

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:**
 - **Privacy and Security**
 - **Electronic Health Records and “Meaningful Use”**
- **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

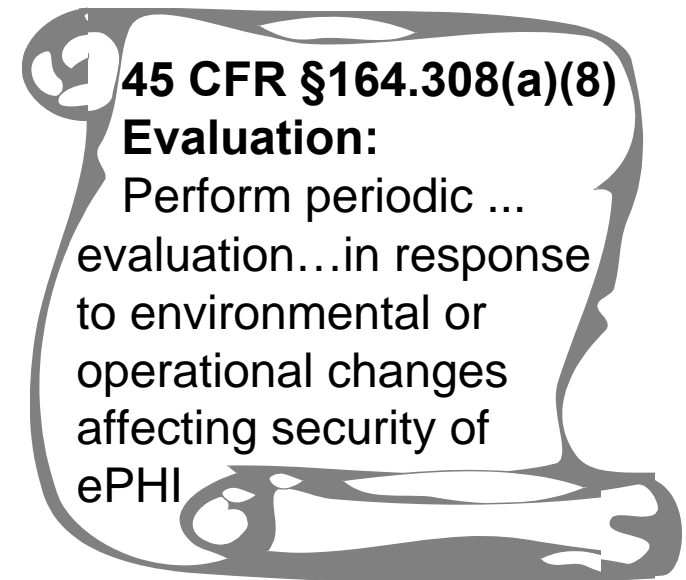
- **Guidance for action consistent with legal, ethical, and organizational requirements**
- **Policies . . .**
 - **Establish goals that procedures and technical measures serve**
 - **Communicate consensus and assign responsibility**
 - **Define enforcement and consequences for violation**
- **Policy 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) on top of old regulations not often complied with**
- **New threats, e.g.,**
 - Identity theft, medical identity theft
 - Economy
 - “Value engineering”
 - HIPAA enforcement
 - “Trusted” third parties
- **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., sending referral information to provider vs. participating in an HIE organization)
- Determine organization's corporate position (e.g., risk averse, risk tolerant)

■ Steps in policy writing

- Draft
- Test
- Introduce, train, reinforce
- Enforce, reinforce

Procedures

Scenario

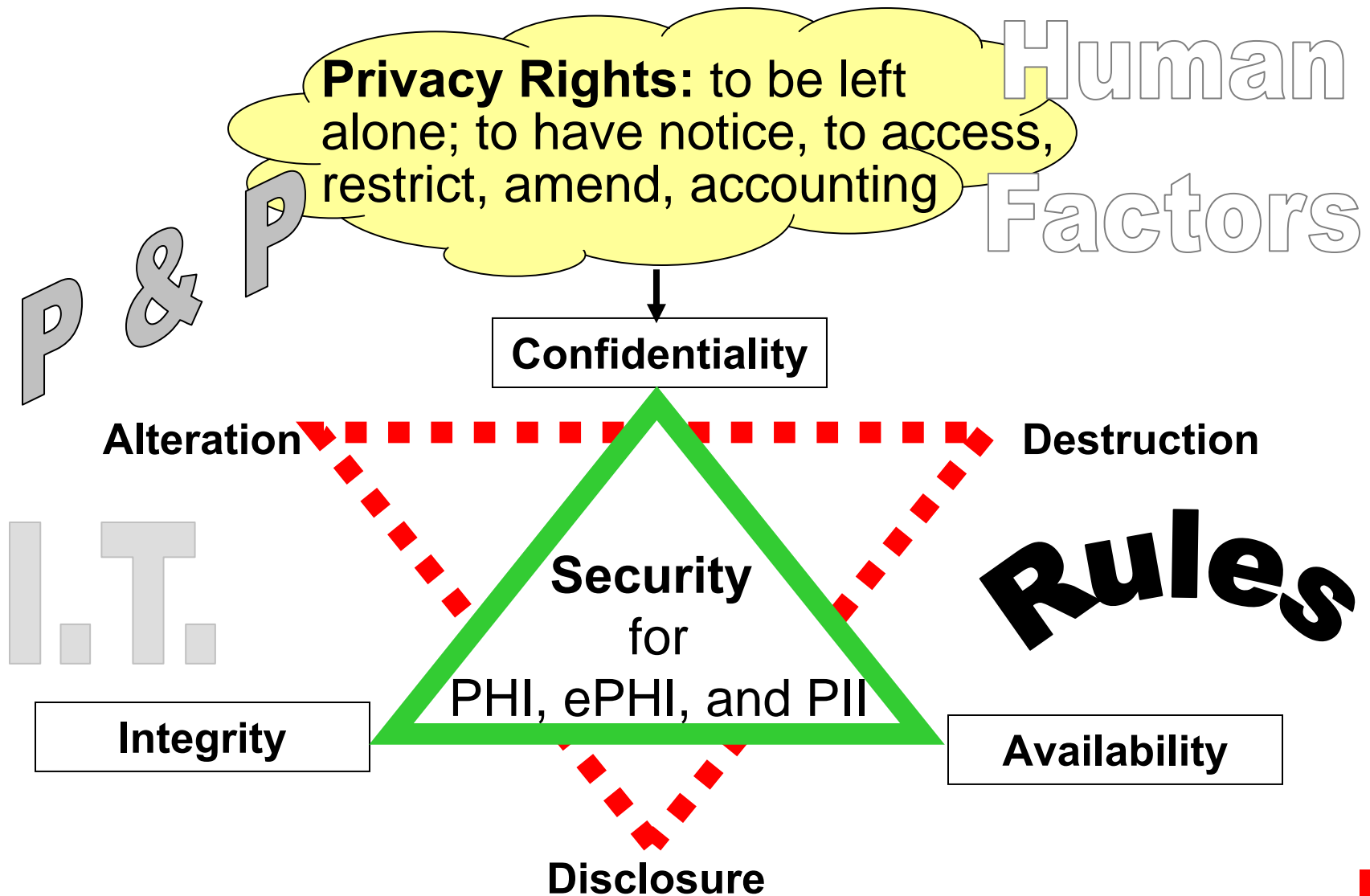
- “I want to review my patient’s record before I enter the exam room”
- “I don’t want to be logging on and off constantly”
- “Every time I log on, I have to click through screens I’ve already looked at”
- Workflow and process changes with HIT must be studied in light of patient care, hassle factors,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

