Advanced Strategies in HIPAA Security Risk Analysis

Margret Amatayakul, RHIA, CHPS, FHIMSS

Steven S. Lazarus, PhD, FHIMSS
Margret A

Margret\A Consulting, LLC

Strategies for the digital future of healthcare information

- Information management and systems consultant, focusing on electronic health records and their value proposition
- Adjunct faculty, College of St. Scholastica; former positions with CPRI, AHIMA, Univ. of Ill., IEEI
- Active participant in standards development
- Speaker and author (Silver ASHPE Awards for “HIPAA on the Job” column in Journal of AHIMA)
Steve Lazarus

Boundary Information Group

Strategies for workflow, productivity, quality and patient satisfaction improvement through health care information

- Business process consultant focusing on electronic health records, and electronic transactions between organizations
- Former positions with MGMA, University of Denver, Dartmouth College; advisor to national associations
- Active leader in the Workgroup for Electronic Data Interchange (WEDI)
- Speaker and author (two books on HIPAA Security and one forthcoming on electronic health record)

- Strategic IT business process planning
- ROI/benefits realization
- Project management and oversight
- Workflow redesign
- Education and training
- Vendor selection and enhanced use of vendor products
- Facilitate collaborations among organizations to share/exchange health care information
Agenda

- Security Rule in context of HIPAA
- Risk-based Approach to Information Security
- Executive Risk Mitigation Strategies
- Planning and Managing the Project
- Risk Management Approaches
- “Best Practices” for Ongoing Compliance
Advanced Strategies in HIPAA Security Risk Analysis

Security Rule in context of HIPAA
“Mini-Security Rule”

- “Mini-security rule” in Privacy Rule is not sufficient
  - Does not address risk analysis
  - Focuses on incidental disclosures
  - Lacks specificity
  - Efforts may be 2 – 4 years old

- “Mini-security rule” does address the need to “secure” paper and oral forms of PHI
<table>
<thead>
<tr>
<th>Fraud and Abuse</th>
<th>Privacy and Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Written standards of conduct &amp; policies &amp; procedures</td>
<td>1. Privacy &amp; security policies &amp; procedures</td>
</tr>
<tr>
<td>2. Designation of chief compliance officer; reports to CEO &amp; governing body</td>
<td>2. Designation of information privacy official &amp; information security official</td>
</tr>
<tr>
<td>3. Regular, effective education &amp; training for all affected employees</td>
<td>3. Training &amp; awareness building</td>
</tr>
<tr>
<td>4. Process to receive complaints &amp; protect whistleblowers from retaliation</td>
<td>4. Privacy complaint &amp; security incident reporting procedures</td>
</tr>
<tr>
<td>5. System to respond to allegations &amp; the enforcement of disciplinary action</td>
<td>5. Complaint/incident handling &amp; enforcement of sanction policy</td>
</tr>
<tr>
<td>6. Audits &amp;/or other evaluation techniques to monitor compliance</td>
<td>6. Ensure uses &amp; disclosures consistent with notice; information system activity review, risk management, evaluation</td>
</tr>
<tr>
<td>7. Investigation &amp; remediation; policies addressing non-employment or retention of sanctioned individuals</td>
<td>7. Termination procedures for members of workforce &amp; business associate contracts</td>
</tr>
</tbody>
</table>
Security of TCS

- Promote adoption of electronic transactions
- Achieve benefits of “direct connectivity”
- Claims attachments coming
Uniform Data Standards for PMRI

- Recommendations
  - Interoperability
  - Comparability

- EHR Initiatives
  - Uniform data sets
  - Pay-for-performance

- Heightened need for:
  - Contingency planning
  - Access controls
  - Authentication

- Interoperability
  - HL7
  - DICOM
  - NCPDP SCRIPT
  - IEEE 1073

- Comparability
  - SNOMED CT®
  - LOINC
  - Federal Drug Terminologies
Advanced Strategies in HIPAA Security Risk Analysis

Using a Risk-based Approach to Information Security
**YOU decide!**

- **Comprehensive**
  - Must address *all* aspects of security for electronic PHI

- **Scalable**
  - Size, complexity, capabilities
  - Technical infrastructure
  - Costs
  - Probability & criticality of risks

- **Technology-neutral**
  - Stable, but flexible

- **Standards**
  - Require compliance

- **Required & Addressable Implementation Specifications**
  - Implement or document alternative

