

# Updating HIPAA+ P&P

HITECH

Red Flags

FERPA

M.U. EHR

Others

**Margret Amatayakul,**

MBA, RHIA, CHPS, CPHIT, CPEHR, FHIMSS

**Margret\A Consulting, LLC**



# Agenda

- **Importance of Policy**
- **Drivers for Updating P&P**
- **Writing Effective P&P**
- **New P&P Needed Today**
- **Implementing P&P**

Jan 12, 2009 10:07 AM



## Good Old HIPAA Violation!

by [shodobe](#)  

This is for everyone's info. recently I got into trouble for a [HIPAA](#) violation at my hospital. First major infraction in 31 years! Early part of last month I was doing a case in the OR when we heard that a RT employee had come into the ED in full code. I was already in the ER roster looking up a potential patient for the surgeon and saw the name and looked to see if I knew him. I know a lot of the RT but didn't know him by name. I forgot about it until a few days ago when I was called into the "principals" office downstairs, not my [Directors'](#) office. I was asked if I had indeed looked and I said yes because I wanted to make sure it wasn't a friend of mine. They told me that there had been quite a number of hits, we use computer nursing, and they were going to talk with everyone. They also told me there would be disciplinary actions taken, but not termination. I thought I would probably get written up and that would be it. Instead I got a 3 day suspension. The HIPAA czar I talked to had said the rules had gotten much stricter after the first of the year but I didn't expect this. I went into our HIPAA manual and looked up the policies concerning punishments. It went from verbal counseling to written, all the way up to suspension and termination. They jumped all the way up to final warning and suspension. I don't mind the suspension as much as they might of changed the policies concerning punishment and did not inservice or inform the employees of such changes. I only think it would be fair on their part to do formal inservices or at least put out memos to the changes. This post is for info for everyone to watch out, "They are watching"!

# Importance of Policy

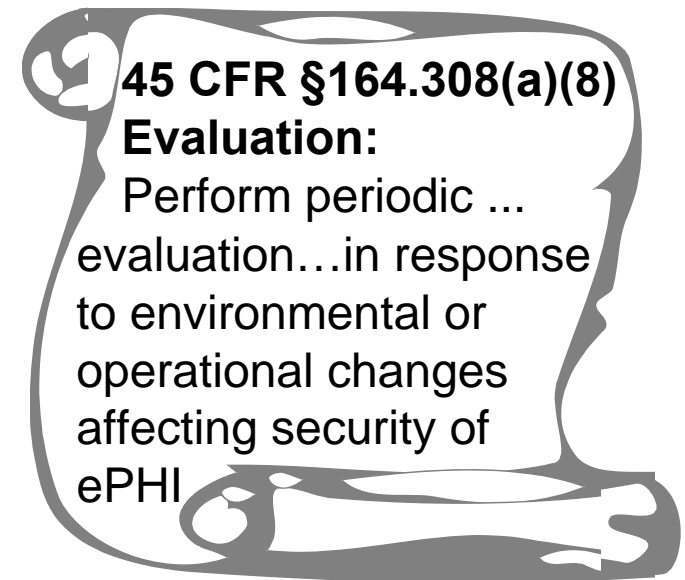
- **Guidance for action consistent with legal, ethical, and organizational requirements**
- **Policies . . .**
  - **Establish goals that procedures and technical measures serve**
  - **Communicate consensus and assign responsibility**
  - **Define enforcement and consequences for violation**
- **Policy is a *mutual agreement* that outlines the expectations your organization has for its workforce**

# Policies, Procedures, Standards, Technical Controls

- **Policies** *guide* action
  - Broad statements
  - Corporate wide
  - Executive approval
- **Procedures** *direct* action
  - Specific steps
  - Focus on process
  - Departmental management
- **Procedures answer:**
  - What to do
  - When to do it
  - Where to do it
  - Who should do it
  - Exactly how to do it
- **Standards** *define* minimum expected performance
  - De facto, e.g., “Passwords should be 8 characters”
  - Consensus driven, e.g., Standards of Practice, HL7
  - Government mandate, e.g., HIPAA Rules
- **Technical controls** *cause* operations to meet policy requirements
  - Example: Access controls cause users to gain applicable access to information

