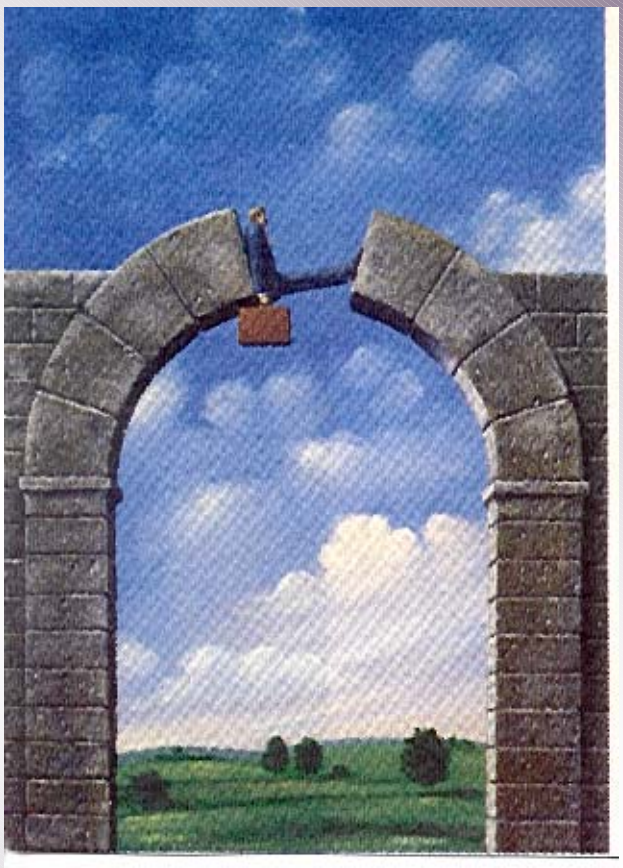
University of Missouri
HEALTH CARE

Implementing an Audit Program for HIPAA Compliance

Mike Lynch

Fifth National HIPAA Summit
November 1, 2002



Seven Guiding Principles of HIPAA Rules

- **Quality and Availability of Care** – Nothing in the proposed HIPAA rules should interfere in any way, with the delivery of quality health care, or threaten the financial stability of health care organizations.
- **Notice** – The Patient has a right to know what information is maintained about them, and how that information may be used or disclosed.
- **Minimum Necessary** – The workforce of health care organizations should access and use only the minimum necessary information about patients to accomplish their assigned duties.

Seven Guiding Principles of HIPAA Rules

- **Onward Transfer** – The Patient has an ownership interest in their confidential information, and has a right to control subsequent uses and disclosures of their confidential information. They also have the right to request an accounting of all such disclosures.

- **Data Security/Privacy/Integrity** – Those who store, process, transmit or use confidential patient information, have an obligation to reasonably protect its confidentiality, and to prevent unauthorized alterations.

Seven Guiding Principles of HIPAA Rules

- **Access** – The Patient has a right to inspect their confidential information to ensure its accuracy and completeness, and to request that erroneous information be corrected.

- **Enforcement** – The Patient has a right to redress of privacy violations. Health care organizations must reasonably prevent and detect the abuse of patient information, mitigate further loss, and sanction offenders.

Five Steps Toward Compliance

- Create appropriate policies and procedures
- Provide context sensitive policy training
- Provide the necessary tools and facilities
- Audit to ensure compliance
- Sanction offenders

Why Audit?

Both the Security NPRM and the Final Privacy rule require access on a minimum need-to-know basis.

- ✓ Must be able to demonstrate that system(s) for accessing information meets these standards
- ✓ And that the entity monitors access to verify that unauthorized access is not occurring.

Why Audit?

Section 160.310—Responsibilities of Covered Entities

"A covered entity must keep such records and submit such compliance reports, in such time and manner and containing such information, necessary to enable the Secretary to ascertain whether the covered entity has complied or is complying with the applicable requirements of part 160 and the applicable standards, requirements, and implementation specifications of Subpart E of Part 164." Refer to § 164.530 for discussion.

