4.06 Revisions to the HIPAA Privacy Program – A Six Month Look Back after the April 2003 Compliance Date

Angel Hoffman, RN, MSN

Director, Corporate Compliance
University of Pittsburgh Medical Center, Pittsburgh, PA
hoffmanam@upmc.edu

Frank Ruelas, MBA

Director, Corporate Compliance
Gila River Health Care Corporation, Phoenix, Arizona
fruelas@grhc.org

Recap of 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

Recap of Key Elements in Identifying Risk (contd.)

- Employees should only access information they need to perform their job (role based access)
- Identifying Business Associates
- Tracking and processing Complaints
- Acknowledging/Addressing Privacy and Security intersections

What happened after we had six months of experience?

What did we find?

- Minor revisions to only a few policies and forms
- Implemented processes are working
- Requests to automate accounting of disclosures
- Need to continue periodic reeducation

Common issues

- Managing complaints
  - Communication with Privacy Officers
  - What are the common issues?
  - Follow up and outcomes
  - Documentation
  - OCR letters

Common issues (contd.)

- 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

Common issues (contd.)

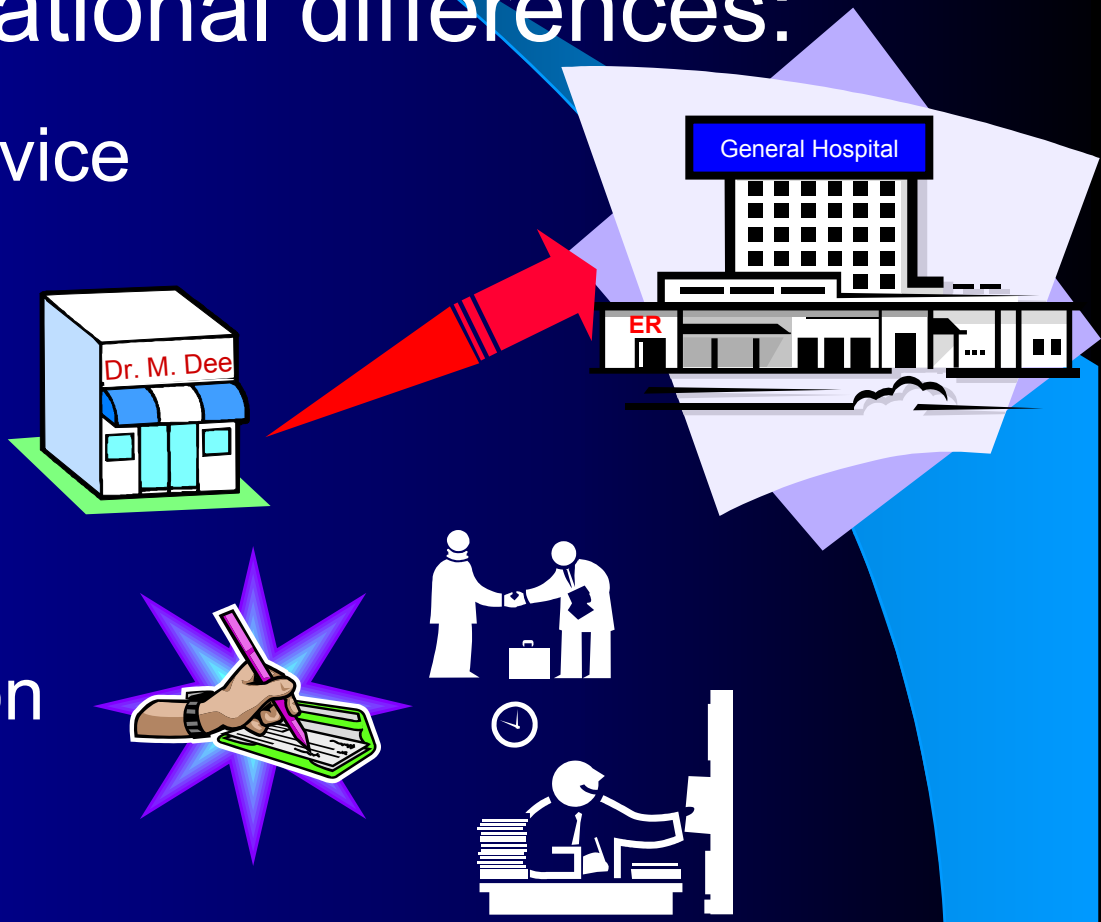
- Budgetary Impact
- Management Support

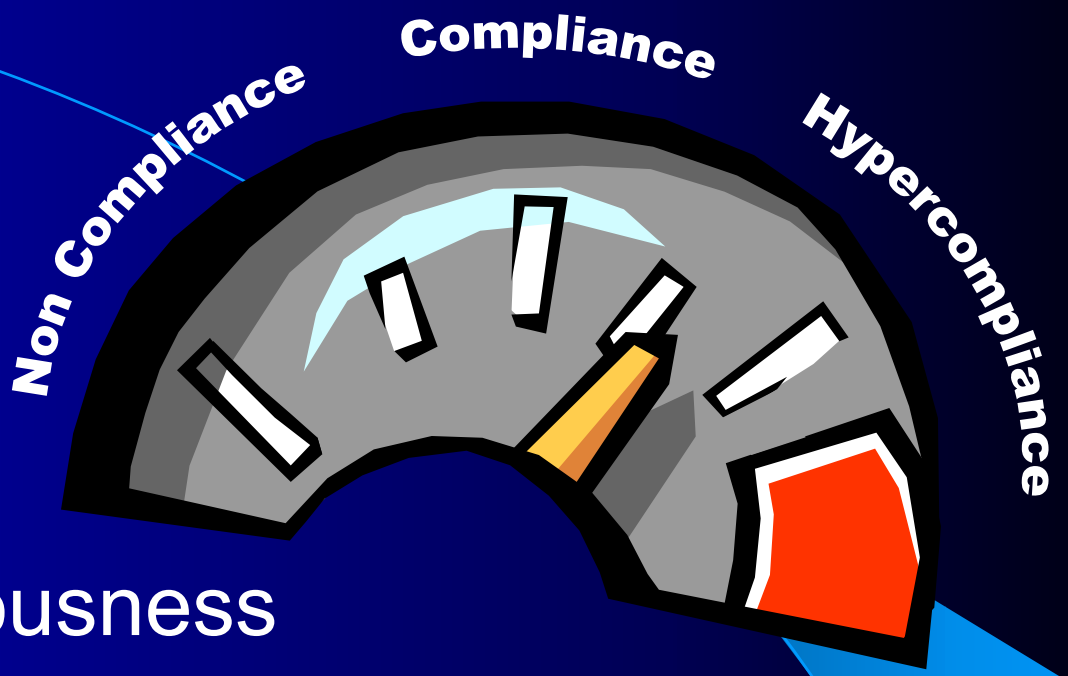
- "Hot topics"
  - Release of HIPAA and clarification of Incidental disclosures vs. violations
  - Business Associates and necessary agreements
  - Use of fax machines and lab auto faxes

A Nonstandard Approach to Standards

Observed organizational differences:

- Size and scope of service
- Use of resources
- Budget allocation





Early HIPAA Era Marked by Cautiousness

Contributing Factors:

- Permitted versus Required Dilemma
- Inward Focus in Applying HIPAA Regulations
- Fear of Penalties

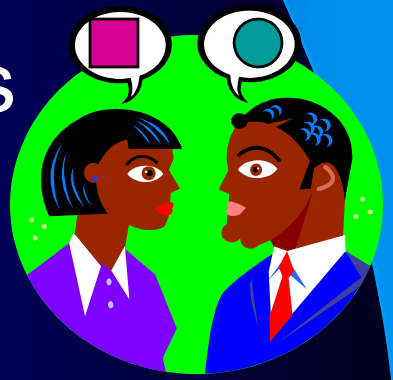
Permitted versus Required Dilemma

Minimal inconsistency in processes when tasks are identified as required:

- Access to medical record
- Accounting of disclosures

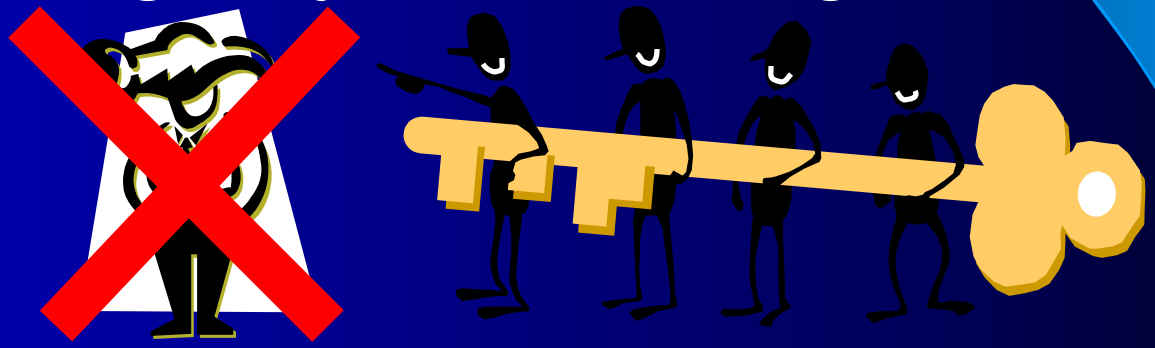
When a process is identified as permitted, all bets are off:

- Disclosure for treatment



Inward Focus in Applying HIPAA Regulations

- Unwilling to try alternative approaches
  - We're right, you're wrong attitude

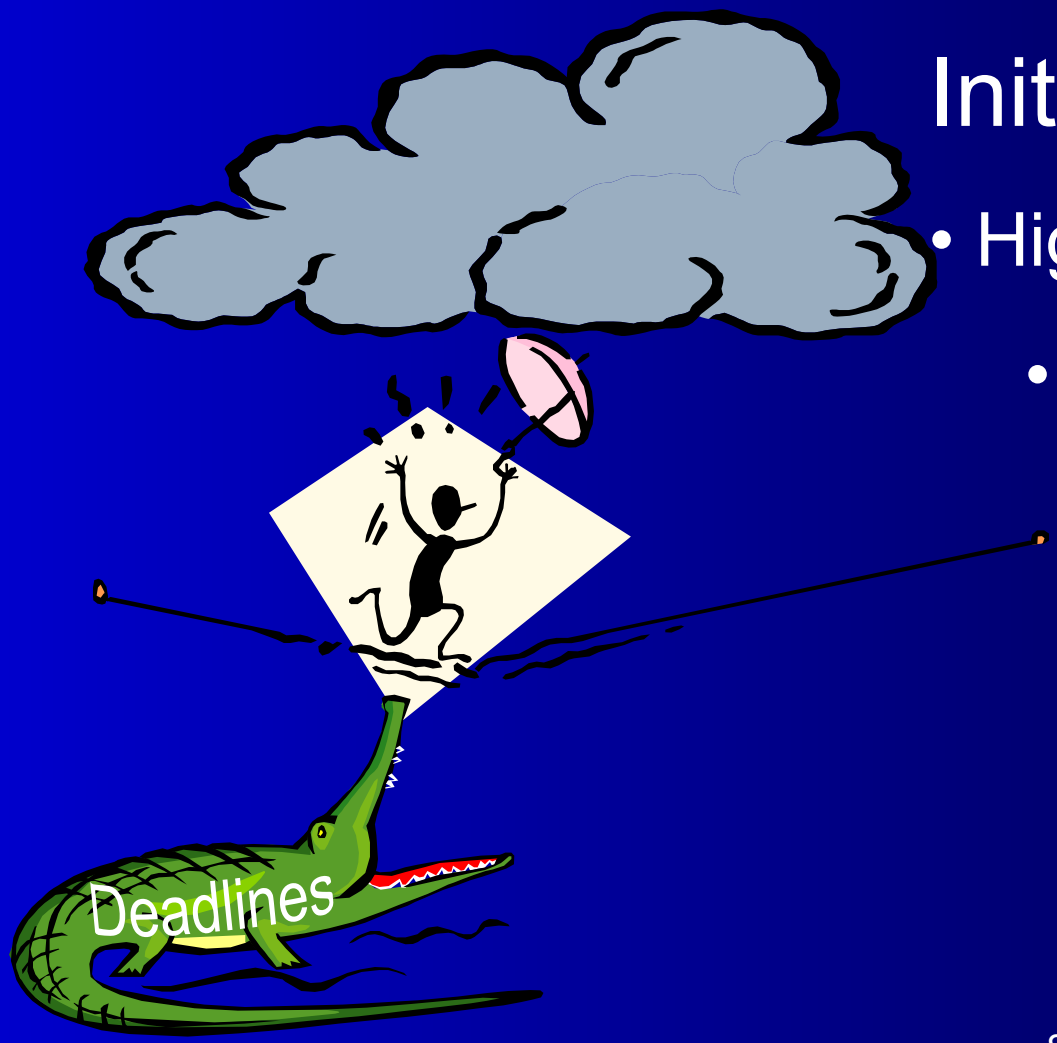


  - Improvement is built on change
- We both can win or lose

Fear of Penalties

- Fines
- Lawsuits
- Jail
- Set precedence

The Placement of HIPAA within the Corporate Culture

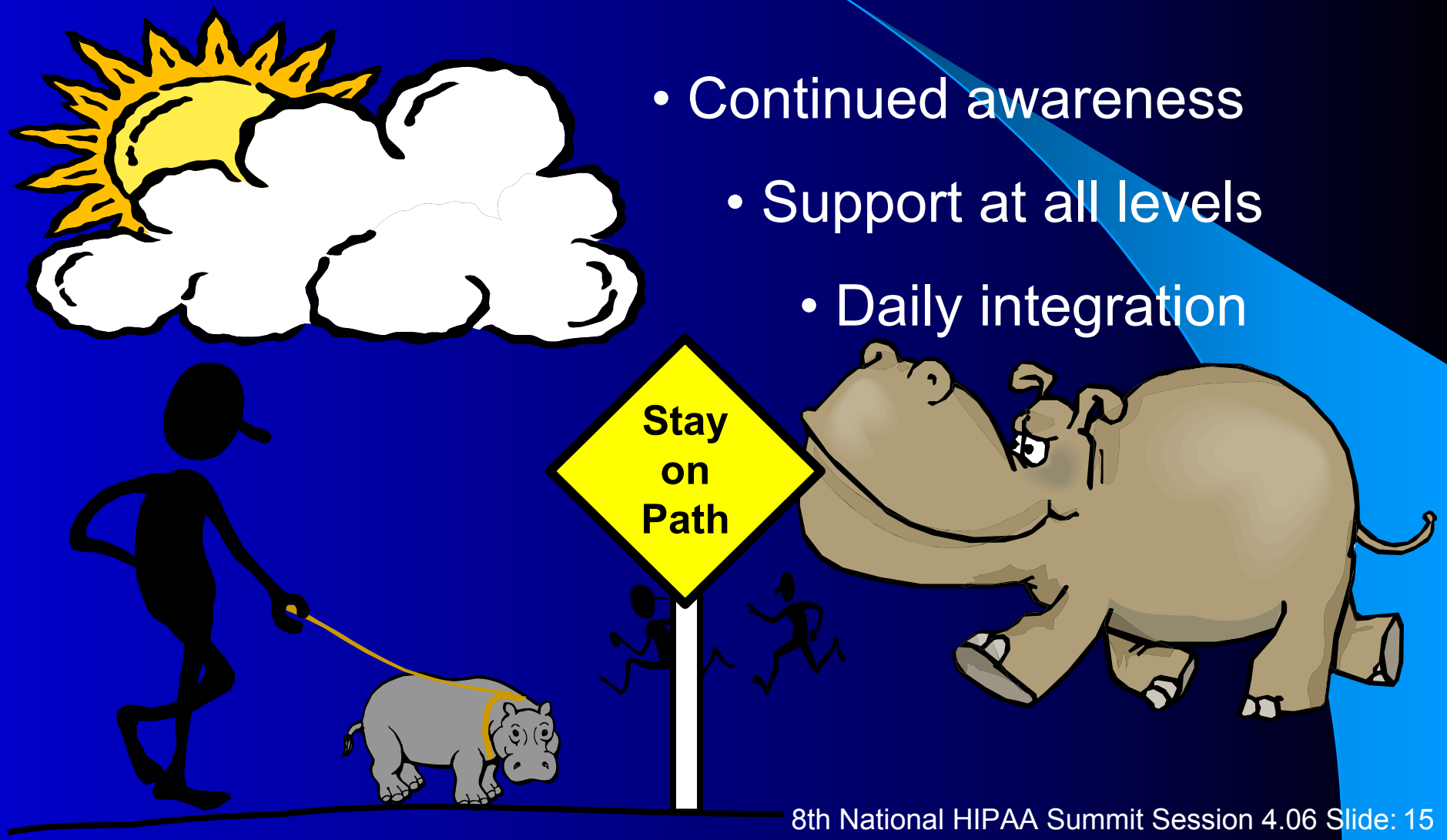


Initial Framework

- High priority
  - High level of attention
    - High visibility
      - High energy

The Placement of HIPAA within the Corporate Culture

- Continued awareness
- Support at all levels
- Daily integration

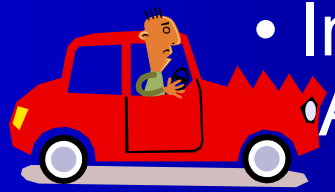


Incidental Disclosure

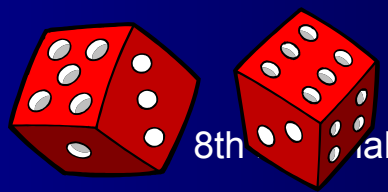
"…the Department [of Health and Human Services] reiterates that the Privacy Rule must not impede essential health care care communications and practices."

(**Federal Register** / Vol. 67, No. 157 / Wednesday, August 14, 2002 / Rules and Regulations / Page 53182)

Possible Contributing Factors



- Incidental may be Accidental
- Trying to control the uncontrollable



Inward to Outward Focus Strategy: A Faxing of PHI Case Study

(c)(1) *Standard: safeguards.* A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2) *Implementation specification: safeguards.*

(i) A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

OCR/HIPAA Privacy/Security/Enforcement Regulation Text
August 2003

-39-

Inward to Outward Focus Strategy:
A Faxing of PHI Case Study

(c)(1) *Standard: safeguards.* A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.

(2) *Implementation specification: safeguards.*

(i) A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart.

(ii) A covered entity must reasonably safeguard protected health information to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure.

