

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

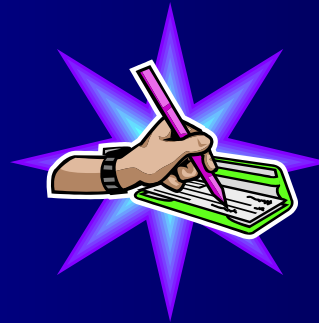
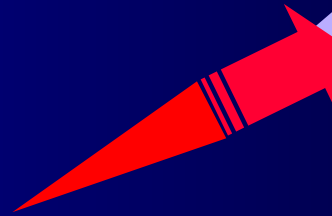
A Nonstandard Approach to Standards

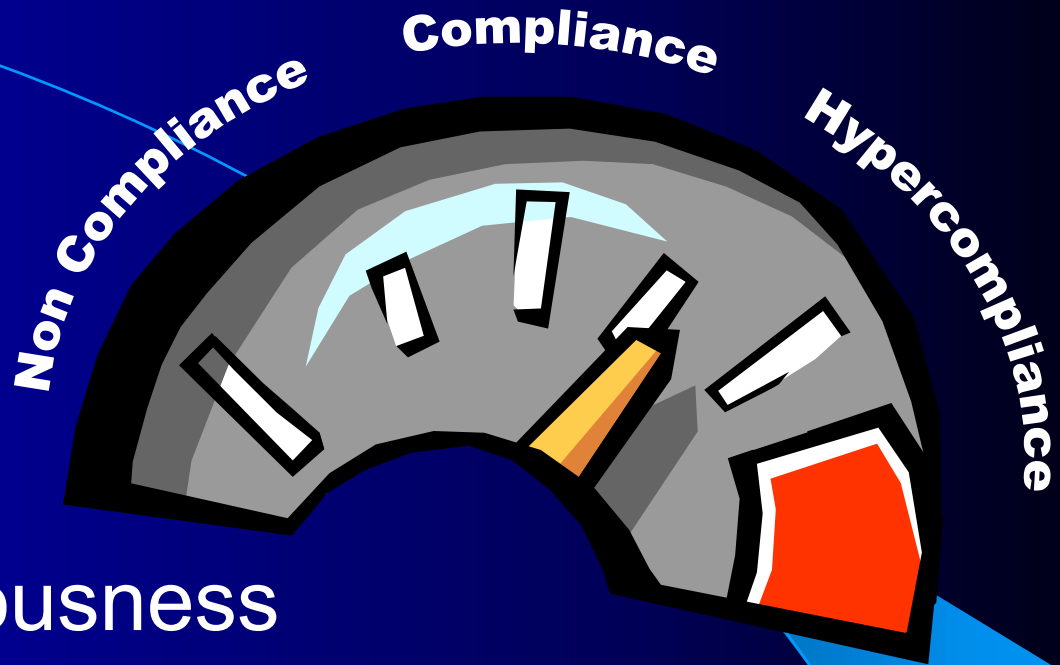
Observed organizational differences:

- 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

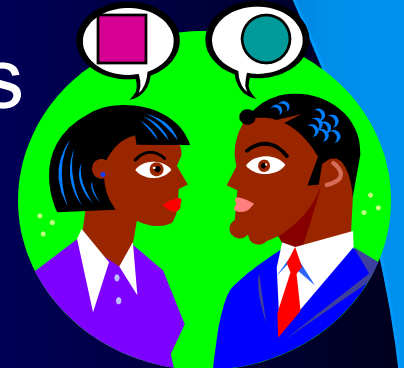
Minimal inconsistency in processes when tasks are identified as required:

