HIPAA SECURITY
Implementation

HIPAA Security Step-By-Step:
A Consensus of Experts
Session 5.04 – 3/9/2004

Presented by:

Robert Happy Grenert, GSEC
Project Leader and co-author, SANS Instructor

Director of Information Systems, HIPAA Security Officer
Mt. Graham Regional Medical Center, Safford, Arizona

Preface

- Motivation for writing the guide
- Objectives and expected results
- Format of the book

Introduction

- What, Who, How, Why and When of HIPAA Security
- Guiding Principles
- Key Concepts
- General Requirements and Structure

Chapter 1 "HIPAA Past, Present and Future"

- A background of the regulation
- Why HIPAA Security is good for everyone
- Includes how HIPAA has progressed from the preliminary regulations until the final regulations were released

Chapter 2 "HIPAA in Plain English"

- HIPAA From 20,000 Feet
- Title II Administration Simplification
- "Three Rules to Secure Them"
- HIPAA Security Rule
- Covered Entities
- Guiding Principals

Chapter 3 "Security Standards"

- Standards vs. Implementation Specifications
- Total of 18 Standards
- 12 Standards with Implementation Specifications
- Reasonable and Appropriate

Administrative Safeguards - 1 of 2

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information Systems Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)		(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)

Administrative Safeguards - 2 of 2

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	
Security Awareness and Training	164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedure	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)		(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement	(R)

Physical Safeguards

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	
Facility Access Controls	164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Controls and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	164.310(b)		(R)
Workstation Security	164.310(c)		(R)
Device and Media Controls	164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data backup and storage	(A)

Technical Safeguards

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	
Access Controls	164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	164.312(b)		(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	164.312(d)		(R)
Transmission Security	164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

Chapter 4 "Overlaps Between Privacy and Security Rules"

- Reviews overlapping points of the Privacy and Security rules
- Where and how they intersect
- Analyzes mutual dependencies

Chapter 4 "Overlaps Between Privacy and Security Rules"

- Overlaps & Interdependencies
- Training & Awareness
- Detailed Requirements
- Appropriate and Reasonable Safeguards

Chapter 5 "Compliance and Enforcement"

- Civil Penalties
- Criminal Penalties
- Unintended Penalties
- Enforcement Jurisdiction
- Enforcement Rule
- Enforcement Process
- Self-Discovery
- Informal Complaint
- Formal Complaint

Chapter 5 "Compliance and Enforcement"

- Incidental versus Systemic
- Compliance Process
- Internal Controls and Audits
- External Audit
- Certification and Accreditation
- Document, Document, Document

Chapter 6 "Gap Analysis"

- Long and involved chapter in the SBS Guide that describes a project methodology for conducting a gap analysis, including:
  - Information audit and assessment
  - Establishing your approach
  - Background interviews, data collection
  - Review of policies and procedures
  - Security review matrix and checklist for determining responsibilities
  - Reporting and analysis thoughts

Chapter 6 "Gap Analysis"

- Diagnose your gaps & decide how to treat/remediate
- Starts with information audit:
  - Documents where you are today from perspectives of people, policies, and procedures
  - Provides direction and establishes complexity of problem
- Primary focus is to evaluate where you are relative to the HIPAA security regulation
  - Provides groundwork for HIPAA mandated risk analysis
  - Not the final risk analysis
- Feeds directly into remediation efforts
  - Organize and present information and data logically in a format that translates to CE's project planning and budget process

