

- Differences between the HIPAA Privacy and Security Rules
  - Continued monitoring required
  - New security policies and procedures
  - Periodic update requirement
  - No Organized Health Care Arrangement (OHCA)
  - Need to coordinate organizational and compliance structures
  - New group health plan requirements

Scope Issues: PHI

- Security standards apply only to ePHI
  - Transmission of information already in electronic form
- Privacy standards apply to PHI transmitted or maintained in any form or media
  - Workforce who work at home with paper-based records vs. electronic records

Scope Issues: PHI (cont.)

- Privacy standards, but not security standards, apply to verbal person-to-person communications, telephonic communications, paper-based records, paper-to-paper faxes, videoconferences, voicemails, xerox/copying systems
- Both apply to transmissions by computer, internet, extranet, leased lines, dial-up lines, private networks, faxback systems, telephone voice response systems, voicemail forwarding

Scope Issues: PHI (cont.)

- Includes physical movement of transportable electronic storage media

– Both apply to wireless remote access

– Security standards for non-ePHI?

Threshold Organizational Considerations

- Coordinates with organizational requirements under Privacy Rule
- Affiliated covered entities
  - Under common ownership or control
  - Designate as a single covered entity
  - CE is responsible for privacy/security rule compliance of its ACEs

Threshold Organizational Considerations (cont.)

- Covered entity vs. hybrid entity
  - Designate covered components
  - Firewall covered components from noncovered components
  - Privacy training/security training
  - Responsibility for privacy/security breaches
  - Applicability of privacy/security policies and procedures

Threshold Organizational Considerations (cont.)

- Organized Health Care Arrangement
  - OHCA is unique to the Privacy Rule:
    - Members not required to have business associate agreements
    - Members could use joint Notice of Privacy Practices and common policies
  - Security Rule does not include OHCA concept, so each member of an OHCA:
    - Needs to conduct risk assessment, adopt security policies and procedures, educate workforce, etc.
    - May need to sign a business associate agreement if another OHCA member handles ePHI on its behalf

Policies and Procedures

Privacy Rule

Workforce Policies
- Access/Minimum necessary standard
- Training

Patient Rights Policies
- Access, Inspect, Copy
- Alternative means of communications
- Accounting of disclosures
- Amendments
- Restrictions
- Complaints

Notice of Privacy Practices
Acknowledgement of Receipt
Authorizations/Consents
Required and Permitted Disclosures
Business Associates
Employee Sanctions
Mitigation
Whistleblower Protections

Security Rule

Administrative Safeguards
- Security management process(R)
  - Risk analysis (R)
  - Risk management (R)
  - Sanction policy (R)
- Assigned security responsibility (R)
- Workforce security (R)
  - Authorization/Supervision (A)
  - Workforce clearance (A)
  - Termination procedures (A)
- Information access management(R)
  - Isolate clearinghouse functions (R)
  - Access authorization (A)
  - Access establishment/modification (A)
- Security awareness and training (R)
  - Security reminders (A)
  - Protection from malicious software (A)
  - Log-in monitoring (A)
  - Password management (A)
- Security incident procedures (R)
- Contingency plan (R)
  - Data backup plan (R)
  - Disaster recovery plan (R)
  - Emergency mode operation plan (R)
  - Testing and revision procedures (A)
  - Applications and data criticality analysis (A)
- Evaluation (R)
- Business associate contracts (R)

Physical Safeguards
- Facility access controls (R)
  - Contingency operations (A)
  - Facility security plan (A)
  - Access control and validation (A)
  - Maintenance records (A)
- Workstation use (R)
- Workstation security (R)
- Device and media controls (R)
  - Disposal (R)
  - Media re-use (R)
  - Accountability (A)
  - Data backup and storage (A)

Technical Safeguards
- Access control (R)
  - Unique user Id (R)
  - Emergency access (R)
  - Automatic logoff (A)
  - Encryption and decryption (A)
- Audit controls (R)
- Integrity (R)
  - Authenticate ePHI (A)
- Person or entity authentication (R)
- Transmission security (R)
  - Integrity controls (A)
  - Encryption (A)

Policies and Procedures (cont.)

- Amend Privacy policies and procedures to coordinate with Security policies and procedures
- Flexibility for Security policies vs. specific Privacy policy requirements
  - May use any security measures that allow the CE to reasonably and appropriately implement security standards
  - Decision factors:
    - Size, complexity and capabilities of CE

Policies and Procedures (cont.)