- Access to medical record
- Accounting of disclosures



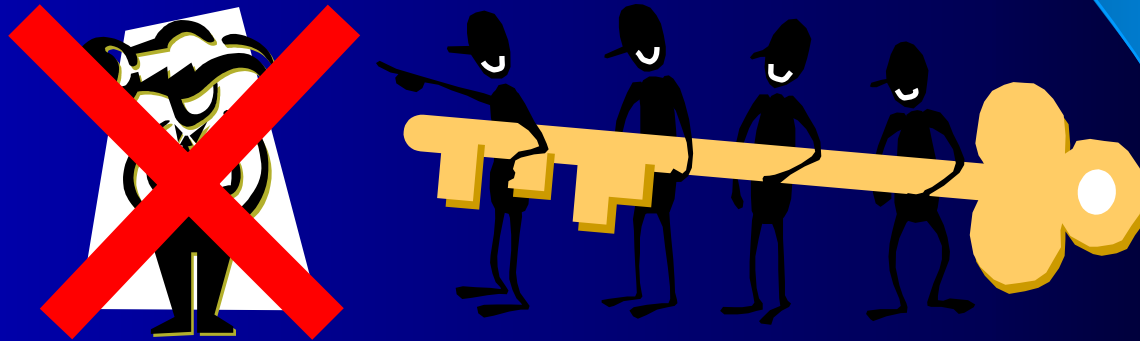
When a process is identified as permitted, all bets are off:

- 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

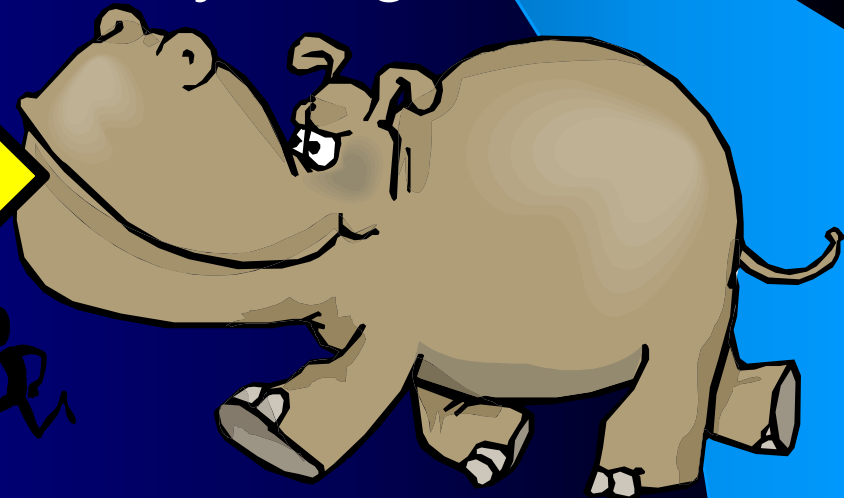
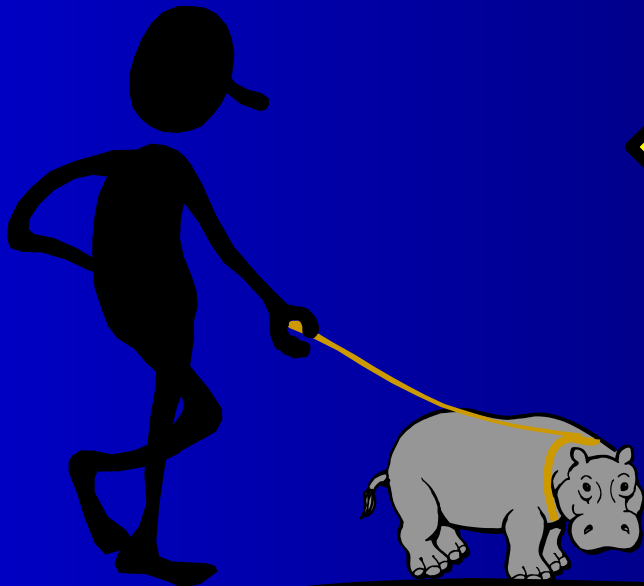
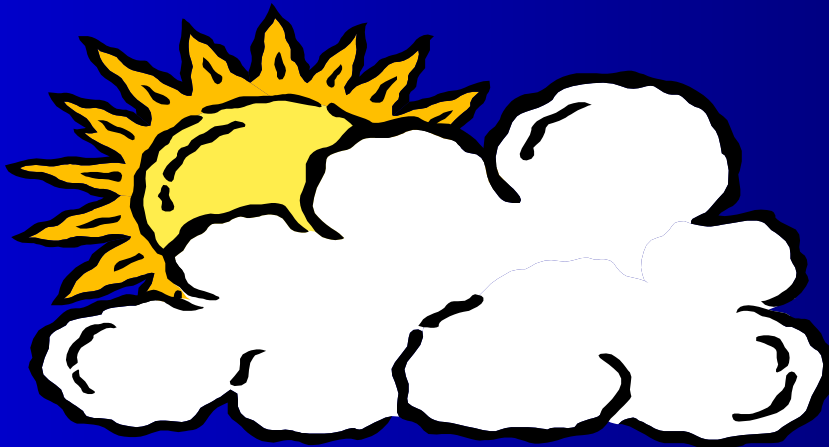
Initial Framework

