How We Were Able to Develop our own HIPAA Policies, Forms, Education Materials, etc. and Spend Very Little Money (Part II)

Angel Hoffman, RN, MSN

Director

Corporate Compliance

UPMC/University of Pittsburgh Medical Center

Review of How we began

- Established HIPAA Program Office
- Understanding HIPAA regulations and identifying the key points.
- Creating teams
- Developing team assignments and timelines
- Creating deliverables (e.g. policies, forms, status reports)
- Revisions to deliverables
- Leadership approval
- Procedures developed at each entity
- Implementation at the entity level
- Audit and evaluation

Creating teams

- HIPAA Privacy – Original members of the ten work groups to reconvene in October 2003
- HIPAA EDI – Advisory Group drives the process
  - Application subgroups with team leader for each application
  - Work driven by entity work team comprised of business and information technology members
- HIPAA Security – Seven Work groups
  - Application/system – Focus team
  - Survey development system level
  - Development of risk assessment tool (VCO)
  - System Kick-off Presentation
  - Meeting with work group leaders

Developing team assignments and timelines

- Corporate sponsors assigned
- Group leader established for each team
- Team members volunteered and/or assigned based upon expertise
- Timelines established to meet overall project timeline
- Minutes maintained and utilized as an ever growing work plan
- Work plans established for each team with assignments and due dates

Understanding the HIPAA regulations and identifying the key points

- Thorough review of the regulations
- Divided into topic areas
- Team(s) formed for each topic area
- Identified leadership for each team
- Meetings held on a regular basis
- Membership composed of experts from across the health system
- To do list and work plan developed for each team

Key elements in Identifying Risk

An individual has the right to privacy and confidentiality

Protect health information from unauthorized access

Monitor release of information

Consent for Treatment/Payment/Health Care Operations

Determining when Authorizations are required/needed

Employees should only access information they need to perform their job (role based access)

Identifying Business Associates

Addressing and maintaining Complaints - per new database

Security – per results of risk assessment tool

Creating Deliverables (e.g. policies, forms)

- Teams identified deliverables by interpretation of the regulations
- Draft policies, forms and miscellaneous documents created/reviewed/revised
- Documents sent to leadership for approval
- Documents placed in approved format and made available on intranet

Procedures developed at each entity

- Implementation sessions scheduled for each entity within the system
- Managers and Privacy Officers were provided education
- Implementation binders developed and distributed to each Privacy Officer
- Information kept current on share drive
- (Process modified for HIPAA EDI and same process to be replicated for HIPAA Security)

HIPAA Implementation

Implementation at the entity level

Procedures developed to implement key areas identified by system policies

Flexibility allowed per entity based upon resources available & operations

Procedures sent to HIPAA Program Office for system file

HIPAA Privacy Awareness Training

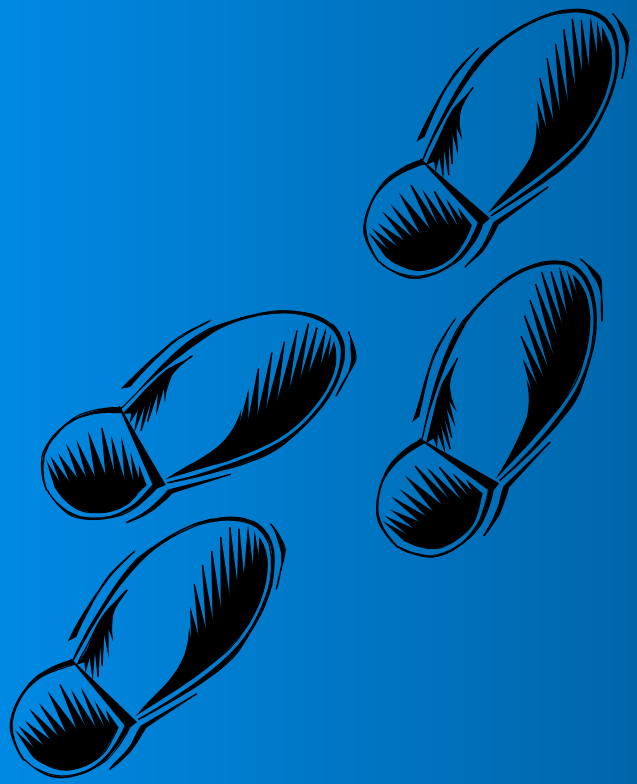
Educational Products

- Basic education
- Physician education
- Manager's Guide
- Clinical Guide (NEW)

Education

- Purchased authoring tool (in the process of exploring an additional tool and LMS)
- Engaged internal experts across system to write material for modules
- Elicited support from University
- Continued communication with University and health plan
- Significant cost avoidance realized

Next Steps???



Process Monitoring

Need for constant reevaluation and monitoring of overall project status.

- Held periodic forums for Privacy Officers
- Frequent communications
- Development of a share drive
- Modification of timeline
- Development of a “HIPAA Ask Us” mailbox
- Answering questions and development of FAQs

Key to Success is: maintaining an entity scorecard for tracking progress and keeping things moving!

Key:

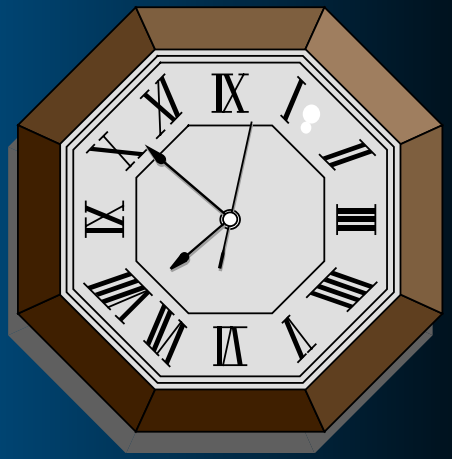
Purple NO REPORT SUBMITTED
Red No progress has been made or past due date
Yellow In progress
Green Completed
Orange Entity has not responded for current report period (listing current date)

Auditing and Monitoring

Established system "Go Live date" prior to government compliance date

Engaged Internal Audit Department to perform readiness surveys prior to compliance deadline

Reviewed data collected to address and refine system activity



HIPAA EDI

TIME IS Running out!

