September 12, 2004

Simplifying the Administration of HIPAA Security

Angel Hoffman, RN, MSN
Director, Corporate Compliance
University of Pittsburgh Medical Center, Pittsburgh, PA
hoffmanam@upmc.edu

Assigning security responsibility

Work group structure, meetings to identify the requirements of the security rule.

Developing standards and entity or application specific procedures

Business associate agreements

Managing the process:

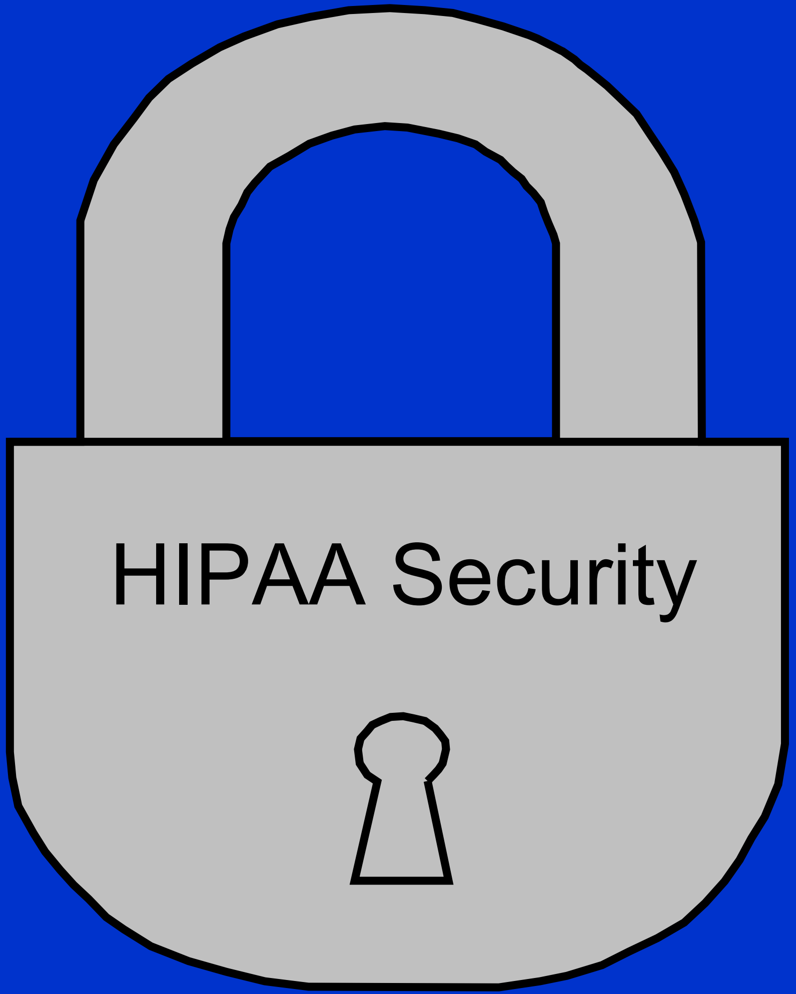
- Holding open forums for education of the security liaisons
- Frequent communications
- Documentation of the process and rationale for decisions

Contingency planning and incident response procedures

How do I get my arms around this?

Feel like a sinking ship???

Implementing A HIPAA Security Compliance Program



Unlocking the secret…

Risk Assessment

- Risk Assessment is identified as an assessment of the potential impact to an organization’s operations and assets.
- In HIPAA Security the risk is the impact of the information on the organization.
- In today’s world of technology, information systems are the life line of the organization.
- Systems communicating to one another while maintaining privacy and data integrity of the information.

So you are not a technology guru…

HIPAA Intersections

We have a head start due to work of HIPAA Privacy workgroups (e.g. Information Security and Privacy Awareness Brochure)

Privacy ↔	Security
Security Awareness & Training	Security Awareness & Training
Business Associate Contracts	Business Associate Contracts
Privacy Officers for All Entities	Security Liaisons for All Entities
Multi-disciplinary Work Groups.	Multi-disciplinary Work Groups

* Remember HIPAA EDI – While maintaining privacy of the information we also need to look at the transactions from a security stand point.