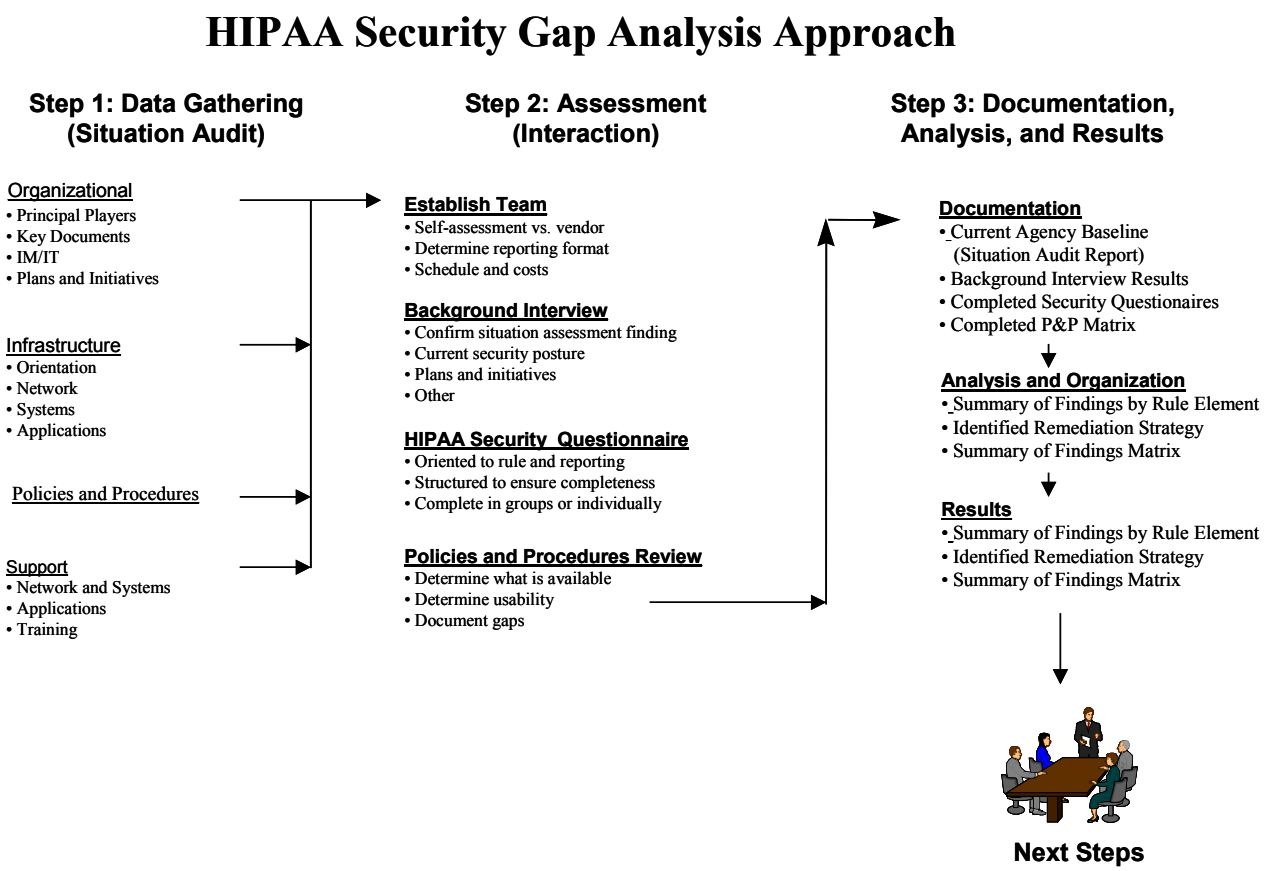
Chapter 6 "Gap Analysis" Organization

- Part One: Project Methodology
  - Document History & Current State of CE
  - Review Policies and Procedures
  - Review Security Specific Elements with Workforce
- Part Two: Analysis and Reporting
  - Determine content & presentation guidelines
  - Force cohesive statement of gaps to help develop implementation plan and resource budget
  - Establish the foundation for information security management within the CE, increasing more critical with the increasing use of medical system automation

Chapter 6 "Gap Analysis" A Word About Consultants

- Self-assessment can work well if you are honest with yourself
- If you outsource to a specialist, review this section and use it as a basis for assessing the study results for which you have contracted
- Firmly establish the scope and boundaries of the HIPAA gap analysis with the consultant!
- Don't pay for additional services you don't need or want!

Chapter 6 "Gap Analysis"
HIPAA Security Gap Analysis Approach



Chapter 6 "Gap Analysis" Step One: Information Audit

- Gather as much data as possible related to security!
  - Information management and technology
  - Processes and procedures
- Goals are to:
  - Establish a summary of your automation systems
  - Document how electronic information is used (including PHI)
  - Understand how CE's security posture is related to your business processes and needs
- Try to complete before Step 2
  - Determine completeness of CE's thought and documentation processes
  - Use results as guide for the development of the tools for Step Two – Questionnaires

Chapter 6 "Gap Analysis"
Step One: Information Audit Checklist Examples

Category	Possible Document Formats
Organizational →	• Organizational Charts • Job Descriptions • Catalog of Documents/Data Sources
• Identify Principal Players • Capture Key Documents • Function of IM Group in CE	
Infrastructure →	• VISIO or graphic diagrams • Tabular information
• Network Orientation • Locations of EPHI & Data Flows • Access Points	• Indexed Documents
Policies and Procedures →	
Support Structure Delivery to End Users →	• System Administration Manuals • Training Schedules/Lesson Plans • Security Orientation/Awareness Materials