What are you doing to prepare?

HIPAA EDI Education for Executive Staff

Preparation for Successful implementation includes:

Risk assessment – identifying gaps, upgrading software

Education - HIPAA EDI training for executives, billing and technology managers and staff (any individuals identified within your organization that are responsible for billing and claim processing)

A business decision – Identify what direction that the organization wants to move toward

Trading partners - talking with trading partners assists you with what you can expect and defines what you need to do

Implementation (continued)

Testing – identifying and correcting errors for clean claim submission

Documentation – and more documentation to provide information regarding your process and the steps taken to work toward and become compliant

Rationale book – keeping a book is a good way to remember and document why you made the decisions that you made and the related reasons

Monitor Progress – establish and utilize a status report/score card

Re-evaluation – remember this is an ongoing process

Status Report should include:

- Status as of (current date)
- Entity Name and FEDERAL EIN
- Billing System
- Responsible Parties
- Testing Status / Issues
- HIPAA Compliance Status
- Financial Opportunities (optional and will be added as identified)
- Contact(s)

Remember:

to also look beyond October 16, 2003…

It doesn't end there!

Continue to monitor CMS website and information from "the experts" in the field (e.g. addenda, new X12 information,etc.)

HIPAA Security

Review of already established - Information Security Awareness Brochure for computer users

Viruses
Security Related Policies
Security Violations/Incident Reporting
Technical Assistance
Printing & Confidentiality
Proper Computer Use
Internet Use
Passwords
Use of Email

Agenda for the Kick-off meeting

- HIPAA Security Regulations Analysis performed
- Identify HIPAA Security Key Components
- Initiatives: Risk Assessment, assignment of Security Liaisons, establishment of work groups,

Current Supporting Initiatives

HIPAA's Intersections: Privacy, EDI, and Security

Timeline

What about challenges?

What does HIPAA Security require?

- Compliance by April 21, 2005
- Analysis of security standards (Required and Addressable)
- Protect and maintain the confidentiality, integrity and availability of electronic protected heath information (EPHI) whether in storage or in transit
- Protection of EPHI against anticipated threats
- Policies

What else?

- Protect and guard electronic data integrity, confidentiality, and availability
- Maintain documentation and make available for 6 years for periodic review/update

Standardize security practices

Some things to consider:

- Size, complexity, and capabilities of organization
- The technical infrastructure, hardware and software capabilities
- Cost and practicality
- Potential risk to organization

HIPAA Security Key Components

I. Administrative Safeguards

II. Physical Safeguards

III. Technical Safeguards

HIPAA Security Sections

I. Administrative Safeguards
- Primarily the policy/practices related to management of protecting data
  - Risk Assessment
  - Risk Management Program
  - Security Policy

HIPAA Security Sections

II. Physical Safeguards
- Access practices and controls
  - Contingency and disaster recovery processes

III. Technical Safeguards
- Information technology applied to assure data security on the application, network and server platforms.

Our HIPAA Security Initiatives

System Privacy Officer and Security Officer

Security Liaisons (Security contacts for each entity)

Risk Assessment Tool (VCO, a self paced tool)

Establishment of Seven work groups

Risk Assessment tool

- self paced
- provides customized recommendations based on current policies, procedures and culture
- **Reporting & Monitoring** provides ad-hoc reporting and on-going evaluation monitoring

Security Workgroups

- HIPAA Business Associate Workgroup
- HIPAA Clinical Applications Workgroup
- HIPAA Contingency Plan Workgroup
- HIPAA Email Security Workgroup
- HIPAA PC/Desktop Workgroup
- Data Center/Operations/Physical Security Workgroup
- Physical Security Workgroup

Role of Security Liaisons

- Responsible for:
- Identified contact
- Completion of risk assessment
  Implementation at the entity level

Information Security Group Supporting HIPAA Projects

Account Administration

Computer Incident Response Team

Minimum Security Baselines

Network Intrusion Detection

Perimeter Monitoring and Security Testing (firewalls)

Policy Review Process (review, create, modify and delete)

Revisit Role Based Access

Education – Security Awareness Training (modules developed as appropriate)

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.

HIPAA Project Management Time Line for HIPAA Security Timeline

2003 HIPAA Privacy and Security	Feb 03	Mar 03 to July 03	Aug 03 to July 04	Aug 04 to Mar 05	Mar 05 to April 05	April 05
Pre-Phase I	Phase I	Phase II	Phase III	Phase IV	Phase V	April 21, 2005
HIPAA Security Info on HIIPAA Share Drive and Infonet: Security Awareness Brochure developed	Feb. 2003 regulations finalized	• Analysis of the regs. • Kick-off meeting July 17, 2003 • Clinical Applications Workgroup has first meeting.	• Workgroups meet • Policy Review and Development	• Implementation at each UPMC entity • Education and training of work force	• Program Evaluation and Auditing	• Compliance Date

What challenges lie ahead?

Compliance Deadline – April 21, 2005

Financial constraints – when funding is limited

Collaborative decisions made to implement at the entity level

Communication

Management support

For Questions…

Call The HIPAA Program Office at Corporate Compliance

HIPAA Compliance

ANY QUESTIONS

???