# Drivers for Updating P&P

- **New regulations (e.g., Red Flags, HITECH)**
- **New threats, e.g.,**
  - Identity theft, medical identity theft
  - Economy
  - “Value engineering”
  - HIPAA enforcement
- **New vulnerabilities, e.g.,**
  - Consumer empowerment
  - Electronic health records
  - Health information exchange
  - Meaningful use requirements



# Writing Effective Policies

- **Policy characteristics**
  - Enforceable
  - Concise and easy to understand
- **Deciding on what the policy should be**
  - Understand circumstances pertinent to policy being written (e.g., confidentiality of PHI vs. government's nuclear weapons program)
  - Determine organization's corporate position (e.g., risk averse, risk tolerant)
- **Steps in policy writing**
  - Draft
  - Test
  - Introduce, train, reinforce
  - Enforce, reinforce

Top Secret

Secret

Confidential

Restricted

Unclassified

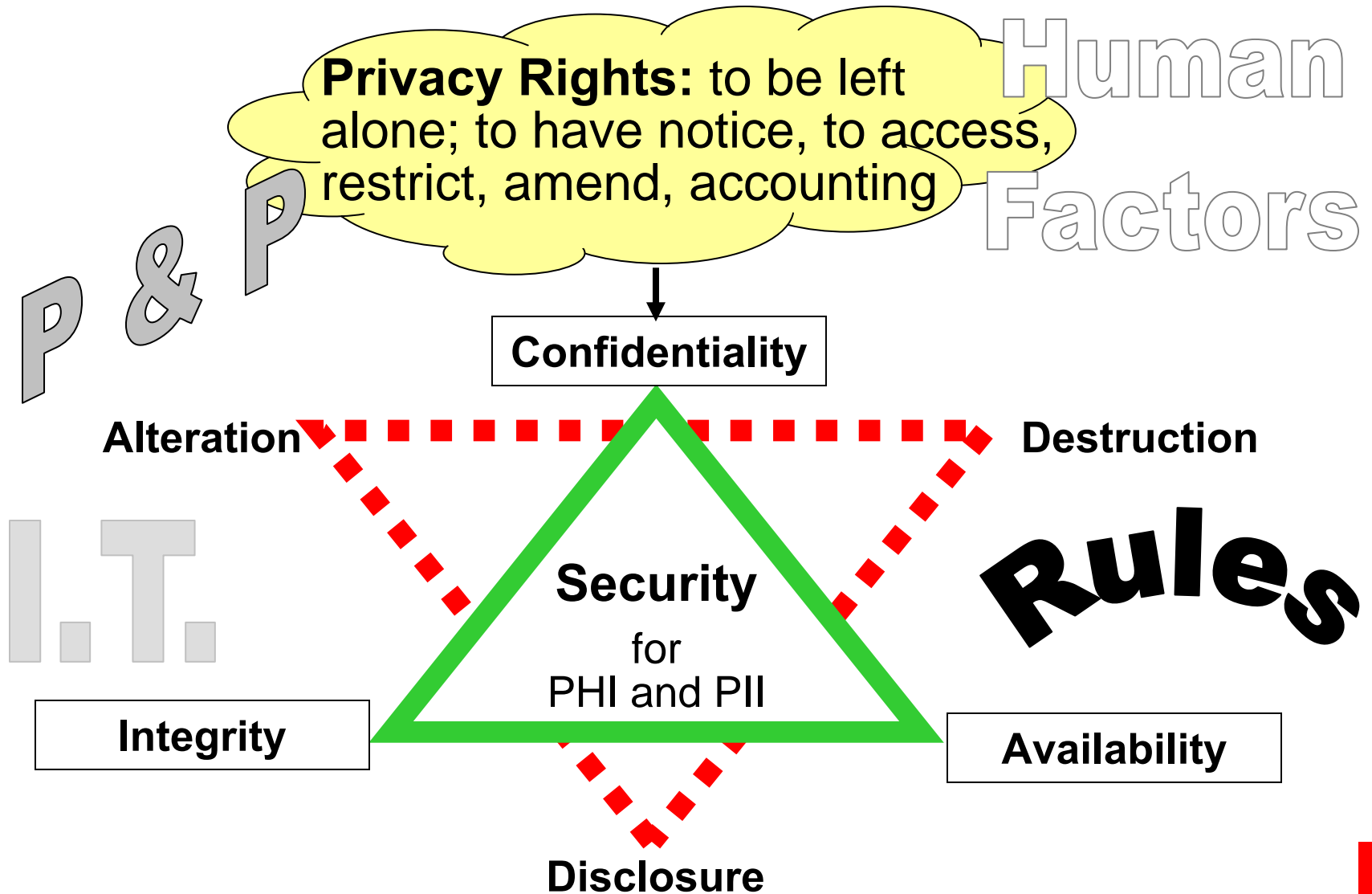
# Procedures

## Scenario

- “I want to review my patient’s record before I enter the exam review”
- “I don’t want to be logging on and off constantly”
- “Every time I log on, I have to click through screens I’ve already looked at”
- Workflow and process changes with HIT must be studied in light of patient care, hassle factors, privacy & security
- A process map or even a use case can actually be an effective tool to design and document procedures

David Blumenthal, MD, ONC – on meaningful use, Dec. 7, 2009: “It’s not the technology that’s important, but its effect. Meaningful use is not a technology project, but a change management project. Components of meaningful use include sociology, psychology, behavior change, and the mobilization of levers to change complex systems and improve their performance.”

# Privacy and Security Integration



# New Policies: Privacy and Security

- **Accounting of disclosures (regulations expected June 18, 2010)**
  - **Address policy and technical controls to account for disclosures from EHR for TPO within past 3 years**
  - **Disclosure**
    - Same meaning as in 45 CFR §160.103
    - means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information

# New Policies: Privacy and Security

## ■ **Breach** notification (Aug. 24, 2009)

- Incorporate federal and state requirements