- **Very specific/very general, e.g.,**
  - Maintenance records
  - Encryption
Benefits of Risk Analysis

- Comply with HIPAA
- Build a business case
- Help executives meet fiduciary duties
- Build staff awareness & support
- Uncover excellent new ideas
- Reduce damages if you are sued
Examples

- Encrypted e-mail
- SSL Web portal
- Reconstruction of examination rooms
- White noise, tranquility, fountains, wall hangings
Risk Analysis Process

Threats + Vulnerabilities = Risk
Targets – Agents - Events

Agent
- Unauthorized Access
- Modification/Destruction of Data
- Denial of Service
- Repudiation

Target
- Confidentiality
- Integrity
- Availability
- Accountability

Event
- Wrongful Disclosure
- Privacy Violation
- Erroneous Information
- Medical Errors
- Lack of Critical Information
- Productivity Recovery Cost
- False Claims
- Lack of Evidence
Threat Sources

- **Accidental Acts**
  - Incidental disclosures
  - Errors and omissions
  - Proximity to risk areas
  - Work stoppage
  - Equipment malfunction

- **Deliberate Acts**
  - Inattention/inaction
  - Misuse/abuse of privileges
  - Fraud
  - Theft/embezzlement
  - Extortion
  - Vandalism
  - Crime

- **Environmental threats**
  - Contamination
  - Fire
  - Flood
  - Weather
  - Power
  - HVAC

What are YOUR concerns?
Internal Threats
Source: eWeek, January 21, 2002

57% - Users accessing resources they are not entitled to
43% - Accounts left open after employee has left company
27% - Access to contractors not terminated upon project completion
21% - Attempted or successful break-in by angry employee

Tangible Losses
- Cost of data recovery
- Lost user productivity
- Investigate/prosecute offenders
- Insurance premium increases
- Fees for contract/regulatory defense
- Cost of fines

Intangible Issues
- Harm to patient
- Lost patient & business partner confidence & loyalty
- Lost reputation, contributing to difficulty in recruitment
- Lower employee morale
- Career-threatening corporate officer liabilities
Vulnerabilities

- Administrative
  - Policy
  - Accountability
  - Management
  - Resources
  - Training
  - Documentation

- Physical
  - Entrance/exit controls
  - Supervision/monitoring
  - Locks, barriers, routes
  - Hardware
  - Property
  - Disposal

- Technical
  - New applications
  - Major modifications
  - Network reconfiguration
  - New hardware
  - Open ports
  - Architecture
  - Controls
Security Vulnerability Tests

- Policy & procedure review
- Workforce perception survey
- Certification/accreditation
- Disaster recovery plan drills
- Social engineering
- Document grinding
- Facility security review
- Communications testing
- Wireless testing
- Backup, maintenance & change control log review
- Internet presence identification & testing
Probability of Occurrence

- Has it happened before?
- How frequently?
- Does threat source have
  - Access, knowledge, motivation?
  - Predictability, forewarning?
  - Known speed of onset, spread, duration?
- Are controls available to
  - Prevent?
  - Deter?
  - Detect?
  - React?
  - Recover?

Criticality of Impact

- Patient care
- Confidentiality
- Complaint/lawsuit
- Reduce productivity
- Loss of revenue
- Cost to remediate
- Licensure/accreditation
- Consumer confidence
- Competitive advantage
## Risk Ranking

<table>
<thead>
<tr>
<th>Probability of Occurrence</th>
<th>Criticality of Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>High</td>
<td>3</td>
</tr>
<tr>
<td>Medium</td>
<td>2</td>
</tr>
<tr>
<td>Low</td>
<td>1</td>
</tr>
</tbody>
</table>
### Example

<table>
<thead>
<tr>
<th>Security Standard</th>
<th>Vulnerabilities</th>
<th>Threats</th>
<th>Probability</th>
<th>Criticality</th>
<th>Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person or entity</td>
<td>Weak password</td>
<td>Shoulder surfing</td>
<td>M</td>
<td>H</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Probability</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>3</td>
</tr>
<tr>
<td>Medium</td>
<td>2</td>
</tr>
<tr>
<td>Low</td>
<td>1</td>
</tr>
</tbody>
</table>