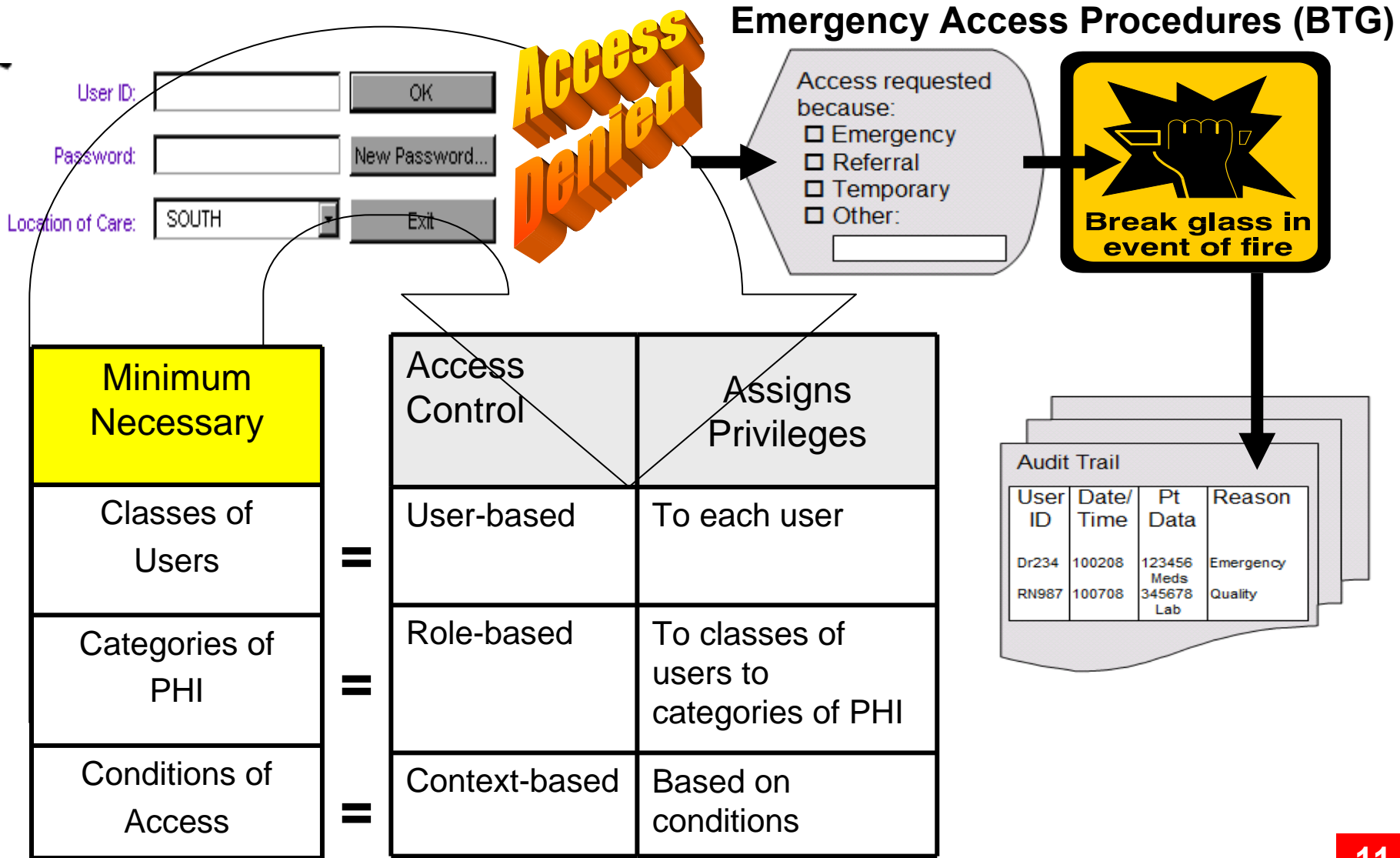
Writing Effective Procedures

- Many organizations adopt the HIPAA implementation specifications as their procedures
- These often are not enough:
 - Accounting for Disclosures
 - Telling a clerk what disclosures NOT to account for is not telling the clerk what disclosures TO account for
 - Incorporating accounting for disclosures requirement in health information management department procedures does not explain to all other departments their obligation to report disclosures that must be tracked
 - Minimum Necessary
 - Requiring the minimum necessary information to be disclosed without explaining precisely what that means is not an effective procedure

Privacy and Security Integration



Access and Audit Controls



New P&P: Breach Notification*

1. Incident occurs. Determine if breach:
 - a. Acquisition, access, use, or disclosure of PHI which compromises the security or privacy of PHI
 - i. **Poses a significant risk of financial, reputational, or other harm to the individual**
 - ii. **De-identified data is excluded**
 - b. Breach discovery starts 60-day clock for notification
2. Determine if PHI:
 - a. Secured (e.g., via encryption), breach notification may not be required
 - b. Unsecured PHI,
3. If unsecured, determine if exception applies that eliminates notification:
 - a. Unintentional access by member of CE or BA workforce
 - b. Inadvertent disclosure to person at same CE or BA and no further use or disclosure in violation of Privacy Rule
 - c. Disclosure where CE or BA believes unauthorized recipient would be unable to retain PHI
4. Delay notification if law enforcement agencies have requested delay where notification may hinder investigation
5. Determine if breach may result in imminent misuse of unsecured PHI, in which case CE should notify individuals by telephone or other means in addition to written notice
6. Send notification letters via first-class mail within 60 days of breach discovery.
 5. Record breach in a log. If fewer than 500 individuals affected, report breach annually
 6. If 500 or more individuals affected, notify HHS: <http://transparency.cit.nih.gov/breach/index.cfm>
 7. If 500 or more live within one state, send a press release to major media outlets
