# Technical Security Challenges in Earning Meaningful Use Incentives for EHR

**Margret Amatayakul,**

MBA, RHIA, CHPS, CPHIT, CPEHR, FHIMSS

**Margret\A Consulting, LLC**

# Agenda

- What is required for M.U.
  - Measures
  - Certification Criteria
- Challenges
  - Risk analysis
  - Access controls
  - Audit controls
  - Encryption

# WHAT IS REQUIRED?

# CMS Risk Analysis Measures

| Stage 1 Objective | Stage 1 Measure | Stage 2 Objective | Stage 2 Measure |
|---|---|---|---|
| Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities | Conduct or review a security risk analysis per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process | Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities. | Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308 (a)(1), including addressing the encryption/security of data at rest and implement security updates as necessary and correct identified security deficiencies as part of its risk management process |

# ONC Standards and Criteria

- **Stage 1**
  - Access control
  - Emergency access
  - Automatic logoff
  - Audit log
  - Integrity
  - Authentication
  - General encryption
  - Encryption when exchanging electronic health information
  - Optional: Acctg for disclosures
- **Stage 2**
  - Authentication, access control, authorization
  - Auditable events and tamper-resistance
  - Audit reports
  - Amendments
  - Automatic logoff
  - Emergency access
  - End-user device encryption
  - Integrity
  - Optional: Acctg for disclosures
  - View, download, & transmit with activity history log
  - Secure messaging

# CHALLENGES: RISK ANALYSIS

# Risk Analysis Measure

- Conduct or review a security risk analysis of certified EHR technology and implement updates as necessary at least once prior to the end of the EHR reporting period and attest to that conduct or review. The testing could occur prior to the beginning of the first EHR reporting period. However, a new review would have to occur for each subsequent reporting period.
- A security update would be required if any security deficiencies were identified during the risk analysis. A security update could be updated software for certified EHR technology to be implemented as soon as available, changes in workflow processes or storage methods, or any other necessary corrective action that needs to take place in order to eliminate the security deficiency or deficiencies identified in the risk analysis.

# ONC Myths on Risk Analysis

- **http://www.healthit.gov/providers-professionals/top-10-myths-security-risk-analysis**

9. Before I attest for an EHR incentive program, I must fully mitigate all risks.

- False. The EHR incentive program requires correcting any deficiencies (identified during the risk analysis) during the reporting period, as part of its risk management process.

# Security Audit, Assessment, Risk Analysis

- **Audit** = overview of security systems and processes to determine *existence of controls*
- **Assessment** = identification of vulnerabilities in security systems and processes to *assess controls*
- **Risk analysis** = couples identification of vulnerabilities with known or potential threats to describe the probability (or likelihood) that a threat would exploit a vulnerability and to assess the criticality of impact (or level of harm) to *select and implement most effective controls*
- **Risk analysis tends to be more proactive; where audit and assessment are more retrospective**

# Key Components of Risk Analysis

**Security Audit**

| HIPAA Security Standard (§ Citation) Implementation Specification (Required/ Addressable) | Vulnerabilities: Policy, Procedure, Documentary Evidence | Vulnerabilities: Guiding Questions (This guidance is drawn from NIST, ONC, ISO, and other security standards) | Vulnerabilities: Survey Results # | Vulnerabilities: Survey Results Level of Risk | Vulnerabilities: Observed Practice | Criticality | Potential Threats: Description of potential threats | Potential Threats: Probability | Risk Score | Risk Management: Recommended Control |
|---|---|---|---|---|---|---|---|---|---|---|
| **ADMINISTRATIVE SAFEGUARDS** | | | | | | | | | | |
| **1. Security Management Process §164.308(a)(1)** | | | | | | | | | | |
| 1.1 Risk Analysis (R)<br><br>Meaningful Use §495.6(d)(15)(ii) and (f)(14)(ii) | | 1.1.1 Has executive management's risk position/level of residual risk tolerance with respect to information security been determined? | | | | | | | | |
| | | 1.1.2 Have threat sources for all aspects of information security been identified? | | | | | | | | |
| | | 1.1.3 Is there intelligence available concerning known information security vulnerabilities of all types maintained? | | | | | | | | |
| | | 1.1.4 Has an information security risk analysis been documented for executive management and board that supports the identification of strategies to reduce risk to what the organization deems an acceptable residual risk? | | | | | | | | |
| 1.2 Risk Management (R) | | 1.2.1 Is there a process to enable ongoing risk analysis and management that | | | | | | | | |

# Threat Inventory

- Accidental acts
  - –Incidental disclosures
  - –Errors and omissions
  - –Proximity to risk areas
  - –Work stoppage
  - –Equipment malfunction
- Deliberate acts
  - –Inattention/inconsistency
  - –Misuse/abuse of privileges
  - –Fraud
  - –Theft/embezzlement
  - –Extortion
  - –Vandalism
  - –Computer crime
- Environmental acts
  - –Contamination
  - –Fire
  - –Flood
  - –Weather
  - –Power
  - –HVAC