- Low
- Medium
- High
Advanced Strategies in HIPAA Security Risk Analysis

Executive Risk Mitigation Strategies
Foreign hacker stole 4,000 medical records from University of Washington, mid-2000
Kaiser Permanente sent 858 patients’ medical records to 19 before error in e-mail upgrade system was caught, Aug, 2000
A 13-year-old daughter brought to work at University Medical Center, Jacksonville, stole patients’ names and phone numbers and called them saying they either had AIDS or were pregnant, March, 1996
A 17-year-old boy reconfigured physicians’ central paging system at Inova Fairfax Hospital to forward pages to his own pager, & called in prescriptions which nurses administered to patients. Dec, 2000

“It won’t happen here”
Executive Engagement

- Sarbanes-Oxley Act of 2002, PL 107-204, impact on private sector:
  - Management must establish and maintain an adequate internal control structure and procedures for financial reporting.

- “A secure information infrastructure is central to many companies’ operational capabilities. Hence, the material condition of the business will be assessed, and certified by officers, in that light.”
  - Richard Marks, Davis Wright Tremaine, LLP
## Risk Mitigation Options

<table>
<thead>
<tr>
<th>Option</th>
<th>NIST Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assumption</td>
<td>Accept risk &amp; continue operating or implement controls to lower risk to an acceptable level</td>
</tr>
<tr>
<td>Risk Avoidance</td>
<td>Avoid risk by eliminating cause and/or consequence</td>
</tr>
<tr>
<td>Risk Limitation</td>
<td>Limit risk with controls that minimize adverse impact of a threat’s exercising a vulnerability</td>
</tr>
<tr>
<td>Risk Planning</td>
<td>Manage risk by developing a plan that prioritizes, implements, and maintains controls</td>
</tr>
<tr>
<td>Research &amp; Acknowledgement</td>
<td>Lower risk of loss by acknowledging vulnerability &amp; researching controls to correct</td>
</tr>
<tr>
<td>Risk Transference</td>
<td>Transfer risk by using other options to compensate for the loss, such as insurance</td>
</tr>
</tbody>
</table>

Wasn’t this done before?

Assessment
- Identify Vulnerabilities
- Prioritize by:
  - Privacy Rule
  - Importance

Risk Analysis
- Identify Vulnerabilities +
- Identify Threats +
- Measure
  - Probability of Occurrence
  - Criticality of Impact
- Determine Risk =
- Select Controls
- Identify Residual Risk
Business Case Example

- HIPAA doesn’t require a hot site
- What form of DRP should you recommend for this environment?

Top ranking states in terms of number of killer tornadoes:
- Texas
- Oklahoma
- Arkansas
- Alabama
- Mississippi
- Illinois
- Missouri
- Indiana
- Louisiana
- Tennessee
Residual Risk

- Level of risk remaining after controls have been implemented
- No such thing as 100% secure
- Estimate in same manner as original risk determination:
  - Probability of a threat exploiting a vulnerability
  - Criticality of impact
  - Probability plus criticality with control define residual risk
Advanced Strategies in HIPAA Security Risk Analysis

Planning and Managing the Risk Analysis Project
Project vs. Process

- Executive Support
- Objectives
- Scope
- Staffing
- Budget
- Timeline
- Reporting Results
- Obtaining Approval for Controls
- Identifying Residual Risk

- Implementation
  - Staffing
  - External resources
  - Vendor selection
  - Licenses & capital
  - Installation & testing
  - Training
  - Documentation

- Ongoing monitoring for compliance
# Staffing the Project Team

<table>
<thead>
<tr>
<th>Members</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Official</td>
<td>Team Leader, Project Manager, Internal Consultant</td>
</tr>
<tr>
<td>User Representatives</td>
<td>Understand threats, evaluate functionality of controls, gain buy-in</td>
</tr>
<tr>
<td>I.T. Professionals</td>
<td>Identify vulnerabilities, evaluate technical capability, learn administrative controls</td>
</tr>
<tr>
<td>Representatives of Other Areas Monitoring Risk</td>
<td>Probability/criticality estimates, support implementation, represent customers</td>
</tr>
<tr>
<td>HR, Labor Relations, Legal, Contract Management</td>
<td>Represent user interests, assures controls meet other legal requirements</td>
</tr>
<tr>
<td>Trainers</td>
<td>Gain insight for training programs</td>
</tr>
<tr>
<td>Information Privacy Official</td>
<td>Coordinate with Privacy Rule compliance</td>
</tr>
<tr>
<td>Executive Sponsor</td>
<td>Interpret message for executives</td>
</tr>
</tbody>
</table>
# Budget & Timeline

