



So You Have Your Assessment

What Now?

February 2003

Presented By: Nelly P. Romero



Panic!!!

Questions

- **How many did a Privacy Assessment?**
- **Did it include Security?**
- **Who is going to do a Security Assessment or review?**

Agenda

- **Privacy and Security**
- **Assessment Process**
- **Implementation**
- **DMAS Examples**

Privacy and Security

Joined at the HIPAA

- Reasonable Safeguards
 - Take reasonable measures to protect PHI
- Protecting Data
 - Policies, procedures, and security technology
- Mapping Protected Health Information Data
 - Where is the data and who has it?
- Access Control - Security states use 1 of 4
 - User based
 - Context based
 - Role based - Required in privacy
 - Encryption

Privacy and Security

Joined at the HIPAA - continued

- Accountability
 - Assign person or group responsibility of oversight
- Third-party Agreements
 - Required in both rules
- Training and Awareness
 - Require training of cover entity's workforce
- What Else?
 - Final Security Rule will tell

What Should an Assessment Accomplish?

- It Should Answer - What is the Current State of the Organization's Compliance with HIPAA?
- It Should Assist the Organization in:
 - Identifying and managing risks associated compliance
 - Preparing the organization to make the best compliance related decisions based upon their unique risks
 - Beginning the foundation of documentation for ongoing reviews
- Identify the Major Risks
- Identify Areas that Require Improvement

Deliverables, Assumptions, and Schedule

- Assessment In / Exit Briefing
- Assessment Report
- Management and Staff Participation
- Access to Documentation
- Interface for Organization and Assessment Team
- Periodic Statuses - Sanity Checks
- Clear Understanding of Schedule and Process

Process

- Assessment Can Involve
 - Interviews, Questionnaires, and/or Checklists
 - Documentation Review
- Identify Staff to Participate in Assessment
- Set Scheduling
- Analysis Output to Determine Risk / Gaps
- Prioritize Risks and Document
 - Green, Yellow, Red
 - 1 - 5
 - Impact and Probability
- Formulate Conclusions

What Has Changed?

- Identify What has Changed
 - Within Organization
 - New State Standards (Virginia)
 - HIPAA Security Rule
- Re-evaluate Risks / Gaps
- Prioritize
- Update Documentation

Focus

- **Document the Current State of the Organization's HIPAA Compliance Resulting in:**
 - A Living Document
 - A Benchmark for Improvement
 - A Foundation for Security Implementation Plan

Implementation Work Plan

- CONTROLS
 - Process Improvement
 - High Level Schedule
 - Cost Capture by Module Business vs. Expenses
 - Reporting Project and Risk
 - Oversight
 - Awareness
 - Demonstrated Compliance

Implementation Work Plan

(Continued)

- DELIVERABLES
 - Schedules
 - Policies and Procedures
 - Audit Controls
 - Training and Awareness
 - ROI Cost Accounting
 - Monitoring Tool
 - Compliance / Documentation Manuals

Implementation Plan and Structure

- Based on the Areas Assessed
- Based on (Proposed) Security Rule and Compliance
- Based on State Standards Guidelines
- Module Structure of Control
 - Security Officer
 - Program Implementation and Controls
 - Risk / Gaps Remediation
 - Policy and Procedure (Governance and Operations)
 - Communications Plan

Implementation Plan and Structure

(CONTINUED)

- Awareness and Training
- Data Usage and Disclosure
- Facilities and Physical Safeguards
- Risk Management and Controls
- Security
 - » Electronic networks, Internet, EDI
- Contingency Planning
- Project Schedule: By Module and Deliverable
- Quality Assurance
- Best Practices
- Performance Improvement

Standard Process Format

- Module Number (cost center)
- Milestone Description
- Description of Compliance Condition
- Implementation Activity (results in deliverable)
- Activity Owner

Standard Process Format

(Continued)

- Earliest Start Date
- Latest Completion Date
- Status-Issues-Comments
- Budget vs. Actual

Project Management Controls

- Cost Accounting
- Project Reporting
- Project Scheduling
- Data Aggregation Comparisons
- Benchmarking

Examples

- Commonwealth of Virginia's Department of Medical Assistance Services
 - Operational Review - Interview Questions Checklist
 - Plans
 - Policy

Operational Review – Interview Question Checklist

Section 5 45 CFR 142.308(a) Security Standard: Administrative Procedures. This citation addresses the administrative functions of a Covered Entity, which need to be implemented, documented, reviewed and audited periodically. There are 12 administrative requirements, which include contracts, certification, plans, anti-virus, policies and procedures, and training – all of which need to be documented.