**For each act:**

- Description
  - Internal staff
  - Telecommuters
  - Temps/locums
  - Business associates
  - External attackers
  - Public accessibility
- Occurrence
  - Here
  - Other healthcare
  - Other industry
- Frequency
  - Negligible
  - Low
  - Medium
  - High
  - Extreme
- Ability
  - Access
  - Knowledge
  - Motivation
- Predictability
  - Forewarning
  - No warning
- Characteristics
  - Fast onset
  - Widespread
  - Long duration
  - Slow
- Controls
  - Preventative
  - Deterrent
  - Detective
  - Reactive
  - Recovery

| Probability of Occurrence | High | Medium | Low |
|---|---|---|---|
| Has it happened before: | | | |
| ■ Here? | | | |
| ■ Other health care? | | | |
| ■ Other industries? | | | |
| How frequently does it occur: | | | |
| ■ Here? | | | |
| ■ Other health care? | | | |
| ■ Other industries? | | | |
| Does threat source have: | | | |
| ■ High access, knowledge, motivation? | | | |
| ■ Predictability, forewarning? | | | |
| ■ Known speed of onset, spread, duration? | | | |
| Are controls available to: | | | |
| ■ Prevent? | | | |
| ■ Deter? | | | |
| ■ Detect? | | | |
| ■ React? | | | |
| ■ Recover? | | | |

| Criticality of Impact | High | Medium | Low |
|---|---|---|---|
| What harm does it do to patient or individual? | | | |
| Does it cause reportable breach of confidentiality? | | | |
| Is there risk of a complaint &/or lawsuit? | | | |
| Does it reduce productivity? | | | |
| Does it cause loss of revenue? | | | |
| What is cost to remediate all aspects? | | | |
| Does it impact licensure/accreditation? | | | |
| Could there be a public relations issue? | | | |
| Does it affect consumer confidence, goodwill, competitive advantage? | | | |

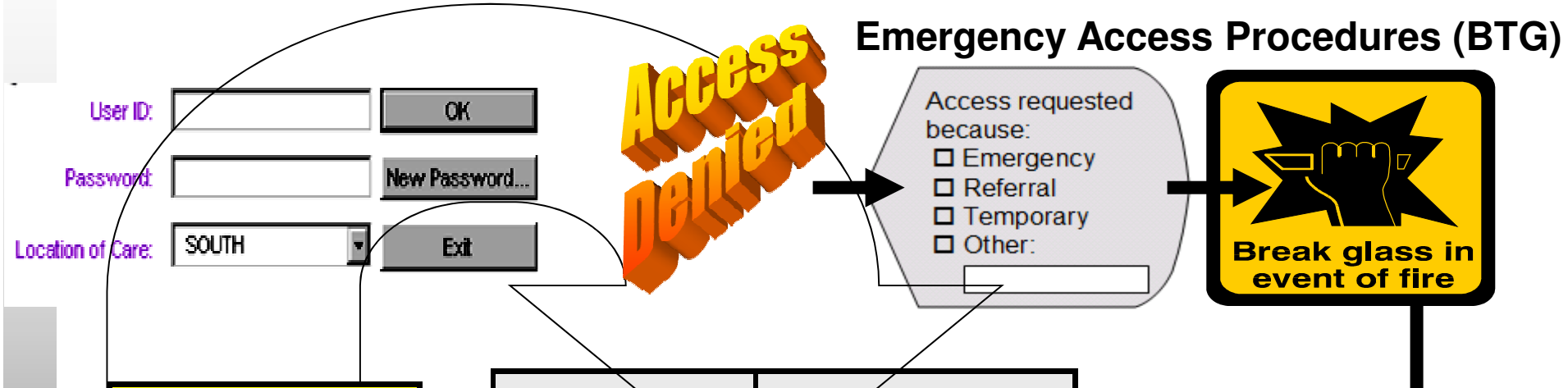
# CHALLENGES: TECHNICAL CONTROLS

# Authentication, Access Control, & Authorization

- Stage 2:
  - Verify against a unique identifier(s) (e.g., username or number) that a person seeking access to electronic health information is the one claimed; and
  - Establish the type of access to electronic health information a user is permitted based on the unique identifier…and the actions the user is permitted to perform with the EHR…
- Stage 1 (Authentication): Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information

| Authentication Strength | Type of Technology Affording This Level of Strength | Examples of Use in Healthcare |
|---|---|---|
| **Demonstration of intent to sign** | Digitized signature (e.g., signature pad on credit card machine at a grocery store) | - Acknowledgment of Receipt of Notice of Privacy Practices |
| **Something only you know** | Password (passwords can be made stronger by using more characters, special characters, no words, etc.) | - Access to a portal<br>- User log on to EHR |
| **Something only you have** | Token (Hardware or software in a variety of strengths; may be used with a password as two-factor authentication) | - MD remote access to EHR<br>- Nurse access to narcotics cabinet |
| **Something about you** | Biometric (e.g., fingerprint, retinal scan; may also be used in combination with a password for two-factor authentication) | - User log on to EHR |
| **Someone you know** | Digital signature (provides for encryption and non-repudiation by use of a digital certification process (trusted authority) | - Access to HIE<br>- E-Rx controlled substances |
| **Combination of two or more** | Combining two or more strengthens process by at least one level | - Access to HIE |