Definitions

The Security NPRM does not provide an exact definition, either in the preamble or the specific text proposed for the CFR for either 'audit trail' or 'audit control'. Health care entities are required to put in place whatever mechanisms are deemed necessary that would enable the organization to record and examine system activity so that an organization can identify suspect data activity, see if high-risk patterns are present, assess its security program and respond to potential weaknesses.

- The Security NPRM defines **AUDIT CONTROLS** as "mechanisms employed to record and examine system activity"

Definitions

- An **AUDIT TRAIL** can be defined as the result of monitoring each operation on information. “(It) …is a chronological record of activities occurring in the system, created immediately concurrent with the user.” (Source: CPRI Security Guidelines).
- WEDI defines **AUDIT TRAIL** as “the result of monitoring each operation on information.” Generally **Audit Trail** identifies **Who** (login ID) did **What** (read-only, modify, delete, add, etc) to what data (identify member and data about that member that was acted upon), and **When** (date/timestamp).
- The Privacy Rule also wants to know “**Why**” the data was accessed, so audit logs created with the Privacy rule in mind will have to go beyond the simple capture of login name, date/timestamp, and action taken associated with the data that was accessed.

A Covered Entity Must Keep an Audit Trail of Disclosures:

- Where authorization is required, and whether initiated by the covered entity or by the individual (i.e. for purposes other than treatment, payment or healthcare operations).
- Where authorization was **not** required for the exceptions listed in the Final Privacy rule (e.g., health oversight activities, public health activities, judicial & administrative procedures, disclosures to coroners & medical examiners, for law enforcement).
- To enforce its own security and privacy policies that implement HIPAA, even if the data needed for enforcement purposes are more detailed than what is required under the Final Privacy rule to be disclosed to patients. (In a “Catch-22” requirement, the Final Privacy rule requires that a patient be allowed to have access to all this detailed data, because the covered entity is logging it for security and privacy enforcement purposes.)

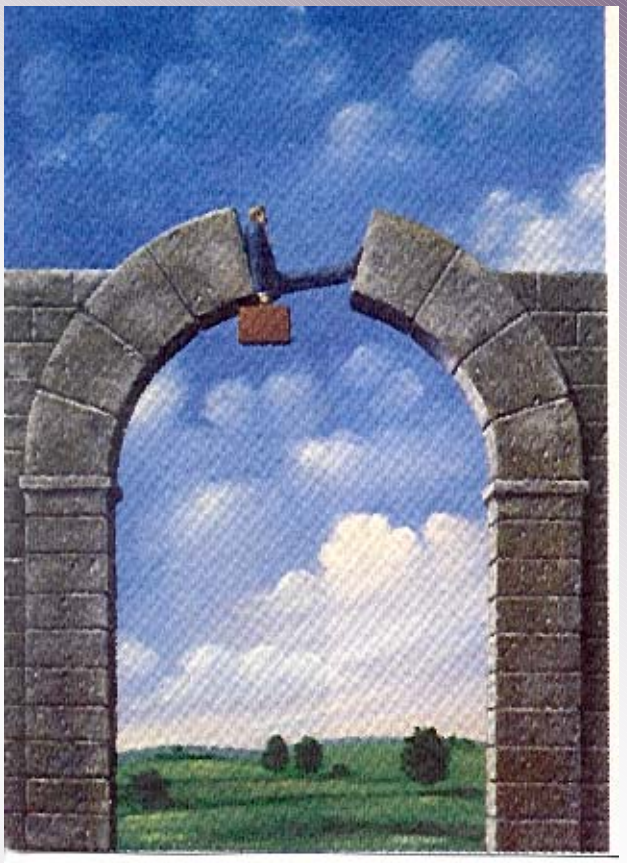
Auditing is a Management Tool That:

- Can be used to "…detect and investigate breaches in security, determine compliance with established policy and operational procedures, and enable the reconstruction of a sequence of events affecting the information." (CPRI);

- Contains identification of the user, data source, particular data viewed person about whom the health information is recorded, provider facility, and other pertinent user if required by statute or regulation or the enterprise's own policies; and

- Provides proof that there was no unauthorized or trivial access to data, if a charge of inappropriate access is leveled at an entity.