 8. If 10 or more letters returned due to out-of-date or insufficient contact information, provide substitute notice (e.g., email, website notice, major print or broadcast media)
7. Notice must be in plain language and include:
 5. Description of breach, date of breach, and date of discovery
 6. Description of types of information breached
 7. Steps individuals should take to protect themselves
 8. Description of what CE is doing to mitigate harm and protect against further breaches
 9. Contact procedures for individuals to ask questions, including toll-free number, email address, web site, or postal address

New P&P: HITECH Privacy

- **Proposed Rule published July 14, 2010**
- **Several very controversial requirements have generated considerable comment**
- **For your P&P:**
 - **Decide if and when to adopt proposed regulations**
 - **Some may be helpful and unlikely to change, such as for business associates**
 - **Others may have long term impact and could cause future confusion, such as restricting disclosure to payer for cash payment**

Some Tips: Business Associates

- Business associate contract (BAC):
 - Incorporate direct accountability to certain provisions of HIPAA Privacy and Security Rules into BAC; but do not abdicate your responsibility to safeguard PHI
 - Do BACs continue to be needed?
- Incorporate breach notification requirements into BAC – some considerations:
 - Within what timeframe does CE want to receive notification of a breach? Who sets the timeframe? Should there be a uniform timeframe?
 - Do you want to receive notice of all incidents or will you permit BA to determine whether incident is a breach?
 - How do both parties define “incident?”
 - Is BA an agent or a subcontractor? (How are these terms defined by OCR?) If agent, will you request the BA to conduct the notification?
- Consider addressing other concerns more proactively, such as:
 - Prohibit exchanging PHI for remuneration without individual authorization
 - Address requirements for de-identification; or prohibit de-identification
 - Address requirements for BA’s agents and subcontractors
 - Require BA to conduct P&S assessments; require audits of such