Where to begin…

Key Elements in Identifying Risk:

- Developing a gap analysis
- Risk assessment tool
- Policies
- Education/training
- Common issues –
    - Budgetary Impact
    - Management Support
    - Multiple systems and applications

Creating the Team

Assignments of work group leaders

Developing work group assignments

Creating and revising deliverables

Leadership support

Implementation at the entity or application specific level

Evaluation

Ongoing monitoring and auditing

Access to all information on a share drive

Timeline

Important dates:

- Work groups completed work Spring 2004
- Training available September 7, 2004
- Complete training December 31, 2004
- Complete gap analysis by August 31, 2004
- External review validation and analysis of program begin mid August 2004
- Action plans and documentation due March 1, 2005 (ongoing monitoring)
- HIPAA Security Compliance April 21, 2005

Moving forward with increased experience…Keep in mind these things to consider:

- Size, complexity, and capabilities of your organization
- Cost and practicality
- Potential risk to organization
- Common sense decisions
- IMPACT ON PATIENT CARE

Information Security and Privacy Awareness Brochure

- Viruses
- UPMC Security Related Policies
- Security Violations/Incident Reporting
- Technical Assistance
- Privacy and Confidentiality
- Proper Computer Use
- Internet Use
- Passwords
- E-mail

What else?

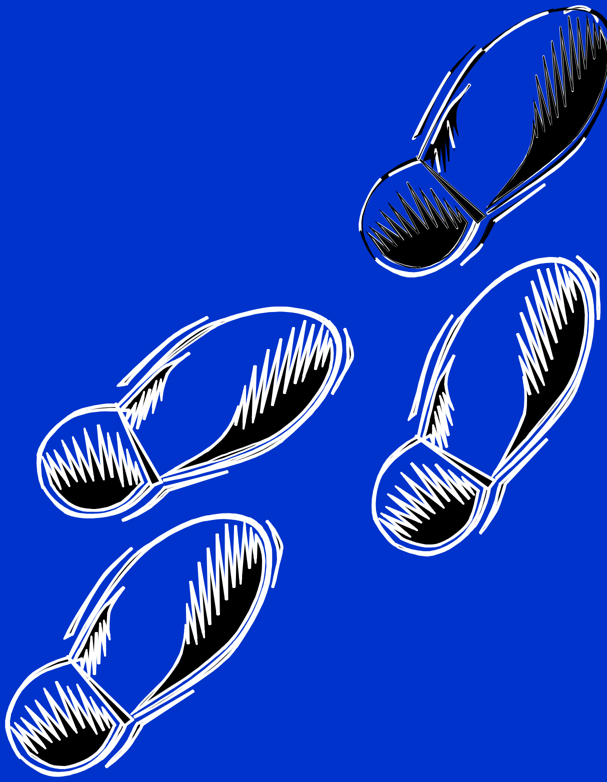
Future challenges:

Protect and guard confidentiality and availability of PHI: verbal, paper and electronic data integrity