- 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



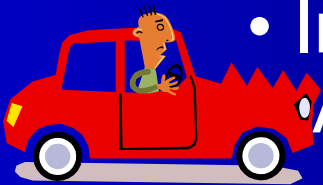
Incidental Disclosure



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

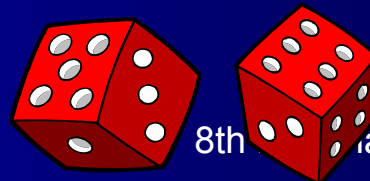
(Federal Register / Vol. 67, No. 157 / Wednesday, August 14, 2002 / Rules and Regulations / Page 53182)

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.

(7) Therefore, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose education or training is required by this subpart, within a reasonable period of time after the initial change becomes effective in accordance with paragraph (1) of this section.

(8) A covered entity must document the training as described in paragraph (6)(2)(b) of this section has been provided, as required by paragraph (4) of this section.

(9) *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.

(6)(1) *Standard: compliance to the covered entity.* A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart or its compliance with such policies and procedures or the requirements of this subpart.

(2) *Implementation specification: documentation of compliance.* As required by paragraph (1) of this section, a covered entity must document all complaints received, and their disposition, if any.

(6)(1) *Standard: notices.* A covered entity must have and apply appropriate notices to all members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart. This standard does not apply to a member of the covered entity's workforce with respect to notices that are covered by and that meet the conditions of § 164.502(j) or paragraph (6)(2) of this section.

(2) *Implementation specification: documentation.* As required by paragraph (1) of this section, a covered entity must document the notices that are applied, if any.

(7) *Standard: emergency.* A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of the policies and procedures or the requirements of this subpart by the covered entity or its business associates.

(8) *Standard: refraining from reusing or re-disclosing.* A covered entity may not intentionally, knowingly, or recklessly reuse, or disclose, information against, or to, the other retaliatory action against:

(1) Individuals. Any individual for the exercise by the individual of any right under or for participation by the individual in any process established by this subpart, including the filing of a complaint under this section;

(2) Individuals and others. Any individual or other person for:

(i) Filing of a complaint with the Secretary under subpart C of part 160 of this subchapter;

(ii) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title 32; or

(iii) Opposing any act or practice made unlawful by this subpart, provided the individual person has a good faith belief that the practice opposed is unlawful, and the nature of the opposition is reasonable and does not involve a disclosure of protected health information in violation of this subpart.

(9) *Standard: notice of rights.* A covered entity may not make any individual waive their rights under § 160.316 of this subchapter or this subpart as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(8)(1) *Standard: policies and procedures.* A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. The policies and procedures must be reasonably designed, taking into account the size and the types of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart.

(2) *Standard: changes to policies and procedures.*

(i) A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements,

and implementation specifications of this subpart;

(ii) When a covered entity changes a privacy practice that is stated in the notice described in § 164.502(b), and makes corresponding changes to its policies and procedures, it may make the changes effective for protected health information that it creates or receives prior to the effective date of the notice revision; the covered entity has, in accordance with § 164.502(b)(3)(CC), included in the notice a statement reserving its right to make such a change in its privacy practice; or

(iii) A covered entity may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with paragraph (1)(5) of this section.

(3) *Implementation specification: changes in law.* Whenever there is a change in law that necessitates a change to the covered entity's policies or procedures, the covered entity must promptly document and implement the revised policy or procedure. If the change in law directly affects the content of the notice required by § 164.502(j), the covered entity must promptly make the appropriate revisions to the notice in accordance with § 164.502(b)(3). Nothing in this paragraph may be used by a covered entity to excuse a failure to comply with the law.