Some Tips: Other Potential Changes

- Authorization for future research use and disclosure
- Period of protection for decedent information
- Disclosures about a decedent to family or others involved in care
- FERPA vs. HIPAA
- Minimum necessary as limited data set and applicability to healthcare operations and business associates
- Permission (opt-in) for fundraising; use of service and outcomes data in fundraising
- Timing of NPP revision relative to breach and other proposed changes; need for acknowledgment
- Request for restriction to disclose information to payer when full cash payment – many downstream issues
- Access to copy of health information in electronic format (of patient choosing) and secure transmission vs. access to content maintained in electronic EHR
- Request for provision of electronic copy of PHI to designee vs. authorization
- Authorization for use and disclosure of psychotherapy notes and marketing and subsidized treatment communications
- Hybrid entity definition
- Assessment of remuneration requirements for disclosures, such as to public health
- Disclosures required by law in relationship to patient requested restrictions

Some Tips: Accounting for Disclosures

- **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: the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information
 - Does not mean to turn over you audit logs to the patient
- **Disclosures through an EHR are most likely to occur in an HIE environment, such as when electronically sending CCD or CCR to a physician to who patient is being referred, sending a prescription to the retail pharmacy, sending immunization data to a statewide registry**
- **Are your information systems able to capture a transmission from your EHR?**

Enforcement Considerations for P&P

- **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 (Dec. 31, 2010-?)

- Applicable to your organization?
- If not, should you not watch for warning signs?

Electronic Health Records

- **Mission critical system requiring . . .**
 - Contingency planning and disaster recovery
 - Technical redundancy: servers, network, telecom
- **Use as intended (not just “meaningful use”)**
 - At point of care by clinician
 - To capture and receive structured data
 - And integrate with information from all sources
 - Ensuring data quality, including with ICD-10-CM codes (October 1, 2013) embedded in many HIT applications
 - In support of clinical decision making,
 - Using evidence-based standards of practice to ensure health care quality
 - With appropriate sensitivity levels established
 - And rationale for overriding alerts
 - While enabling and assuring application of professional judgment

Policy Implications for Meaningful Use Requirements

- **Adoption of HIT standards**
 - Including X12 5010 version by January 1, 2012
 - Including Operating Rules forthcoming from the Affordable Care Act
- **What measures; “through EHR”**
- **Exclusions**
- **Donations of EHR**
- **Hospital-based physicians**
- **“Meaningful use” attestation**
- **Reassignment of incentives**
- **Audits of attestation**

CORE Set of Criteria Stage 1

Objectives (Standards)	EP/H	Measures	Application
1. Use CPOE for medication orders directly entered by any licensed health care professional	Both	> 30% of pts w/one medication on EHR med list have ≥ 1 order entered via CPOE	<input type="checkbox"/> CPOE
2. Implement drug-drug and drug-allergy interaction checks	Both	Enabled (Y/N)	<input type="checkbox"/> CPOE/eRx <input type="checkbox"/> CDS
3. Generate and transmit permissible prescription electronically (eRx) (NCPDP)	EP	>40% transmitted via EHR <i>Exclusion if <100 prescriptions written in reporting period</i>	<input type="checkbox"/> eRx
4. Record demographics (or “decline”): <ul style="list-style-type: none"> ■ Preferred language ■ Gender ■ Race ■ Ethnicity ■ Date of birth ■ Date/preliminary cause of death 	Both Both Both Both Both H	> 50% recorded as structured data for all pts	<input type="checkbox"/> PMS <input type="checkbox"/> R-ADT <input type="checkbox"/> EHR Connection
5. Maintain up-to-date problem list of current and active diagnoses (ICD-9-CM or SNOMED)	Both	> 80% all pts have one entry or indication of no problems recorded as structured data	<input type="checkbox"/> Problem List <input type="checkbox"/> Mapping tools
6. Maintain active medication list (RxNorm)	Both	> 80% all pts have at least one entry recorded as structured data	<input type="checkbox"/> Med List <input type="checkbox"/> CPOE/eRx Connection