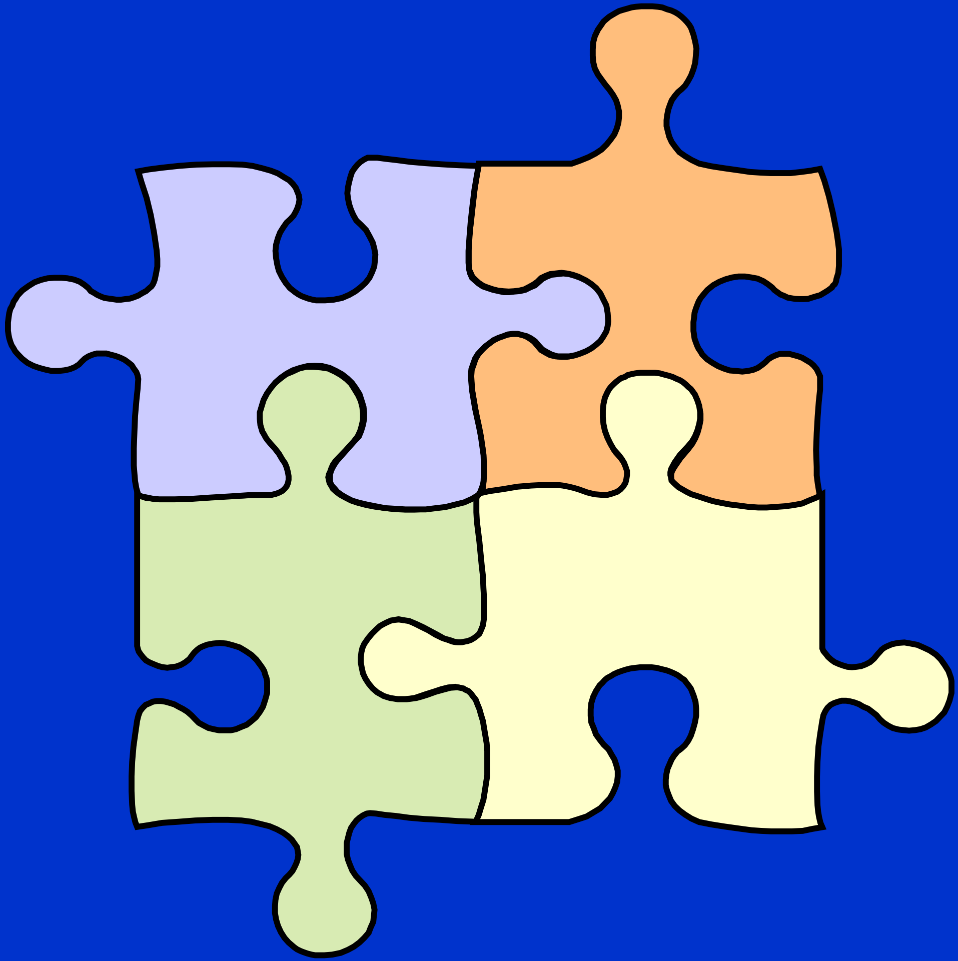
Maintaining knowledge of HIPAA EDI and Security Rule requirements

Maintain documentation and make available for review (6 years for privacy)

Next Steps???



Fitting all of the pieces together…



Virtual Compliance Officer (VCO)

- An Automated Assessment Tool
- Scalable Self-paced Questionnaire
- Provides Gap Analysis
- Generates Recommendations
- Provides an Ongoing Evaluation Monitoring Capability

HIPAA Security Implementation Guide

Provides information for the Security Liaisons to follow as they implement the program

Objectives:

To document the organization's implementation steps for complying with the HIPAA Security Standards

To provide Security Liaisons with guidance on complying with the HIPAA Security Standard.

To provide Security Liaisons with information to complete required responsibilities

Security Liaisons

Establish individuals for each entity

Train these individuals on their responsibilities

Coordinate security risk assessments

Evaluate existing security controls compliance with UPMC policies and standards

Remedy any security control gaps

Conduct ongoing compliance activities and monitoring

Report all required information to the HIPAA Program Office

Assist in addressing security issues

Responsibilities

- Understand subject to comply with HIPAA Security regulations
- Develop action plan to comply with HIPAA Security Standards by April 21, 2005 (internal deadline March 1, 2005)
- Create policies, standards, and procedures to comply with HIPAA Security Standards
- Educate and identify appropriate key stakeholders within business units to HIPAA Security Standard requirements
- Report compliance efforts progress and/or any obstacles and document them
- Maintain the privacy and security of all confidential information.

Security Liaison Job Description

Qualifications:

- Background to technical and administrative processes related to computers, network, applications, physical security and contingency planning
- Ability to work with departments involved with storage, transmission, processing of electronic protected health information within their entity
- Ability to sort priorities, handle situations, solve problems and independently make decisions within timeframes of the HIPAA security regulation
- Working together collaboratively with Corporate Legal Staff, Senior Management, Information Security Group and the HIPAA Program Office at Corporate Compliance

Security Liaison Job Description (cont.)