Chapter 6 "Gap Analysis" Step Two: Assessment (4 Parts)

1. Establish your approach
   - How can you validate the information gathered in Step 1?
   - What is the scope and direction of your effort?
   - Should we do a self assessment?
   - Have you committed resources to do the gap analysis?
   - How should the results be organized and presented to be the most useful?
   - How should the project be managed?
2. Background Interviews with Key Stakeholders
   - Objective: Validate assumptions, confirm information gathered in Step One, and draw out responses to potential corporate issues involving security
   - Guided but not necessarily form driven
   - Allocate at least 30 minutes per interview
   - Plan on a team of two per interview (Discussion leader and note taker)

Chapter 6 "Gap Analysis" Step Two: Assessment (Cont.)

3. Develop Data Collection Questionnaire
   - Structured tool, organized relative to the structure of the rule
   - Options are to build your own, buy (and tailor) or use the one provided by your consultant
     - Make sure the consultant addresses all your issues
4. Review of Policies and Procedures (P&Ps)
   - Policy and Procedure Checklist
   - Survey Organizational P&Ps
   - Summarize and Evaluate Existing P&Ps

Chapter 6 "Gap Analysis"
Step Three: Documentation, Analysis & Results

- Deliverables include:
  - Summary of the information collected during Step One
    - Organize content to find and update this information
    - Creation of a valuable reference for the organization
  - Completed set of background interviews
    - Organize by date, interviewee and topic
  - Compiled results from HIPPA Security Assessment questionnaire and P&P review
    - Create a master version upon which you can analysis and results
    - Results should reflect lowest common denominators across organization
    - Important differences between sites should be acknowledged
  - Analysis Report
    - Summarize gaps relative to each part of the rule
    - Summary matrix that presents overall compliance of CE with HIPAA and areas where remediation is needed

Chapter 6 "Gap Analysis"
Step Three: Results- Sample Presentation

Table 1: Remediation Findings/Work Breakdown Structure Elements Relative to HIPAA Security Rule

Gap Analysis / Remediation Categories WBS Element			Security Management Program (WBS 1.0)	Business Continuity & Disaster Recovery (WBS 2.0)	Policies and Procedure (WBS 3.0)	Human Resources Procedures (WBS 4.0)	Business Associate Agreements (WBS 5.0)	Training / Awareness (WBS 6.0)	Technical Architecture (WBS 7.0)	Evaluation (WBS 8.0)	System /Network Management (WBS 9.0)	User Management (WBS 10.0)
Rule/Section		**Gap**										
Administrative Safeguards												
164.308(a)(1)	Security Management Process	◗	✓		✓					✓	✓	
164.308(a)(2)	Assigned Security Responsibility	●										
164.308(a)(3)	Workforce Security	◗			✓	✓						
164.308(a)(4)	Information Access Management	◗							✓		✓	✓
164.308(a)(5)	Security Awareness and Training	◗				✓		✓				✓
164.308(a)(6)	Security Incident Procedures	○	✓		✓			✓				✓
164.308(a)(7)	Contingency Plan	◗	✓	✓							✓	
164.308 (a)(8)	Evaluation	○							✓	✓	✓	
164.308 (b)(1)	Business Associates Contracts	◗					✓					
Physical Safeguards												
164.310(a)	Facility Access Control	◗		✓								
164.310(b)	Workstation Use	◗			✓							
164.310(c)	Workstation Security	◗			✓			✓			✓	
164.310(d)	Device and Media Controls	◗	✓	✓	✓						✓	
Technical Safeguards												
164.312(a)	Access Controls	◗							✓		✓	✓
164.312(b)	Audit Controls	○									✓	✓
164.312(c)	Integrity	●										
164.312(d)	Person or Entity Authentication	◗			✓				✓		✓	
164.312(e)	Transmission Security	◗								✓	✓	
Organizational Requirements												
164.314(a)	Business Associate Contracts or Other Agreements	◗					✓					
164.314(b)	Requirements for Group Health Plans	**N/A**										
Policies and Procedures and Documentation Requirements												
164.316		◗	✓						✓		✓	

○ = No Compliance, ◗ = Partial Compliance, ● = Full Compliance, **N/A** = Not Applicable