CORE Set of Criteria Stage 1, Continued

Objectives (Standards)	EP/H	Measures	Application
7. Maintain active medication allergy list	Both	> 80% all pts have at least one entry recorded as structured data	<input type="checkbox"/> Med List <input type="checkbox"/> CPOE/eRx Connection
8. Record/chart changes in V/S: <input type="checkbox"/> Height, weight, blood pressure <input type="checkbox"/> Calculate and display BMI <input type="checkbox"/> Plot and display growth charts (for 2-20 y/o, including BMI)	Both	>50% pts age \geq 2 y/o have height, weight, BP recorded as structured data in EHR <i>Exclusion if pts ht, wt, & BP have no relevance to scope of practice</i>	<input type="checkbox"/> Vital signs <input type="checkbox"/> Trend data
9. Record smoking status \geq 13 y/o	Both	>50% unique pts age \geq 13 y/o recorded as structured data in EHR <i>Exclusion if no pts \geq 13 y/o</i>	<input type="checkbox"/> Social hx
10. Implement one CDS rule relevant to specialty or high clinical priority, w/ability to track compliance w/rule	Both	Implement (Y/N) one CDS rule	<input type="checkbox"/> CDS
11. Provide pts on request electronic copy (CCD or CCR) of: <input type="checkbox"/> Diagnostic test results <input type="checkbox"/> Problem list <input type="checkbox"/> Medication list <input type="checkbox"/> Medication allergy list <input type="checkbox"/> Discharge summary <input type="checkbox"/> Procedures	Both Both Both Both H H	>50% of pts who request, within 3 business days from EHR <i>Exclusion if no pts request electronic copy during reporting period</i>	<input type="checkbox"/> CD, PHR, pt portal, with encryption

CORE Set of Criteria Stage 1, Continued

Objectives (Standards)	EP/H	Measures	Application
12. Provide pts electronic copy of discharge instructions	H	>50% of pts w/EHR who request <i>Exclusion if no pts request electronic copy during reporting period</i>	<input type="checkbox"/> CD, PHR, pt portal ,with encryption
13. Provide pts clinical summaries (CCD or CCR) for each office visit	EP	>50% of all visits w/EHR w/in 3 business days <i>Exclusion if EP has no office visits</i>	<input type="checkbox"/> CD, PHR, pt portal, with encryption
14. Ability to exchange key clinical information w/providers & pt authorized entities (CCD or CCR), e.g., <input checked="" type="checkbox"/> Problem list <input checked="" type="checkbox"/> Medication list <input checked="" type="checkbox"/> Medication allergies <input checked="" type="checkbox"/> Diagnostic test results	Both	At least one test of capacity (Y/N)	<input type="checkbox"/> CD, PHR, provider portal, with encryption <input type="checkbox"/> HIE
15. Protect electronic health information created or maintained by EHR through implementation of appropriate technical capabilities	Both	Conduct or review a security risk analysis per HIPAA and implement security updates as necessary and correct identified security deficiencies (Y/N)	
16. Report clinical quality measures (CQM) to CMS or State	Both	2011: Attest to aggregate numerator, denominator, exclusions	<input type="checkbox"/> Report writer <input type="checkbox"/> Select from all measures

MENU Set of Criteria Stage 1

Objectives (Standards)	EP/H	Measures	Application
17. Implement drug-formulary checks	Both	Enabled (Y/N) with access to at least one internal or external formulary for reporting period	<input type="checkbox"/> eRx <input type="checkbox"/> PBM data feed (e.g., SureScripts)
18. Incorporate clinical lab test results (in +/- or numerical format) into EHR as structured data	Both	>40% of lab test results ordered w/EHR in reporting period <i>Exclusion if no lab tests in +/- or numerical format</i>	<input type="checkbox"/> LIS <input type="checkbox"/> Trend data
19. Generate lists of pts by specific conditions for QI, reduction of disparities, research, or outreach	Both	Generate at least one report (Y/N) listing pts with a specific condition	<input type="checkbox"/> Report writing
20. Use EHR to identify pt-specific education resources and provide if appropriate	Both	> 10% of all pts provided pt-specific education resources	<input type="checkbox"/> Pt portal <input type="checkbox"/> Education resource integrated w/EHR
21. EP or H who receives a patient from another setting of care or provider of care or believes an encounter is relevant should perform medication reconciliation	Both	>50% of transitions of care w/EHR <i>Exclusion if EP or H not recipient of transitions</i>	<input type="checkbox"/> CPOE <input type="checkbox"/> Pharmacy IS <input type="checkbox"/> E-MAR <input type="checkbox"/> Medication reconciliation utility
22. Capability to submit electronic syndromic surveillance data to public health & actual submission	Both	One test (Y/N) of capacity and follow up submission (unless no capacity) <i>Exclusion if does not collect reportable data on pts</i>	<input type="checkbox"/> Report writing <input type="checkbox"/> Transmission routine <input type="checkbox"/> HIE