(6) *Implementation specification: changes to privacy practices used in the service.*

(1) To implement a change as provided by paragraph (6)(2)(i) of this section, a covered entity must:

(A) Post the policy or procedure, as revised to reflect a change in the covered entity's privacy practice as stated in its notice, comply with the standards, requirements, and implementation specifications of this subpart;

(B) Document the policy or procedure, as revised, as required by paragraph (1) of this section; and

(C) Revise the notice as required by § 164.502(b)(3) to state the change of practice and make the revised notice available as required by § 164.502(b). The covered entity may not implement a change to a policy or procedure prior to the effective date of the revised notice.

(ii) If a covered entity has not revised its right under § 164.502(b)(3)(C) to change a privacy practice that is stated in the notice, the covered entity is bound by the privacy practices as stated in the notice with respect to protected health information created or

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.

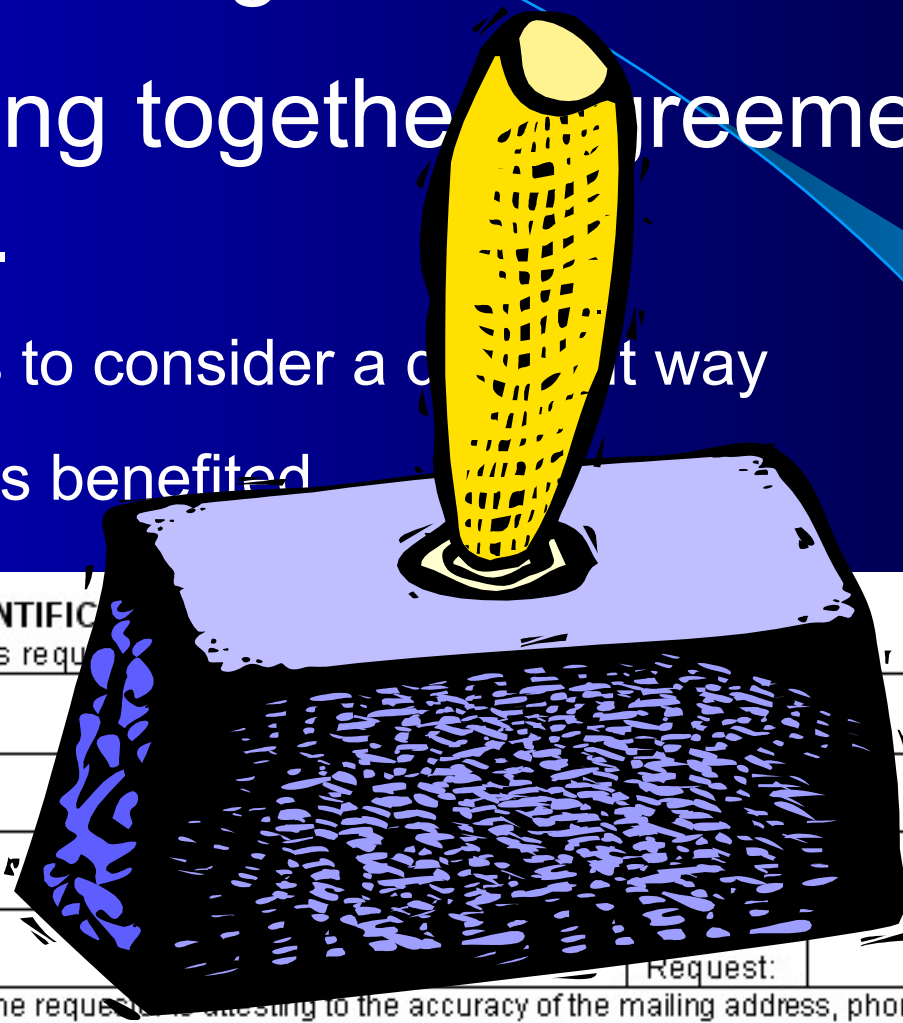
Safeguards Concern

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

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

By working together an agreement was reached.