- Address incident reporting and response
  - HITECH: **Breach** means unauthorized acquisition, access, use, or disclosure of PHI which compromises security or privacy of PHI, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information
  - Exceptions, “breach” does not include
    - Unintentional acquisition, access, or use of PHI if made in good faith and within scope of employment or professional relationship; and
    - such information is not further acquired, accessed, used, or disclosed; or
    - any inadvertent disclosure from an individual who is otherwise authorized to access PHI to another similarly situated individual at same facility; and
    - such information is not further acquired, accessed, used, or disclosed without authorization by any person
  - **Notification is required if a breach of unsecured PHI occurs**

# New Policies: Privacy and Security

- **Business associate (regulations expected Feb. 18, 2010)**
  - Incorporate direct accountability to certain provisions of HIPAA Privacy and Security Rules;
  - Business associate contract for HIO
- **Guidance on “psychotherapy notes” (Feb. 18, 2010)**
- **Prohibit exchanging PHI for remuneration without individual authorization (Aug. 18, 2010)**
- **Provisions regarding marketing and fundraising (Feb. 18, 2010)**
- **Requirements for de-identification (Feb. 18, 2010)**
- **Rights (Feb. 18, 2010)**
  - Request restrictions (to payers where patient pays)
  - Minimum necessary; guidance on what constitutes minimum necessary (Aug. 18, 2010)
  - Access (provision of electronic information)

# New Policies: Privacy and Security

- **Technical guidance on safeguards (Feb. 18, 2010; annual updates)**
- **Unsecured PHI (Guidance Apr. 27, 2009)**
  - **Encrypt**
  - **Destroy**
  - **(De-identify ≠ HIPAA)**
- **Enforcement by State Attorneys General (applies after Feb. 17, 2009)**
- **Enforcement amendments (October 30, 2009)**
- **Willful neglect provisions in HIPAA Enforcement Rule (Aug. 18, 2010)**
- **Sharing civil money penalties or settlements with harmed individuals (Feb. 18, 2012)**
  - **Impact on organizational policies? Training? Awareness**

# Consumer Empowerment

## ■ FERPA (Joint Guidance Aug. 2008)

- Applicable to your organization?