MENU Set of Criteria Stage 1, Continued

Objectives (Standards)	EP/H	Measures	Application
23. EP or H who transitions pt to another care setting or refers pt to another provider provide summary of care record for each transition or referral	Both	>50% of transitions of care and referrals w/EHR <i>Exclusion if no transfer of care</i>	<input type="checkbox"/> Report writing <input type="checkbox"/> CCD/CCR <input type="checkbox"/> Encryption
24. Capability to submit electronic data to immunization registries or Immunization Information Systems and actual submission in accordance with applicable law and practice	Both	One test (Y/N) of capacity & follow up submission (unless no capacity) <i>Exclusion if immunizations not administered</i>	<input type="checkbox"/> Report writing <input type="checkbox"/> Transmission routine <input type="checkbox"/> HIE
25. Capability to submit electronic data on reportable lab results to public health and actual submission	H	One test (Y/N) of capacity and follow up submission <i>Exclusion if public health has no capacity to receive</i>	<input type="checkbox"/> Report writing <input type="checkbox"/> Transaction <input type="checkbox"/>
26. Record advance directives for pts ≥ 65 y/o	H	>50% of pts status recorded in EHR <i>Exclusion if no pts ≥ 65 y/o</i>	<input type="checkbox"/> R-ADT <input type="checkbox"/>
27. Send reminders to pts per pt preference for preventive/follow up care	EP	>20% of pts ≥ 65 y/o, or ≤ 5 y/o sent via EHR reminder for reporting period <i>Exclusion if no pts in ages</i>	<input type="checkbox"/> Report writing <input type="checkbox"/> PHR, pt portal, with encryption
28. Provide pts timely electronic access to lab results, problem list, med list, allergies within 4 business days of information being available	EP	>10% of all pts provided timely electronic access subject to discretion to withhold information	<input type="checkbox"/> CD, PHR, pt portal, with encryption

Patient Summary Record Standards

- ASTM CCR is a core data set that supports referrals, transfers, and other uses by different providers
- HL7 CDA is a document markup specification providing a multi-level architecture accommodating varying degrees of markup granularity
- CCR + CDA = CCD may be incorporated into a data exchange by reference to a PDF (in HL7 V2.x) or embedded as an XML format (in HL7 V3)

Continuity of Care Record

Date Created: Fri Jan 20, 2006 at 04:34 PM UTC-06:00
 From: Levi A Wright (Provider)
 To:
 Purpose: Transfer of Patient Data

Patient Demographics

Name	Date of Birth	Gender	Identification Numbers	Address / Phone
Levi A Campbell	Date of Birth: 7/26/1972 12:00:00 AM	female	Social Security Number: 652-07-4756	Home: 327 Farm Road Round Rock, TX Home: (320)804-

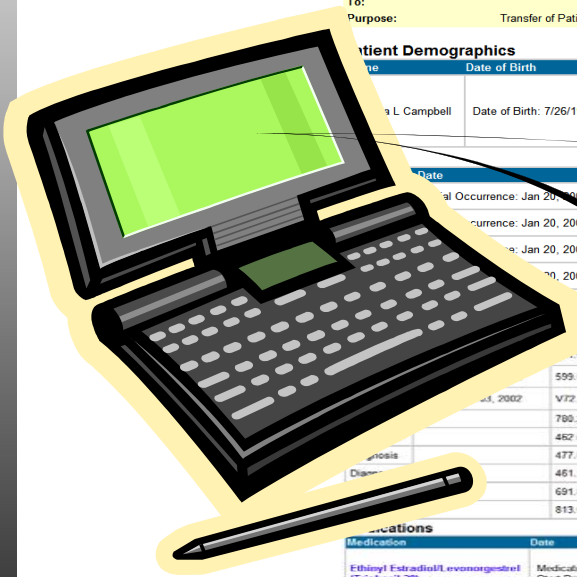
Date	Code	Description	Reaction	Source
Occurrence: Jan 20, 2006			- Moderate	Levi A Wright
Occurrence: Jan 20, 2006			- Severe	Levi A Wright
Jan 20, 2006			- Mild	Levi A Wright
Jan 20, 2006			- Moderate	Levi A Wright