- CE's technical infrastructure, hardware and software security capabilities
- Cost of security measures
- Probability and criticality of potential risks to ePHI
- Required vs. addressable specifications

– Addressable specifications - Assess whether Implementation Specification is "reasonable and appropriate" for CE
  - If so, implement
  - If not, document why not and identify and implement equivalent attainable measure "if reasonable and appropriate"

Policies and Procedures (cont.)

- "Reasonable and appropriate" analyzed with reference to "likely contribution" to protecting ePHI
  - Problem of Monday Morning quarterbacks
- External certification not required, but may be prudent

Policies and Procedures (cont.)

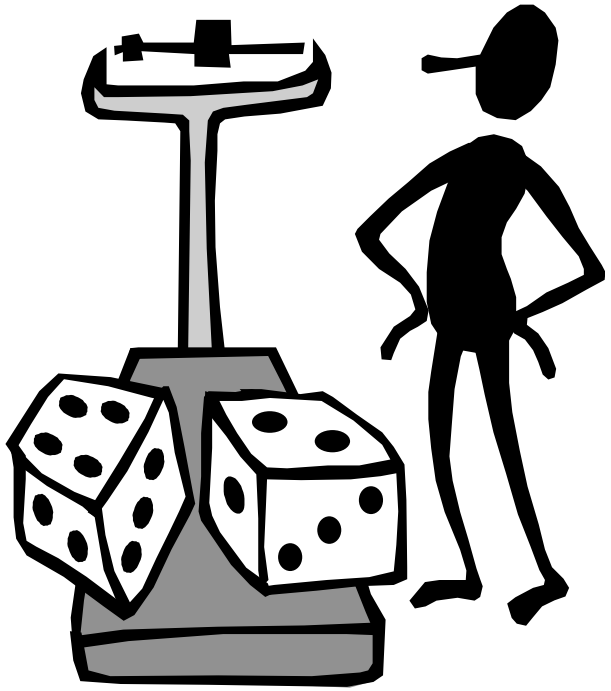
- Updates - Review Security policies and procedures periodically and update in response to environmental or operational changes affecting the security of ePHI
  - "Periodic" not defined
  - Upgrade security safeguards (CQI)
  - No periodic review or update requirement for Privacy policies

Risk Management

- Risk assessment the first step in Security Rule compliance
  - Conduct an accurate and thorough assessment of potential risks to ePHI; consider "all relevant losses" caused by unauthorized uses/disclosures if security measure is absent
    - Quantitative vs. qualitative assessment information
    - Assess assets, value of assets, threat/ vulnerability of assets, frequency/probability of threat, magnitude of potential loss, available protective safeguards, safeguard effectiveness, relative cost

Risk Management (cont.)

- Risk management goals
  - Risk elimination
  - Risk reduction
  - Risk transference
  - Risk acceptance



Risk Management (cont.)

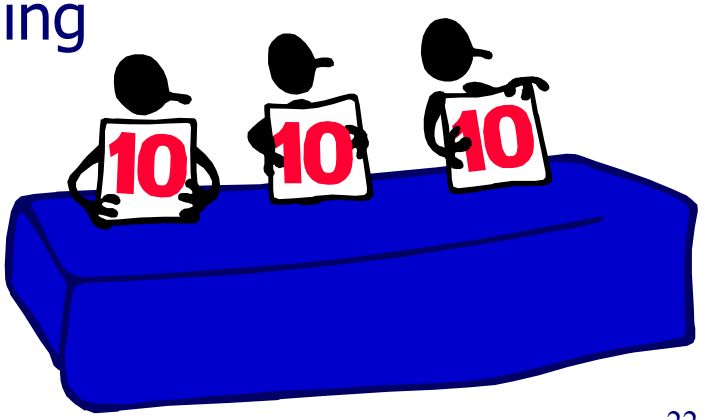
- Privacy Rule does not focus on risk assessment, although many CEs performed gap analysis
- Control evidence of non-compliance in analysis and assessment process
- Attorney-client privilege advisable for analysis and assessment under both Rules

Attorney-Client Privilege

- Attorney-Client Privilege may protect communications and work product
  - To help secure privilege:
    - Use attorneys to engage consultants
    - Identify legal reasons for investigation
    - Identify counsel as person conducting investigation
    - Advise employees of confidential nature of investigation
    - Have counsel present at discussions

Controlling Evidence of Non-Compliance

- Reports and scorecards
- Avoid overly negative language and conclusions
  - Send directly to counsel
  - Limit access to senior level
  - Consider not distributing electronically
- Examples to avoid:
  - "Red, yellow, green" coding
  - "There are over 1,000 identified HIPAA gaps"



Controlling Evidence of Non-Compliance (cont.)