- Willingness to consider a different way
- Both entities benefited



IV. REQUESTOR IDENTIFICATION

The person making this request is:

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

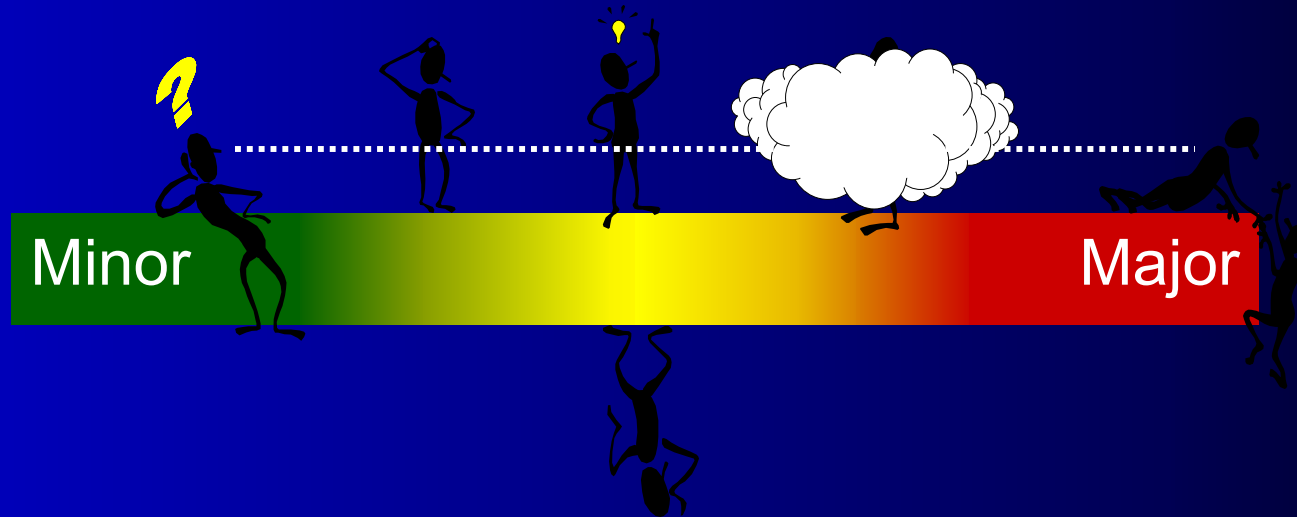
By signing this request, the requestor is attesting to the accuracy of the mailing address, phone number, and fax number presented in the Requestor Identification Section so as to provide an administrative safeguard under 45 CFR 164.530 that the requested information is routed correctly to the attention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

Policy and Procedure R&R

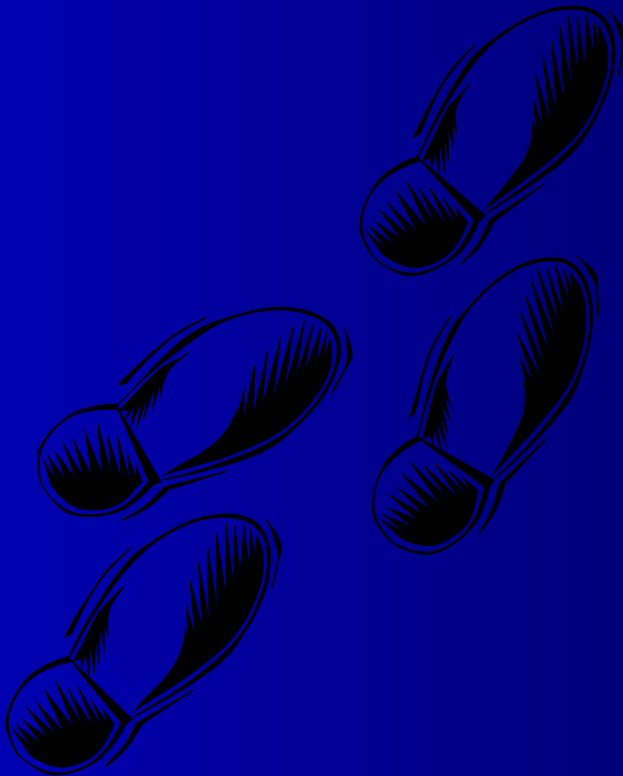
Anything but Rest and Relaxation

- 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

???