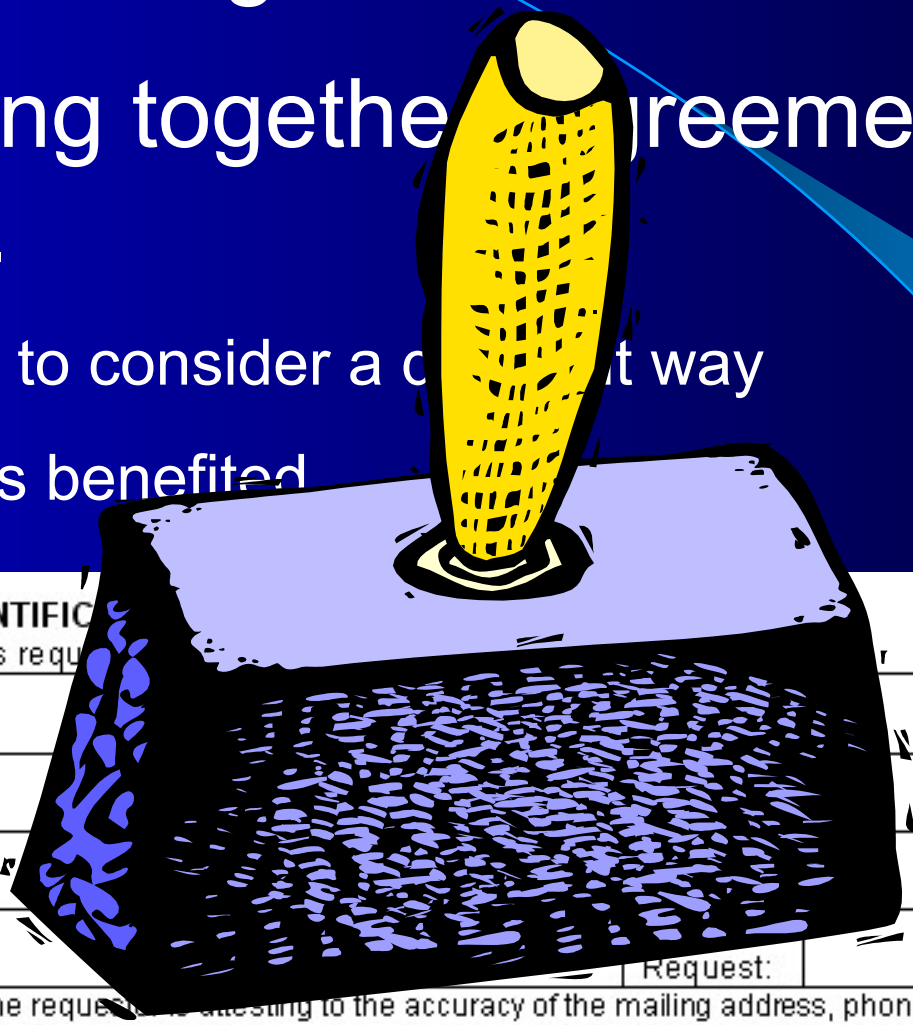
Safeguards Concern

- Reasonableness
- Verification of Identity
- Accurate Information
- Incidental disclosure

Inward to Outward Focus Strategy:
A Faxing of PHI Case Study

By working togethe greement was reached.