## ■ FTC Health Breach Notification Rule

- Published Aug. 25, 2009, effective Sept. 24, 2009, full compliance required by Feb. 22, 2010
- Impacts Personally Identifiable Information (PII) in personal health records (PHRs) provided by vendors or other entities, such as schools, charities, and non-profits
- Applicable to your organization?
- Buried disclosures in privacy policy?

## ■ Red Flags Rules (enforcement began Aug. 1, 2009)

- Applicable to your organization?
- What warning signs should you look for?

# Electronic Health Records

- **Mission critical system requiring . . .**
  - Contingency planning and disaster recovery
  - Technical redundancy: servers, network
- **Use as intended**
  - Applying clinical decision support
    - Applying evidence-based standards of practice
    - Sensitivity levels
    - Rationale for override
  - At point of care
  - By clinician
  - To capture structured data
    - Ensuring data quality, including with ICD-10-CM codes (October 1, 2013) embedded in many HIT applications
  - While enabling and assuring application of professional judgment

# Health Information Exchange

- **Applying HIT standards**
  - **Continuity of Care Document**
- **Consent directives in HIO**
  - **Authorization vs. consent (HIPAA §164.506 Consent is not effective to permit a use or disclosure when an authorization is required)**
- **Stage 1 criteria for meaningful use**
  - **Test capability of certified EHR technology to electronically exchange key clinical information among providers of care and patient authorized entities**
  - **Test capability to communicate with public health agencies**

# Meaningful Use Requirements

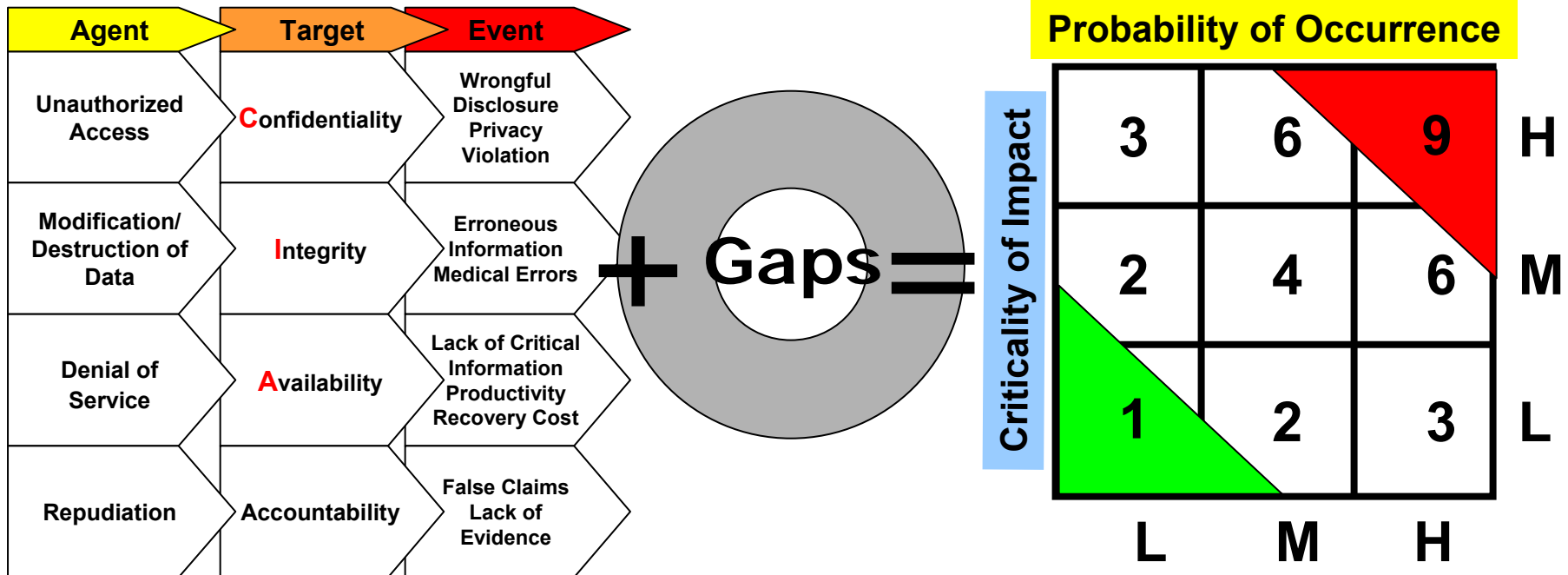
- **Adoption of HIT standards**
  - Including claims and eligibility, using X12 5010 version by January 1, 2012
- **Clinical quality measure reporting**
- **Conduct or review **security risk analysis** per 45 CFR §164.308(a )(1)**
- **Donations of EHR**
  - Include PMS?
  - Provide 1099?
- **Hospital-based physicians**
- **“Meaningful use” attestation**
- **Reassignment of incentives**