<u>Yes</u>	<u>No</u>	<u>N/A</u>	<u>Description</u>
[]	[]	[]	Do you scan any reports containing PHI?
[]	[]	[]	Do you email any PHI – encrypted or not?
[]	[]	[]	Do you use any security software?

Operational Review – Interview Question Checklist

Section 6 45 CFR 142.308(b) Security Standard: Physical Safeguards to Guard Data Integrity, Confidentiality, and Availability. This citation addresses the Covered Entity’s requirement for implementation, documentation, review and auditing of physical facility safeguards. There are six security safeguard requirements, including control of electronic media that store PHI, access to the locations where PHI is stored/used, location of PHI work areas and awareness training in PHI security.

<u>Yes</u>	<u>No</u>	<u>N/A</u>	<u>Description</u>
[]	[]	[]	Do you have access to the Printer/File room?
[]	[]	[]	If so, is there a log, locks or other security procedures?
[]	[]	[]	Are reports or documents with PHI shredded after use?
[]	[]	[]	Are reports or documents with PHI locked when not used?
[]	[]	[]	Is there a recycle bin for PHI documents which are discarded?
[]	[]	[]	Are files and cabinets locked after hours?

Operational Review – Interview Question Checklist

Section 7 45 CFR 142.308(c) Security Standard: Technical Security Services to Guard Data Integrity, Confidentiality, and Availability. This citation addresses the required implementation, documentation, review and audit of the technical security functions that protect the covered Entity’s PHI. There are five security service requirements, which include control of access to the PHI by the workforce, authentication of the workforce using the PHI, and auditing functions to ensure integrity and confidentiality of the PHI.

<u>Yes</u>	<u>No</u>	<u>N/A</u>	<u>Description</u>
[]	[]	[]	Do you store PHI files on your PC?
[]	[]	[]	Do you use security services such as virus protection, passwords on files, zipped files, etc.?
[]	[]	[]	Do you access any other systems other than the MMIS (ie: DIT)?
[]	[]	[]	Do you have a laptop or any other device which uses PHI? (Other than your DMAS PC).
[]	[]	[]	Do you use any software/report writing tools (ie: SAS)?

Operational Review – Interview Question Checklist

Section 8 45 CFR 142.308(d) Security Standard: Technical Security Mechanisms to Guard Against Unauthorized Access to Data that is Transmitted over a Communications Network. This citation addresses the required implementation, documentation, review and audit of technical security devices, which protect the Covered Entity’s PHI when it is being transmitted electronically over a communication media. There is one security mechanism requirement (with at least one feature required) and additional features for networks. Features such as encryption, alarms, audits and authentication would be required under this standard.

Yes No N/A Description

 Do you use any security services other than those provided by DMAS?

Plans

- Under 45 CFR 142.308(b) Security Standard: Physical Safeguards to Guard Data Integrity, Confidentiality, and Availability, there is a requirement for data security, business recovery and emergency response plans.
 - Emergency Response Plan
 - » Planning for the continuity of the business of DMAS in the aftermath of a potential disaster.
 - Policy on Emergency Operations and Personnel Protection
 - » It is embodied in the DMAS Business Recovery Plan, Business Continuity and Contingency Plan, Physical Security Plan and physical threat handling procedures and facility evacuation plans and associated procedures.

Policy Format

- Use Template
- Use Standard Numbering System
- Policy Summary
 - What is HIPAA “data security”?
 - Why DMAS needs a HIPAA Data Security Policy?
 - What this HIPAA Data Security Policy means?
- Citations
- Privacy Standard
- Objective
- Coverage
- Policy
- State Law Preemption Review
- Policy Related Definitions



Questions and Answers