Description	Status	Source
Other specified visual disturbance (ICD9-CM)	Chronic	Bryce FF Miller
Acute sinusitis, maxillary (ICD9-CM)	Active	Bryce FF Miller
UTI (ICD9-CM)	Active	Jackie Enders
Well woman exam (ICD9-CM)	Active	Jackie Enders
Fainting spells (ICD9-CM)	Active	Jackie Enders
Pharyngitis (ICD9-CM)	Active	Jackie Enders
Allergies (ICD9-CM)	Active	Jackie Enders
Sinusitis, unspecified (ICD9-CM)	Active	Jill Byrd
Atopic dermatitis (ICD9-CM)	Active	Jill Byrd
Closed fracture of head of radius (ICD9-CM)	Active	Bryce FF Miller

Medication	Date	Status	Form	Strength	Quantity	SIG	Indications	Instruction	Refills	Source
Ethinyl Estradiol/Evonorgestrel (Triphasil 28)	Medication Start Date: Sep 03, 2002	Active	Tablet	1.28	tablet	Oral		as directed, as directed		Jackie Enders
Ethinyl Estradiol/Evonorgestrel (Triphasil 28)	Medication Start Date: Sep 03, 2002	Active	Tablet	1.28	tablet	Oral		as directed, as directed		Jackie Enders

```

<?xml version="1.0" ?>
- <ContinuityOfCareRecord xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns=""
  <CCRDocumentObjectID>e-Mds_DocID_1236144204</CCRDocumentObj
- <Language>
  <Text>English</Text>
</Language>
<Version>V1.0</Version>
- <DateTime>
  <ExactDateTime>2006-01-20T16:34:41-06:00</ExactDa
  </DateTime>
- <Patient>
  <ActorID>1001</ActorID>
  </Patient>
- <From>
  <ActorLink>
    <ActorID>AA00</ActorID>
    <ActorRole>
      <Text>Provider</Text>
    </ActorRole>
  </ActorLink>
</From>
- <Purpose>
  <Description>
    <Text>Transfer of Patient Data</Text>
  </Description>
</Purpose>
  