Responsibilities:

- Working to establish a system-wide oversight committee
- Enabling compliance with UPMC’s security policy, standards and procedures for their entity or computer applications
- Participating or representative identifying an entity representative to participate in workgroups
- Overseeing all HIPAA Security activities for their entity and computer applications
- Identifying opportunities to leverage existing Information Security services and processes that may include minimum security baselines, role base access control, and incident response
- Communicating a clear understanding of the HIPAA regulations and addressing issues as appropriate

HIPAA Security Workgroup Policy and Standard Review

- HIPAA Business Associate Workgroup- developed the language requirements for business associate contracts based upon the HIPAA Security regulations
- HIPAA Clinical Applications Workgroup- developed/modified the policies and standards for application specific security controls, such as audit, integrity, encryption, and authentication controls
- HIPAA Contingency Plan Workgroup- developed/modified the policies and standards related to contingency planning
- HIPAA E-mail Security Workgroup- developed/modified the policies and standards for electronic mail and messaging
- HIPAA PC/Desktop Workgroup- developed/modified the policies and standards related to desktop computers

HIPAA Security Workgroup Policy and Standard Review (cont.)

- Data Center Operations/Physical Security Workgroups- developed/modified the policies and standards related to data center operations and physical security

Policies

Policy Review

- New Policies - 3
- Revised Policies - 7
- Deleted Policies - 1

Standards Review

- New Standards - 8
- Existing Standards Updated - 12

External Review

- Contracted consulting firm to review security architecture, perform vulnerability assessment and provide recommendations for implementation.

Security Awareness Training

- Staff
- Physician
- Manager Directions
- Security Liaison Directions

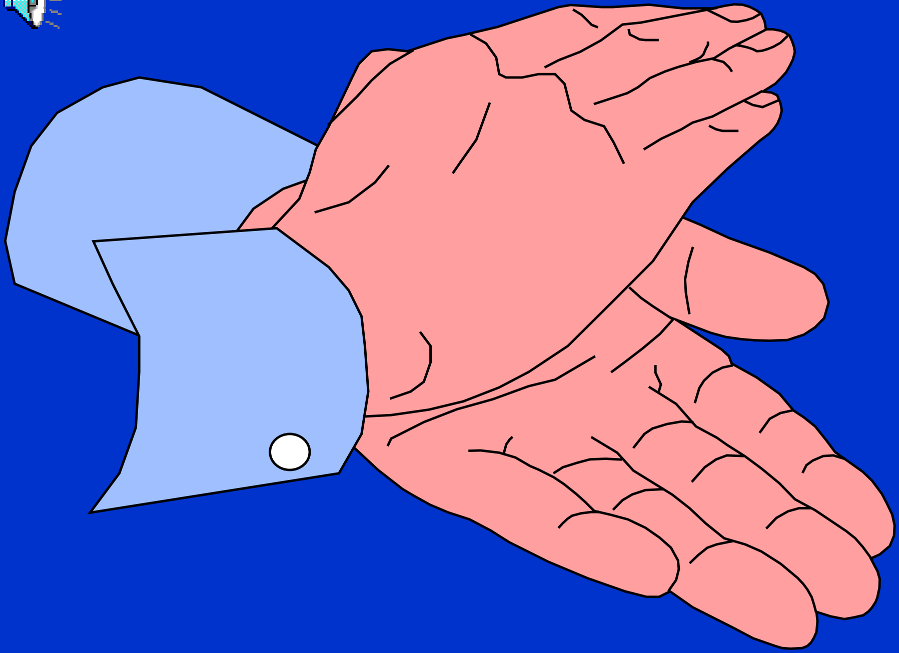
Other methods of education

- Reinforcing key elements through education/training
  - Multiple modalities for asking questions (e.g. HIPAA Ask Us Mailbox)
  - Identifying common questions for posting FAQs on internal web site
  - Articles in internal newsletters/publications as a quick reminder

Reporting Progress

- Using a Web-Based Scorecard
- Monthly Reporting: July- December 2004
- Biweekly: January- February 2005
- Weekly: March- April 2005

Compliance



ANY QUESTIONS

???