- Willingness to consider a c t way
- Both entities benefited



IV. REQUESTOR IDENTIFIC

The person making this requ

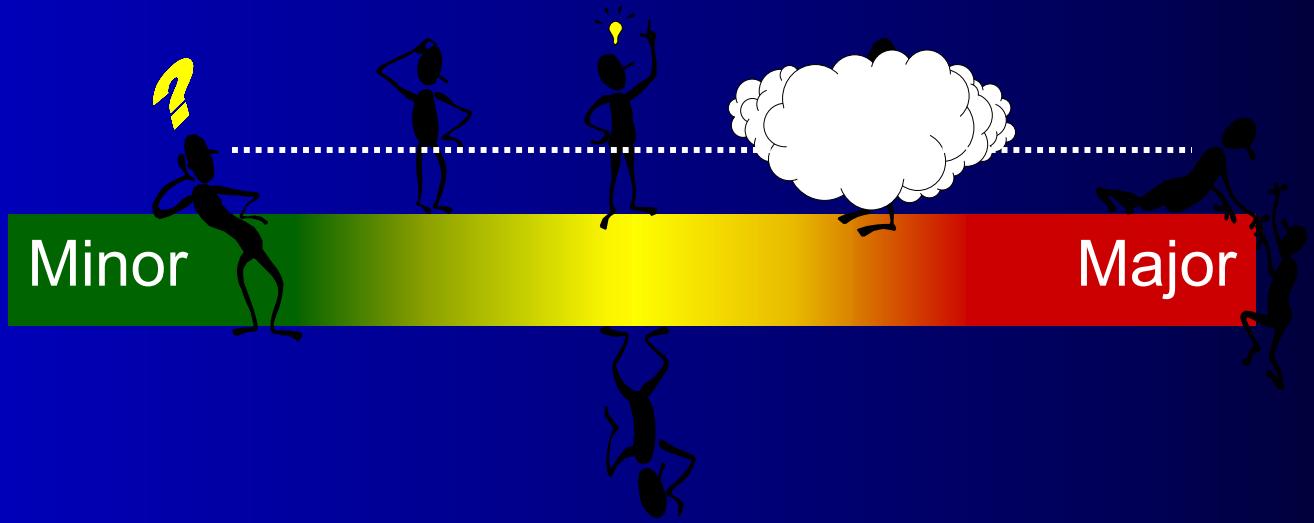
Printed Name and Title:			
Mailing Address:			
Phone Number:			
Requestor's Signature:		Request:	

By signing this request, the reque attesting to the accuracy of the mailing address, phone number, and fax number presented in the Requestor Identification Section so as to provide an administrative safeguard under 45 CFR 164.530 that the requested information is routed correctly to the attention of the requestor. (Form approved 12/2/03)

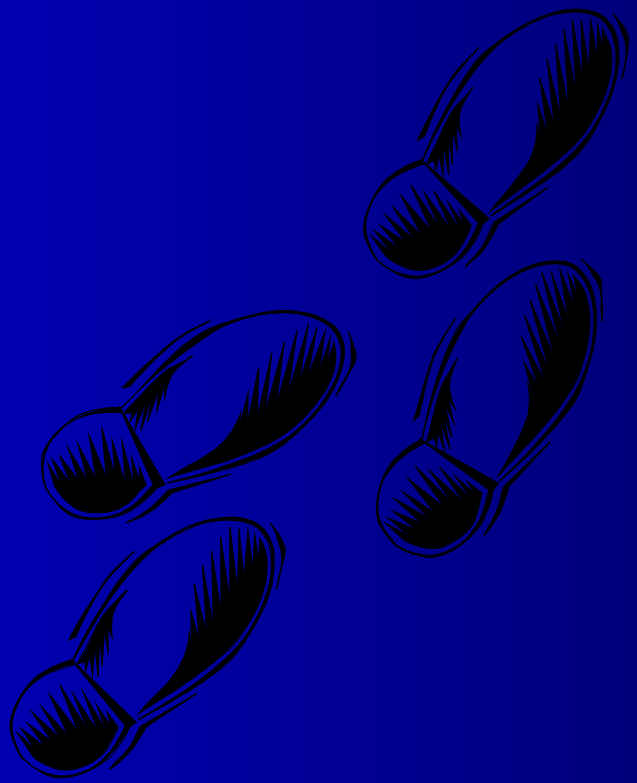
Policy and Procedure R&R

Anything but Rest and Relaxation

- Review and Revision process often reflects:
  - Changes in operations
  - New information
  - Lessons learned (experience)



Next Steps???



Time for reevaluation

- Review data collected to address and refine system activity
- Privacy work groups reconvened to review policies, forms and processes
  - Policies
  - Forms
  - Processes
- What did we find?
  - Minor revisions needed to only a few policies and forms
  - Processes put in place are working
  - Requests to automate accounting of disclosures

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 6 years for periodic review/update

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

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.

Build on Experience

Share information and lessons learned through experience

- Partnering
- Information sharing
- Inter-organizational learning
- Innovation
- Trust

ANY QUESTIONS

???