```

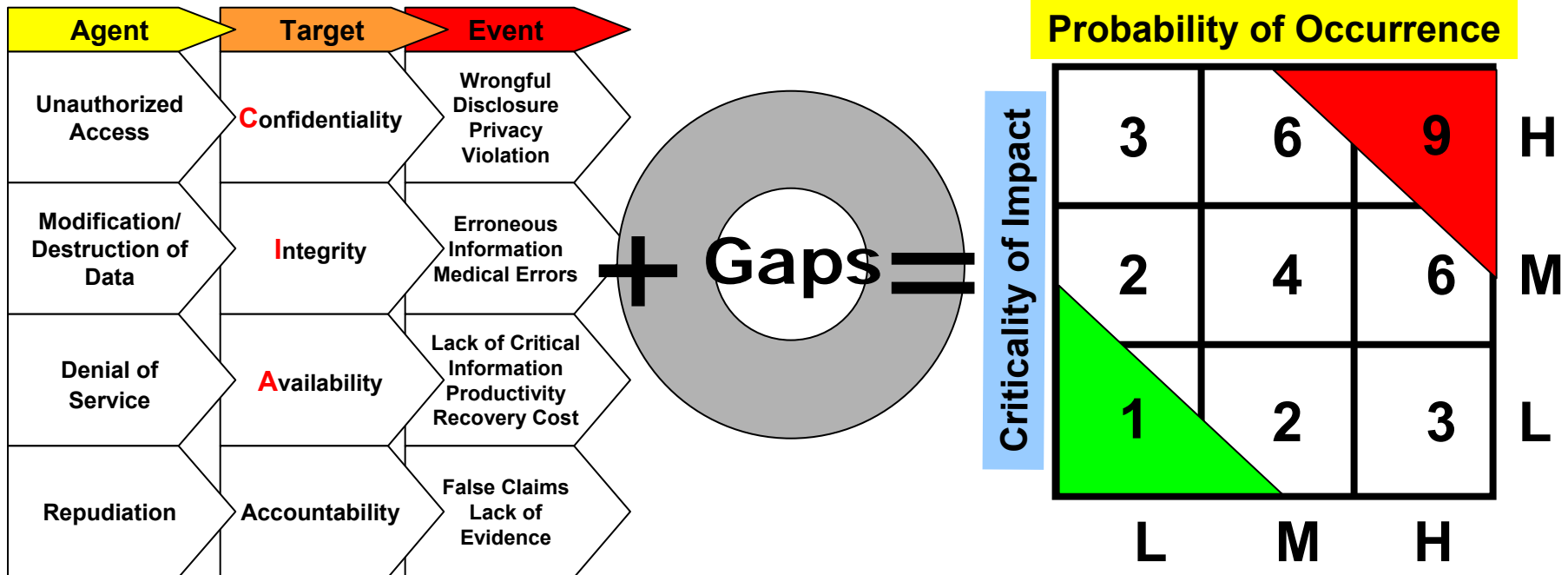


Security Risk Analysis

Threats

Vulnerabilities

Risk

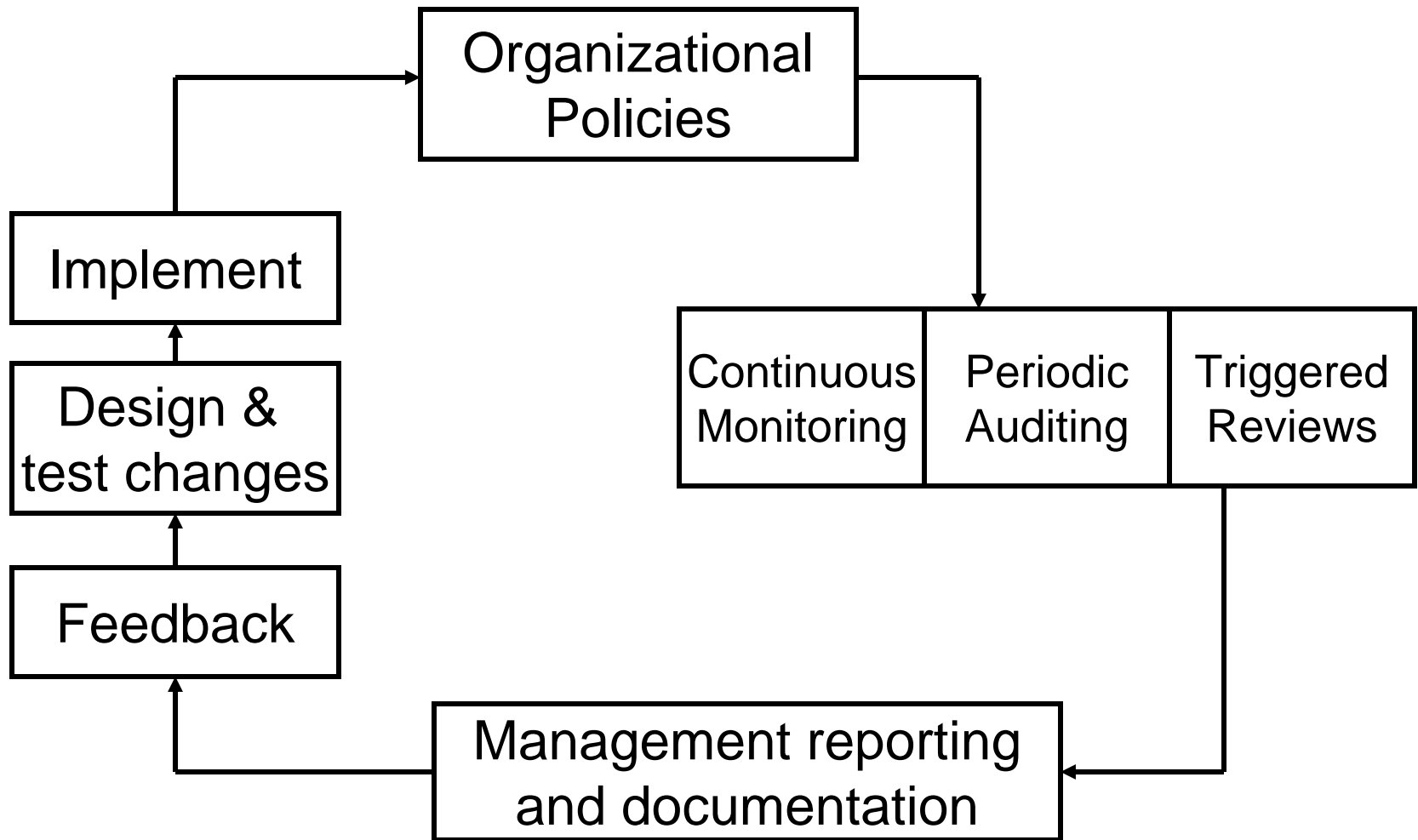


Computer Security Division

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 medical nurse who pled guilty to wrongfully disclosing a patient's private 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.

Balance

Margret Amatayakul

Margret\A Consulting, LLC

Schaumburg, IL 60193

Tel. 847-895-3386

margret@margret-a.com

www.margret-a.com