Implementation Considerations



Implementation Considerations

1. To what extent are other Technical Security Services mechanisms (e.g., access controls, authorization controls, data authentication, and entity authentication) applied or applicable to the entity?
2. Take into consideration the vulnerabilities of the system on which the data is stored to help determine how stringent the Audit Controls should be.
3. Check for failed data accesses when an authorized system/application user tries to access off-limits data.
4. Checks for “CRUD” accesses (Create, Read, Update or Delete).
5. Frequency of audit trail reviews, and whether it is the sole means to uncover inappropriate access.

Implementation Considerations

6. Different level of audit controls for different types of member-identifiable data being stored, depending on its value and on specific regulatory requirements that, for example, may mandate recording of access by data element or field.
7. Storage of the audit control data being recorded (e.g., On-line vs. Archived; Duration of on-line storage; Enable on-demand retrieval from archive; Duration of archived storage).
8. Authorization & responsibility of person/group reviewing audit trail data.
9. Fit of audit controls and their review with the Security Rule's overall Internal Audit requirement.
10. Audit controls may apply to an application, a system, a network, or any other technical processes; all must be considered.

Implementation Considerations

11. Processes for the audit trail review (e.g., external reviews, internal reviews, random or structured reviews, reviews the responsibility of data owner).
12. Required retention periods for audit trail information may differ by the type of data being stored (builds upon #7 above).
13. With the potential for vast amounts of audit trail data to be reviewed, it may be appropriate to build filters or triggers to prompt review.
14. Should an entity have different processing platforms (e.g., MVS, NT, UNIX, Manual, Windows XX) consideration may be given to developing a common format and ‘data store’ for audit trail data, otherwise multiple filters and reports would be required to review the information.

Implementation Considerations

15. A manual capture of audit trails would be necessary for non-electronic environments.
16. The entity must be able to withstand an audit of its audit trail capture and evaluation process.
17. An audit trail capture and evaluation process should identify who will do the reporting and what reports will be required.
18. The ability to identify disclosure of PHI (Personal Health Information) and capture the 'Who, What, Why, and When' of each disclosure (i.e., the audit trail).
19. The ability to comply with the FIP (Fair Information Practices) requirement to provide information to the patient on who the PHI was disclosed to (i.e., audit trail reporting); to what extent will existing FIP reporting requirements satisfy HIPAA?

Security Issues

1. Determine if the audit controls deemed necessary are available commercially or if they need to be custom-built.
2. Evaluate costs to implement the technical portions of the audit controls you determine are necessary.
3. Evaluate personnel costs to review and act upon the information the audit controls produce.
4. Evaluate hardware costs to store the audit trail data, whether on-line or in archival format.
5. Performance impact to manual or automated processes upon implementation of the audit controls determined to be necessary.

Security Issues

6. Determine commitment to perform periodic evaluations.
7. Determine how these audit controls balance with your company environment and atmosphere.
8. Determine whether, especially in a multi-state environment, there may be other state law issues or guidelines,
9. Identify the current security risks that audit controls and review of audit trails can help close.