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff</td>
<td>$</td>
</tr>
<tr>
<td>External resources</td>
<td>$</td>
</tr>
<tr>
<td>Learning &amp; benchmarking resources</td>
<td>$</td>
</tr>
<tr>
<td>Software tools</td>
<td>$</td>
</tr>
<tr>
<td>Assessment tools &amp; services</td>
<td>$</td>
</tr>
<tr>
<td>Resource office</td>
<td>$</td>
</tr>
</tbody>
</table>
## Results & Approval

### Microsoft Excel - Risk Analysis Tool

<table>
<thead>
<tr>
<th>Security Standard</th>
<th>Vulnerabilities</th>
<th>Threats</th>
<th>Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy, Procedure, Form</td>
<td>Process/Control, Vulnerability</td>
<td>Threats</td>
<td>Action</td>
</tr>
<tr>
<td>Resources</td>
<td>Approved</td>
<td>Responsible</td>
<td>Start/End Dates</td>
</tr>
</tbody>
</table>

### HIPAA Security Risk Analysis and Risk Management Documentation Checklist

1. Security Management Process §164.308(a)(1)
   - 1.1 Risk Analysis (R)
   - 1.2 Risk Management (R)
   - 1.3 Sanction Policy (R)
   - 1.4 Information System Activity Review (R)

2. Assigned Security Responsibility §164.308(a)(2)

3. Workforce Security §164.308(a)(3)
   - 3.1 Authorization and/or Supervision (A)
Advanced Strategies in HIPAA Security Risk Analysis

Risk Management Approaches
Risk Analysis Approaches

- **Qualitative**
  - Scenario-based
  - Rating probability and criticality and ranking risk
  - Integrates administrative, physical, and technical factors

- **Quantitative**
  - Attempts to determine annualized loss expectancy from value of information assets
  - Difficult to assign monetary value to health care information
Quantitative Analysis

☐ Annualized Loss Expectancy (ALE):
  ■ Asset value, times
  ■ % of asset loss caused by threat, times
  ■ Frequency of threat occurrence in a year

☐ Cost of Safeguard:
  ■ Purchase, development, and/or licensing costs
  ■ Physical installation costs; disruption to normal productivity during installation and testing
  ■ Normal operating costs, resource allocation, and maintenance/repair costs

☐ Cost of Safeguard vs. ALE:
  ■ Positive, recommend remediation
  ■ Negative, consider other alternatives
Steps to Conduct the Process

1. Executive management guidance on risk
2. Inventory & characterize policies, procedures, processes, physical layout, systems
3. Identify threats
4. Identify vulnerabilities
5. Determine likelihood risks may actually occur
6. Analyze impact if risk actually occurs
7. Determine & rate each risk
8. Analyze appropriate types of controls
9. Recommend controls & describe residual risk
10. Document results
## Practical Assessment

**Find Lowest Common Denominator**

<table>
<thead>
<tr>
<th>Administrative</th>
<th>Corporate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Site/Department</td>
</tr>
<tr>
<td>Technical</td>
<td>Application</td>
</tr>
<tr>
<td></td>
<td>Data Center</td>
</tr>
<tr>
<td></td>
<td>Network</td>
</tr>
<tr>
<td></td>
<td>Platform</td>
</tr>
</tbody>
</table>
## Pair Threats & Vulnerabilities

<table>
<thead>
<tr>
<th>Workstation</th>
<th>Location</th>
<th>Vulnerability/Threat Analysis</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop</td>
<td>Nursing units</td>
<td>Staff only area, staffed continuously, all workstations turned away from public, high need for availability</td>
<td>Screen saver only</td>
</tr>
<tr>
<td>Desktop</td>
<td>Outpatient reception area</td>
<td>Public area, not staffed continuously</td>
<td>User log off on exit reminder &amp; automatic logoff set at 10 min.</td>
</tr>
<tr>
<td>Notebook</td>
<td>Exam room</td>
<td>Integrity issue, rotation of users need accountability</td>
<td>User log off on exit</td>
</tr>
</tbody>
</table>
## Security Architecture

<table>
<thead>
<tr>
<th>Security service</th>
<th>Function to be accomplished</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security mechanism</td>
<td>Control that provides security function</td>
</tr>
<tr>
<td>Security architecture</td>
<td>Structure of controls to achieve functions</td>
</tr>
</tbody>
</table>

Diagram:
- Perimeter
- Network
- Host
- Application
- Data
Advanced Strategies in HIPAA Security Risk Analysis

“Best Practices” for Ongoing Compliance
“Best Practices”

- Most effective and efficient
- “Most appropriate”
- What a prudent person would do
- Whether or not specified in regulations
- Not...