- Have counsel involved with memos to file if deciding not to undertake remediation measures
  - Required v. addressable implementation specifications
  - Required risk analysis
- Consider disclosure responsibilities to investors and auditors

Audits v. Accountings

- Security Rule requires records sufficient for audits (i.e., access reports, activity log, movement of hardware/electronic media, security incident tracking)
- Privacy Rule does not require audits
  - Requires records to satisfy patient's right to receive an accounting of disclosures
  - Significant exceptions for privacy accountings (payment, treatment and operations) not exceptions under Security Rule

Workforce Access Controls

- Implementation Standards

Privacy Rule

Minimum necessary standard ("MNS")

- MNS protocols for routine recurring workforce disclosures
- Individualized MNS determinations for other workforce disclosures per criteria
- No disclosure of entire medical record except when specifically justified

Privacy training

Workforce sanctions

Security Rule

Administrative measures - prevent unauthorized workforce access

- Authorization/supervision procedures
- Workforce clearance
- Access modification/termination procedures
- Security awareness and training
- Periodic security updates
- Log-in monitoring
- Password management

Physical safeguards

- Facility access limited to authorized persons
- Workstation security

Technical safeguards

- Unique user ID/Authentication
- Audit controls (use and activity, security incident tracking and response)

Workforce sanctions

Workforce Access Controls (cont.)

- General standards
  - Privacy Rule -- reasonable effort to limit access of authorized persons or classes of persons to PHI to which access is needed to carry out their duties
    - Reasonableness standard
    - Security requirement currently effect

Work Force Access Controls (cont.)

- Security Rule Standards

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the privacy regulations.

(4) Ensure compliance with this subpart by its workforce.

Workforce Access Controls (cont.)

- "Ensure" is a higher standard?
  - Congress intent to "set an exceptionally high goal for the security of [ePHI]"
  - Required to "take steps, to the best of [the CE's] ability to protect [ePHI]" 68 Fed. Reg. 8346
  - Protect against any reasonably anticipated uses or disclosures that are not permitted or required
  - Implement through "reasonable and appropriate policies and procedures"
- Violation of Security Rule by workforce may/would violate Privacy Rule as well

Security Incidents

- Security incident - means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system
  - Violation of privacy standards (e.g., unauthorized workforce access) may constitute a "security incident"

Security Incidents (cont.)

- Policies and procedures to address security incidents
  - Identify and respond to security incidents
  - Mitigation requirement
  - Document security incidents and their outcomes
  - BA reporting requirement
- Coordinate with Privacy Rule complaint procedures
  - No mandatory privacy breach reporting by workforce under Privacy Rule
- Whistleblower protections

Enforcement Standards

- Common enforcement standards
- Civil Penalties (HHS/OCR)
  - CMP of $100 for each violation; $25,000 annual cap on total CMP for identical violations
  - CMP may not be imposed if CE did not know, and by exercising reasonable diligence would not have known, of such violation

Enforcement Standards (cont.)

- CMP may not be imposed if violation was due to "reasonable cause and not willful neglect", and is corrected
- CMP may be reduced to the extent the penalty would be excessive relative to the compliance failure involved
- Notice and hearing requirements; ALJ hearing; review by Departmental Appeals Board

Enforcement Standards (cont.)

- Interim enforcement rule published in April 2003 applies to both Privacy and Security Rules
- "Compliance and Enforcement" sections of Section 160.300 address the following for Privacy but not Security:
  - Cooperation and assistance of CEs
  - Complaint procedures
  - Compliance reviews by Secretary of DHHS
  - Responsibilities of CEs

Enforcement Standards (cont.)

- Criminal Penalties (DOJ)
  - Knowingly - 1 year/$50,000
  - False pretenses - 5 years/$100,000
  - Malice, commercial advantage, personal gain - 10 years/$250,000

Business Associate Requirements

- Need to amend BA contracts by April 21, 2005 to address Security requirements
- Same liability standards - failure to cure or report known pattern of violative activity
- Same material breach/termination standard
- Most difficult issue – determining what specific safeguards to require a Business Associate to implement to "reasonably and appropriately" protect the confidentiality, integrity and availability of ePHI

Business Associate Requirements (cont.)