Chapter 7 "Justification"

- Describes how project managers, executives, security engineers, and other IT people can justify the cost of a HIPAA project to their executive management team

Chapter 7 "Justification"

- Presentation
  - Executive summary
  - Problem statement
  - Identify existing infrastructure
  - Identify your recommendations
  - Provide alternatives
  - Cost/Benefit analysis
  - Project Plan
  - Executive Summary

Chapter 8 "Developing the Project Plan"

- Define your company's role pertaining to HIPAA
- Rules to work by
- Defining the goals
- Identifying the existing tools
- Identifying the cost of doing nothing

Chapter 8 "Developing the Project Plan"

- Possible Phases of a Compliance Project:
  - Project Plan roadmap
  - System Discovery and identification
  - Baseline existing systems
  - Gap, Risk analysis, management, acceptance
  - Remediation
  - Review and follow-up

Chapter 9 "Budgeting the Plan"

- Step 1: Conduct a Risk Assessment
- Step 2: Engage Business Units
- Step 3: Understand Financial Data
- Step 4: Personnel vs. Non-Personnel Costs
- Step 5: Determining TCO
- Step 6: Return-on-Investment
- Step 7: Writing the Budget Proposal

Chapter 9 "Budgeting the Plan" Summary

Key elements of successfully obtaining funding:

- Assess current state of security with Gap Assessment
- Align the plan with your organization's strategic direction and day-to-day operations
- Articulate the merits of the plan on the basis of business need
- Model the proposal after previously successful funding proposals
- Obtain buy-in from Management and Business Units that HIPAA compliance will actually provide quality improvement for the organization

Chapter 10 "Risk Analysis and Risk Management"

- Types of Risk
- Scope the Subject of the Threat
- Closer Look – Qualitative Risk Analysis
- Closer Look – Quantitative Risk Analysis
- Enforcing Safeguards with Policies
- Risk Options

Chapter 10 "Risk Analysis and Risk Management"

- Step-By-Step Summary
  - Read background info
  - Select a methodology
  - Scope assets, missions, security objects
  - Work through the analysis methodology
  - Balance the impact of threats with potential safeguards
  - Select safeguards and implement them
  - Document all findings

Chapter 11 "Administrative Safeguards and Documentation"

- Based on the scheduled activities in the project plan
- Outcome of risk analysis step
- Enumerates and explains steps
- Points out how the addressable requirements should be dealt with

Administrative Safeguards - 1 of 2

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	
Security Management Process	164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information Systems Activity Review	(R)
Assigned Security Responsibility	164.308(a)(2)		(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)

Administrative Safeguards - 2 of 2

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable	
Security Awareness and Training	164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedure	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	164.308(a)(8)		(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement	(R)

Chapter 11 "Administrative Safeguards and Documentation"

- Security Incident Procedures
  - single I.S., Response and Reporting, which is a *required* standard
  - This writer recommends a 6 step Incident Handling process:
    - Preparation
    - Identification
    - Containment
    - Eradication
    - Recovery
    - Lessons learned

Chapter 12 "Physical Safeguards" Overview

- Facility Access Control – Policy + Procedure
  - Contingency Operations (A) - Procedure
  - Facility Security Plan (A) – Policy + Procedure
  - Access Control and Validation Procedures (A) - Procedure
  - Maintenance Record (A) – Policy + Procedure
- Workstation Use – Policy + Procedure
- Workstation Security – Physical Safeguards
- Device and Media Controls – Policy + Procedure
  - Disposal (R) – Policy + Procedure
  - Media Re-use (R) - Procedure
  - Accountability (A) – Record of Movement
  - Data Backup and Storage (A) – Copy before Move

Chapter 12 "Physical Safeguards" Facility Access Control – Maintenance Record (A)

- Define what facility repairs pertaining to security (hardware, walls, doors, locks, cable pipe, CCTV, UPS, etc)
- Defines what (keys, access code to alarms, UPS shelf life, etc.) needs to tracked, how (forms, reports, etc) and for how long (6 years?)
- Support for audit, periodical test and event investigations

Chapter 12 "Physical Safeguards" Summary

- Based upon threat, vulnerability and risk
- Integrate with administrative safeguards
- Integrate with technical safeguards

Chapter 13 "Technical Safeguards" Introduction

- Identification
- Authentication
- Authorization
- Emergency Access
- Automatic Logoff
- Encryption
- Auditing
- Integrity
- Data Transmission
- Perimeter Security

Chapter 13 "Technical Safeguards" User Identification: Who are you?