- Most expensive
- Expected to fill every gap
- Necessarily common in industry
Proposed Security Rule

☐ Access controls
☐ Alarms
☐ Audit trail
☐ Encryption
☐ Entity authentication
☐ Event reporting
☐ Integrity controls
☐ Message authentication

Included in YOUR vendor offerings?
Security
Identity Management

Access Management Software

Password Reset

Biometrics

Password Synchronization

Single Sign-on

Tokens & Smart Cards

Copyright © 2004, Margret\A Consulting, LLC and Boundary Information Group
Local LAN

Corporate WAN

Internet Gateway

Proprietary Connectivity

Supporting Systems

Security Event Management
### Minimum Necessary

<table>
<thead>
<tr>
<th>Classes of Users</th>
<th>User-based</th>
<th>To each user</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role-based</td>
<td>Role-based</td>
<td>To classes of users to categories of PHI</td>
</tr>
<tr>
<td>Context-based</td>
<td>Context-based</td>
<td>Based on conditions</td>
</tr>
</tbody>
</table>

### Access Control

<table>
<thead>
<tr>
<th>Conditions of Access</th>
<th>Assigns Privileges</th>
</tr>
</thead>
</table>

**But, if there is no treatment relationship...**

**Break glass in event of fire**
Compliance

- Policies
- Standards
- Procedures
- Specifications
- Reports & logs

Extent to which IT security decisions were guided by policy

Documentation

1. Rules & Regulations
   Policies & Procedures
   Training Materials

2. Records: of Training
   Awareness Building

3. Contracts

4. Sensitive Findings
   Audit Trails
   Incident Reports
Compliance Assurance

HIPAA Standards & Organizational Controls

Implement

Design & Test Changes

Analyze

Continuous Monitoring of Actions

Auditing of Events

Triggered Reviews of Incidents

Management Reporting & Documentation
Compliance Assurance Plan

<table>
<thead>
<tr>
<th>HIPAA Privacy and Security Compliance Assurance Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of Plan:</td>
</tr>
<tr>
<td>Compliance Goal:</td>
</tr>
<tr>
<td>Standard(s):</td>
</tr>
<tr>
<td>Owner(s):</td>
</tr>
<tr>
<td>Risk:</td>
</tr>
<tr>
<td>Current Control(s):</td>
</tr>
<tr>
<td>Compliance Process(es):</td>
</tr>
<tr>
<td>Schedule:</td>
</tr>
<tr>
<td>Resources:</td>
</tr>
<tr>
<td>Results:</td>
</tr>
<tr>
<td>Recommendations:</td>
</tr>
<tr>
<td>Follow up:</td>
</tr>
</tbody>
</table>
Required specifications and prioritization based on:
- National Research Council, *For the Record: Protecting Electronic Health Information*
- www.nap.edu

Significant reference to NIST Special Publications (SP) 800 Series documents:

NIST certifying activities:

CMS IT Security –
http://cms.hhs.gov/it/security/References

WEDI – www.wedi.org/snip

SP 800-30, Risk Management Guide for Information Technology Systems, Chapters 3 and 4
- Revision A DRAFT, Jan. 21, 2004

SP 800-16, Information Technology Security Training Requirements, A role and performance based model

SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems

SP 800-33, Underlying Technical Models for Information Technology Security

SP 800-26, Security Self-Assessment Guide for Information Technology Systems

CMS Information Security Acceptable Risk Safeguards V1.1
References & Resources

www.brownstone.com
- Amatayakul
- Lazarus

www.hcpro.com
- Amatayakul

https://catalog.ama-assn.org
- Amatayakul
- Lazarus
- Walsh
- Hartley
Contact Information

- Margret Amatayakul, RHIA, CHPS, FHIMSS
  Margret\A Consulting, LLC
  Schaumburg, IL
  MargretCPR@aol.com
  www.margret-a.com

- Steven S. Lazarus, PhD, FHIMSS
  Boundary Information Group
  Denver, CO
  SSLazarus@aol.com
  www.boundary.net