Privacy Rule

- Establish permitted and required uses and disclosures of PHI by BA
- Prohibit BA from using or disclosing PHI except as permitted by contract or law
- Require BA to use appropriate safeguards to prevent improper use or disclosure of PHI
- Report to CE improper use of PHI of which BA becomes aware
- Ensure that agent of BA agrees to same restrictions
- Make PHI available for access, amendment, accounting
- Make books and records available to Secretary for compliance purposes
- Upon termination, return or destroy PHI or extend protections

Security Rule

- Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI that BA creates, receives, maintains or transmits on behalf of CE
- Report to the CE any security incident of which it becomes aware
- Ensure that any agent of BA agrees to implement reasonable and appropriate safeguards to protect ePHI

Business Associates

- Specifics to consider with IS vendors:
  - Access for implementation and ongoing support
  - Maintain confidentiality of passwords, IDs, keycards and tokens
  - Responsibility for viruses, worms, etc.
  - Notice if the vendor's systems have been compromised
  - Agreement to not access more than the minimum necessary data or systems

Contracting for Security Consultants

- Scope of services
  - Definition
  - Description of milestones
  - Description of deliverables
  - Commencement and completion dates
- Avoid "scope creep"
  - Through change control provisions
  - Through project management

Contracting for Security Consultants (cont.)

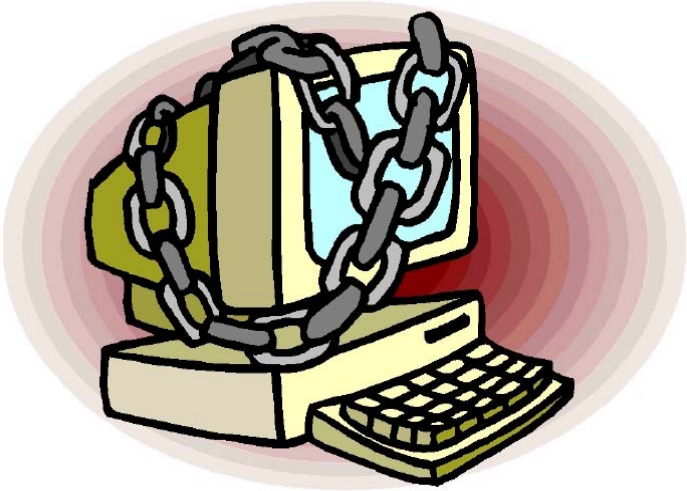
- Consider using RFP/RFI descriptions
- Resist attempts to shift obligations through use of "Assumptions" and "Client Responsibilities"
- Consultants typically disclaim responsibility for "legal advice"
- Carefully analyze indemnification provisions and limitations of liability

Contracting for Security Consultants (cont.)

- "Governance provisions" - include for large or complex projects
  - Periodic meetings and reports
  - Assign liaisons
  - Include project plan and schedule
- Limit individuals who can authorize additional work/fees

Group Health Plans

- Plan documents must be amended to require the plan sponsor to:
  - Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the ePHI it creates or handles for the plan



Group Health Plans (cont.)

- Plan documents must be amended to require the plan sponsor to:
  - Ensure that the adequate separation required by the Privacy Rule is supported by appropriate security measures
  - Ensure that any agents and subcontractors to whom it provides ePHI agree to implement reasonable and appropriate security measures to protect ePHI
  - Report to the group health plan any security incident of which it becomes aware

Miscellaneous

- Privacy official/Security official
  - One person must have ultimate responsibility
  - Can be the same person for Privacy and Security Rules
- Training:
  - Who must be trained – broader scope in the Security Rule
  - Periodic security updates vs. Privacy Rule retraining only for material changes in privacy policies

Miscellaneous (cont.)

- Disposal - Restrictions on use/disclosure of PHI under Privacy Rule vs. reasonable and adequate policies for disposal of hardware/ePHI media storage under Security Rule
- Preemption analysis for Privacy regarding more stringent state laws does not apply to Security

Conclusions

- Need effective privacy/security compliance program
  - Secure information infrastructure is mission critical in the health industry
  - Heightened security concerns post-9/11
  - Heightened accountability of boards post-Enron
    - Application of Sarbanes-Oxley to nonprofits, including reporting of "material operational issues"
    - Obligation to know and reasonably address ePHI security issues

Top Ten Tips for Compliance

- Start now; educate board and management
- Coordinate with strategic planning process
- Educate everyone that the Security Rule is not just an IT issue
- Use a corporate compliance approach for meeting and maintaining requirements

Top Ten Tips for Compliance (cont.)

- Define business objectives, resources and limitations
- Determine scope -- narrower than the Privacy Rule in some respects and broader in others
- Use caution in documenting risk analysis
- May enhance confidentiality to have counsel engage consultants

Top Ten Tips for Compliance (cont.)

- Make sure policies and procedures are industry standard (or better)
- Keep top management informed and engaged

SECURITY IS EVERYONE'S BUSINESS