Privacy Issues

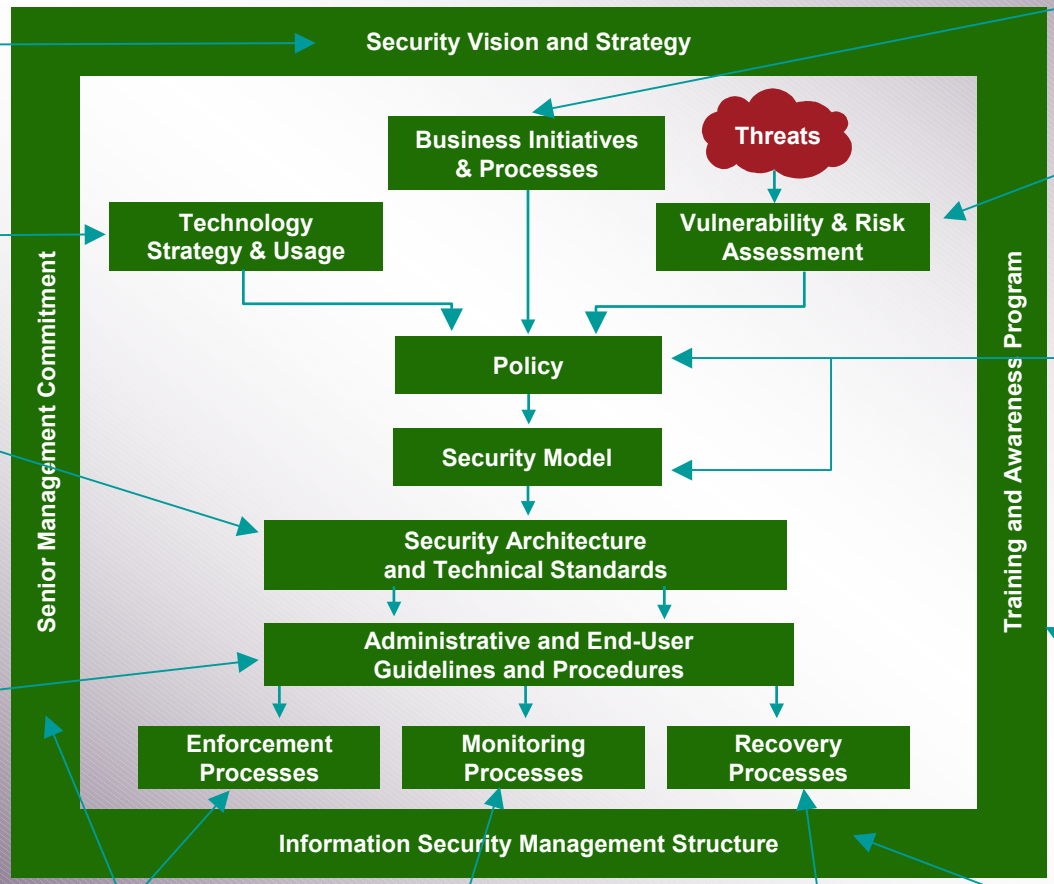
10. Identify the kind of staffing required to address the Fair Information Practices reporting requirements identified in the Final Privacy rule.
11. Identify the frequency of reporting required to address the Fair Information Practices reporting requirements identified in the Final Privacy rule.
12. Identify the process for securing the transmission of and capturing the audit trail information on any FAXED information that contains PHI.
13. Identify the process for capturing the audit trail information for any hand delivery of medical records.

Reasonableness Test

- What is the situation you are trying to correct?
- What are the possible solutions?
- What are the strengths and weakness of each?
- Do they all meet legal and regulatory requirements?
- Of these that do, which solutions can you afford?
- Of these that do, which one offers the best value?
- Formally describe why a particular solution was chosen
- Revisit decisions as often as technology changes
- Specific requirements of the rules trump reasonableness