# Security Risk Analysis

## Threats

## Vulnerabilities

## Risk

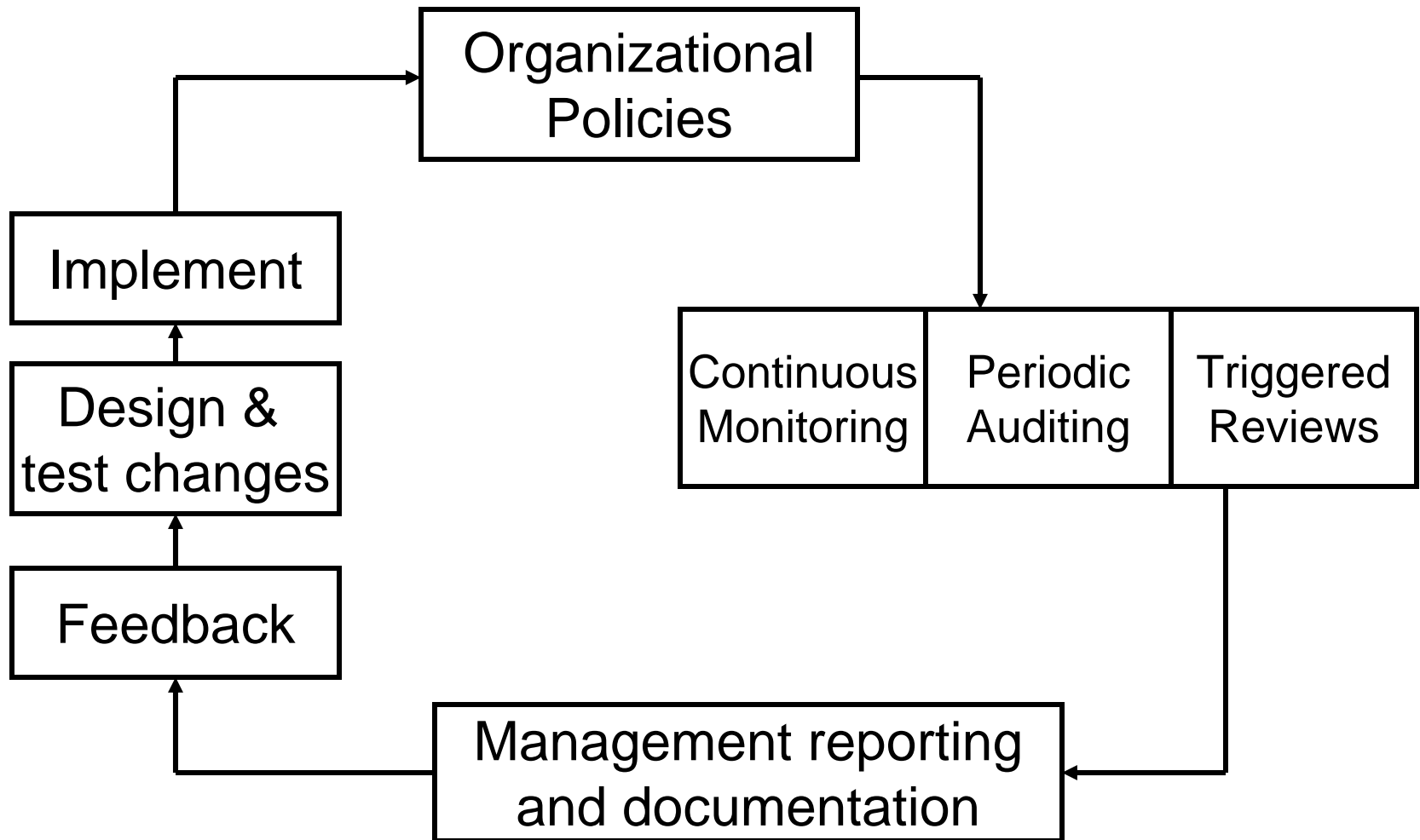


Copyright © 2010, Margret\A Consulting, LLC

Computer Security Division  
Computer Security Resource Center

- SP800-122, Jan. 13, 2009 Draft Guide to Protecting Confidentiality of Personally Identifiable Information (PII)
- SP800-115, Sept. 2008 Technical Guide to Information Security Testing and Assessment
- **SP800-114, Nov. 2007, User's Guide to Securing External Devices for Remote Access**
- **SP800-111, Nov. 2007, Guide to Storage Encryption Technologies for End User Devices**
- **SP800-88, Sept. 2006, Guidelines for Media Sanitization**
- SP800-66 Oct. 2008 Introductory Resource Guide for Implementing HIPAA Security Rule
- SP800-53, Aug. 2009, Recommended Security Controls for Federal Information Systems and Organizations
- SP800-53A, Jul. 2008, Guide for Assessing Security Controls in Federal Information Systems
- **SP800-52, Jun. 2005, Guidelines for Selection and Use of Transport Layer Security (TLS) Implementations**
- SP800-39, Apr. 3, 2008, Draft Managing Risk from Information Systems: An Organizational Perspective

# Implementing Policies



## Blundering past HIPAA

Privacy laws running amok

SUNDAY, January 24, 2010

Recently, at my local Starbucks I asked the barista behind the counter about a medical problem she had that will require surgery. Her answer left me astonished, "Management said I can't talk about my health — it's a HIPAA violation."