- Uniqueness
- Non-repudiation
- Identification technologies
- Hardening against attack
- Account aging

Chapter 13 "Technical Safeguards" User Authentication: Prove it!

- What you know
- Who you are
- What you have

Chapter 13 "Technical Safeguards" Emergency Access:

Which comes first: Patient health or application security?

- Identification and authentication
- Audit
- Disaster recovery

Chapter 13 "Technical Safeguards" Automatic logoff: Is that still you?

- Idle time
- Passive authentication
- Other technologies

Chapter 13 "Technical Safeguards" Auditing: Who, what and when?

- What is logged?
- How and when is it audited?
- How long is it kept?

Chapter 13 "Technical Safeguards" Perimeter Security: Only as strong as the weakest link

- Firewall
- Antivirus
- Network Intrusion Prevention
- Host Intrusion Prevention
- VPN
- Vulnerability Assessments

Part V

- **Post-Implementation Issues**

- Chapter 14 – "HIPAA Audit"
- Chapter 15 – "Ongoing Compliance: Maintaining Security Best Practices for the Future"
- Glossary
- Appendices

Chapter 14 "HIPAA Audit"

- Preparing for the Audit
  - Goal of the Audit or Evaluation
  - Gathering Manuals, Policies, Documentation
  - Determining Need for Audit Committee
  - Risk Analysis
  - Documents Need (**extensive list!**)

Chapter 14 "HIPAA Audit"

- The Audit Process
  - Interviewing the Staff
  - Determining Time of Day, Testing Methods, Limitation of Effect on Production Systems
  - Arrange for Site visits
  - Ensure they have Indemnification Statement
  - Inventory of Systems, Physical Location

Chapter 14 "HIPAA Audit"

- The Audit Process - continued
  - List of Software
  - Network Topology
  - Operating Systems
  - Review Written Policies, Prepare Recommended Changes
  - Review of Past Incident Reports

Chapter 14 "HIPAA Audit"

- The Audit Process - continued
  - Review and Inspection of Training Procedures
  - Use of tools during Audit Process – Comparison to Industry Best Practices
  - Interview Staff – Determine understanding of Policies & Procedures
  - Interview CIO, Sys Admin, Security Director, HIM, Legal/Counsel

Chapter 14 "HIPAA Audit"

- Concluding the Audit
  - The Exit Interview
  - Review the Delivered Report
  - Perform Remedial Action
  - Document Actions Taken

Chapter 15 "Ongoing Compliance" Presentation Objectives

In this chapter you will discover how to develop an effective:

1. Security policy
2. Information Security Management Organization
3. Security Development Lifecycle
4. Methodology for Ensuring Controls are Operating Correctly
5. Vulnerability Management Program
6. Enterprise Patch Management Procedures
7. Security Incidents Management Program
8. Disaster Recover Plan

Chapter 15 "Ongoing Compliance"
Introduction to Maintaining Compliance

- Maintaining best security practices appears in section 164.308 (a) (1) (B) of HIPAA
- Involves managing risk discovered in the risk assessment and analysis section of compliance efforts, and ensuring gaps remain closed between security state and HIPAA compliance
- Best practice is to use globally accepted standards such as ISO 17799 and NIST as the basis for a risk management program and to ensure defensibility

Chapter 15 "Ongoing Compliance"
Enterprise Patch Management

Strategies for effective patch management:

1) Patches
2) Hot fixes
3) Service/Feature Packs

- Assessing for required updates
- Testing and evaluation
- Installing updates

Chapter 15 "Ongoing Compliance" Summary

An effective risk management strategy is:

- A substantial undertaking for all organizations
- Affects virtually every part of an organization
- Carefully coordinated, adequately resourced and sustained
- A means to reduce costs through user training, smooth transitions, reduced risk exposure and more effective handling of security incidents
- Based upon globally recognized standards such as NIST and ISO 17799.

Glossary, Appendix A & B

- List of HIPAA and Security terminology
- A timeline history of the HIPAA Security Rule
- HIPAA sections found in the U.S. Code and Code of Federal Regulations

Appendix C

- "Recommended Hardware Configurations"
  - Routers
  - Firewalls
  - VPN
  - Windows-based Web Servers
  - Windows-based Mail Servers
  - Wireless Access Points
  - Modems

HIPAA SECURITY
Implementation

- Q & A