Good Practice Model

Source: PriceWaterhouse Coopers



Chain of Trust Partner Agreement

Communications/ Network Controls

Authorization Control

Digital Signature

Security Configuration Management

Data Authentication

Entity Authentication

Policy/Guideline on Work Station Use

Secure Work Station Location

Internal Audit

Formal Mechanism for Processing Records

Certification

Information Access Control

Personnel Security

Termination Procedures

Media Controls

Physical Access Controls

Access Control

Training Program

Security Awareness Training

Assigned Security Responsibility

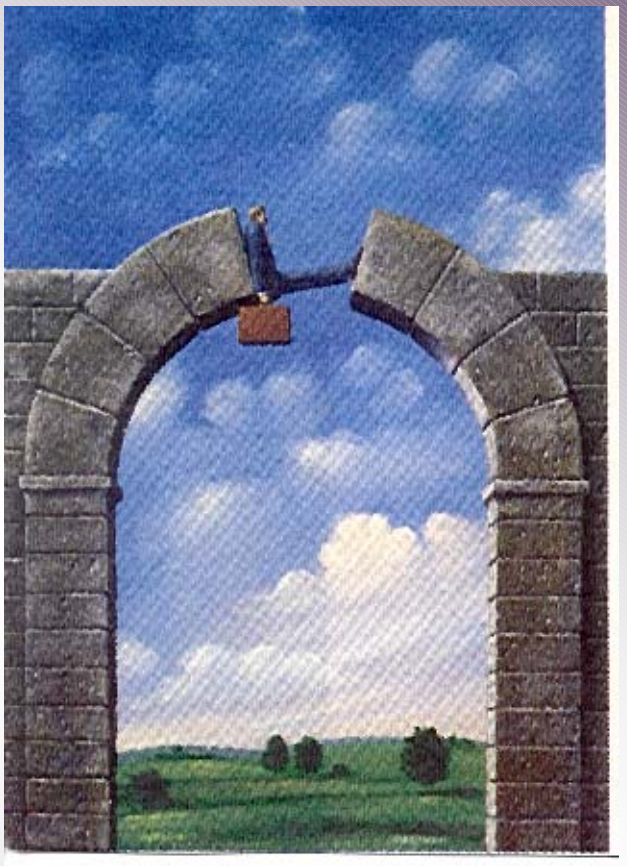
Security Management Process

Audit Control

Security Incident Procedures

Contingency Plan

Our Approach: Develop a Proof of Concept System



Our Three-Dimensional Approach

- A random selection of patients to check for suspicious activity
- A random selection of staff to check for suspicious activity
- Targeted selection of suspicious activity based on expert rules
- We propose to develop one system which meets the FIP and audit requirements

Random Audits

- No expectation of wrongdoing
- The volume of examinations are based on our capacity to review records with available staff
- Medical Records, compliance or internal audit staff may have necessary knowledge to judge appropriateness
- Should become a predictable, periodic activity
- Once examined, candidates disqualified one cycle
- No reliable method of predicting ideal sample size

Random Audit - Patients

- We have 25,000 annual inpatient visits
- We have 500,000 annual outpatient visits
- Allow for 15% duplication
- Total of 450,000 patient record candidates
- Whatever time is available would be used to review as many patient access as possible

Random Audit - Staffing

- We have 6,000 in our workforce
- 2,000 have access to the most sensitive PHI
- Our goal is to annually review each member
- We estimate that a review will require 20-30 min.
- Total annual required hours estimated 666-1000
- Suspicious activity detection will not be timely
- We may have to consider a bi-annual review to reduce the required staff time, or simply review as many as we have time for

Targeted Audits

- Is a user logged-on in more than one location?
- Is a user on vacation, sick leave, etc.?
- Are accesses appropriate for job responsibilities?
- Are physicians accessing records outside their specialty?
- Is record access more than 30 days +/- from DOS
- Is there a suspicious pattern to accesses?
- Is the time/day of the access unexpected?

Targeted Audits

- Include employees that have discipline problems
- A security breach in a particular department may indicate a need for a focussed audit
- All accesses to a high-profile patient's records
- All accesses to workforce members/patients (particularly by those in the same department)
- Include all new employees during first 60 days

Targeted Auditing Staffing

- The more sophisticated your filtering tools, the less staffing will be required
- The more restrictive your expert rules for selection of suspicious activity, the less staffing will be required
- Medical Records, compliance or internal audit staff may have necessary knowledge to judge appropriateness

Implementation Suggestions

- Define access needs for each position
- Identify the sensitivity of each access
- Require annual re-certification for access
- Use systems that effectively limit accesses
- Use systems that effectively log accesses
- Investigate products that centralize security
- Investigate products that centralize access policy development and enforcement

Final Comments

- Remember, the more effective your access controls, the less need for audits
- Audits cannot compensate for poorly designed or implemented access controls
- A consistent, fair and effective audit program will likely survive a challenge of being retaliatory, punitive, harassing, or an attempt to shift or place blame
- Seek legal advice prior to implementation

Resources

AFEHCT security self-evaluation. Includes 15 questions concerning "Monitoring of Access" (i.e., audit). http://www.afehct.org/securityeval.html.
Note: This is not per all compliance items in Proposed Security

Regulation CPRI Security Guidelines ("Toolkit")
http://www.3com.com/healthcare/securitynet/hipaa/4_9_1.html
http://www.cpri-host.org

NCHICA Security Questionnaire (available at a fee) http://www.nchica.org

University Health Care HIPAA Audit Plan https://docs.hsc.missouri.edu
Select HIPAA and scroll down the list for the title
Mike Lynch e-mail: lynchm@health.missouri.edu