This shows what a farce things have become with HIPAA, the 1996 Health Insurance Portability and Accountability Act. Forget for a moment about the kind of management that mandates such nonsense. From the outset, this law has been poorly understood and badly implemented.

### Nurse Pleads Guilty to HIPAA Violation

By Debra Wood, RN, contributor



Privacy provisions of HIPAA are serious and have significant consequences if they are violated, as evidenced in the recent legal proceedings against an Arkansas nurse.

A licensed practical nurse who pled guilty to wrongfully disclosing a patient's health information for personal gain faces a maximum penalty of 10 years imprisonment, a \$250,000 fine or both.

Andrea Smith, LPN, 25, of Trumann, Arkansas, and her husband, Justin Smith, were indicted on federal charges of conspiracy to violate and substantive violations of the Health Insurance Portability and Accountability Act (HIPAA) in December. At the time, Smith worked as a nurse at Northeast Arkansas Clinic, a multispecialty clinic in Jonesboro, Arkansas.

Smith accessed a patient's private medical information on November 28, 2006, according to the indictment. She then shared that information with her husband, who on that same day, called the

patient. Justin Smith reportedly told the patient he intended to use the information against the patient in an upcoming legal proceeding.

Balancing

# Margret Amatayakul

**Margret\A Consulting, LLC**

**Schaumburg, IL 60193**

**Tel. 847-895-3386**

**[margret@margret-a.com](mailto:margret@margret-a.com)**

**[www.margret-a.com](http://www.margret-a.com)**