# Access and Audit Controls




| Minimum Necessary | | Access Control | Assigns Privileges |
|---|---|---|---|
| Classes of Users | = | User-based | To each user |
| Categories of PHI | = | Role-based | To classes of users to categories of PHI |
| Conditions of Access | = | Context-based | Based on conditions |

# Access Controls

- Preamble to the Privacy Final Rule, Federal Register Vol. 67, No. 157, August 14, 2002, Page 53194:

> However, an incidental use or disclosure that occurs as a result of a failure to apply reasonable safeguards or the minimum necessary standard, where required, is not a permissible use or disclosure and, therefore, is a violation of the Privacy Rule. For example, a hospital that permits an employee to have unimpeded access to patients' medical records, where such access is not necessary for the employee to do her job, is not applying the minimum necessary standard and, therefore, any incidental use or disclosure that results from this practice would be an unlawful use or disclosure under the Privacy Rule.

# Issues with Access Controls

- Who is provider of record?
- How do consultants and others become providers of record?
- How do nurses and other clinicians become associated with the record?
- How is access controlled for exceptions to ancillary staff (lab techs, coders, billers)?
- Philosophical issues with “controls”
- Reasons for BTG
- Auditing BTG

# Audit Logs: Recording

## M.U. Stage 1

- Record actions
  - Date
  - Time
  - Patient identification
  - User identification
- When information is:
  - Created
  - Modified
  - Accessed
  - Deleted
- Which action by whom

## M.U. Stage 2

- **Record actions as specified in ASTM E2147:**
  - 7.2 Date and time of event
  - 7.3 Patient identification
  - 7.4 User identification
  - 7.6 Type of action:
    - Additions
    - Deletions
    - Changes
    - Queries
    - Print
    - Copy
  - 7.7 Identification of patient data that is accessed (optional)
- Record audit log status (enabled/disabled)
- Record encryption status
- Audit log protection
- Audit log detection of alteration

# Audit Reports

- **Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the data specified in the standards (see previous)**
- **Issues:**
  - **Storage**
  - **Analysis**
    - **Software**
      - –False positives and false negatives
      - –Trained staff/time to interpret
    - **Follow up**

# End-User Device Encryption

- EHR that is designed to locally store electronic health information on end-user devices must encrypt the information on such devices after use of the EHR stops
  - Any encryption algorithm identified by NIST as an approved security function in Annex A of FIPS Publication 140-2
  - EHR must be set by default to perform this capability; and
    - Unless this configuration cannot be disabled by any user, the ability to change the configuration must be restricted to a limited set of identified users
- EHR is designed to prevent electronic health information from being locally stored on end-user devices after use of EHR on those devices stops

# Integrity

- Create a message digest in accordance with the standard equal to or greater than SHA-1 as specified by the NIST in FIPS 180-4 (March 2012)
- Verify in accordance with the standard upon receipt of electronically exchanged health information that such information has not been altered

# Integrity Note:

- *Guidance Specifying the Technologies and Methodologies that Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (issued April 27, 2009 for Breach Notification) references FIPS 140-2, *which includes*:
  - NIST 800-52 (TLS)
  - NIST 800-77 (IPsec VPNs
  - NIST 800-113 (SSL)
  - And may include others which are FIPS 140-2 validated
- FIPS 140-2 address more security functions than only the Secure Hash Standard (SHS)
- FIPS 140-2 addresses:
  - Symmetric Key
  - Asymmetric Key
  - Secure Hash Standard (FIPS 180-4)
  - Random Number Generators
  - Message Authentication, including SHS

# Margret Amatayakul

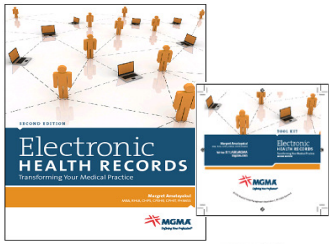
Margret\A Consulting, LLC
Schaumburg, IL 60193
Tel. 847-895-3386
margret@margret-a.com
www.margret-a.com

# References & Resources

## Margret Amatayakul, MBA, RHIA, CHPS, CPHIT, CPEHR, FHIMSS

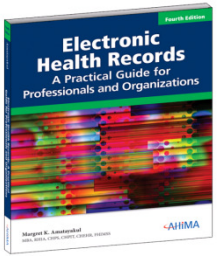

*Handbook for HIPAA-HITECH Security*, Chicago: American Medical Association, Second Edition, 2013, includes CD with tools

- https://catalog.ama-assn.org/Catalog/



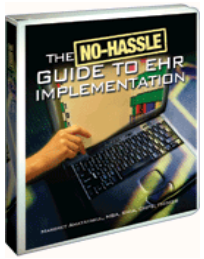

*Electronic Health Records: Transforming Your Medical Practice*, Second Edition, Denver: Medical Group Management Association, 2010; CD Toolkit available

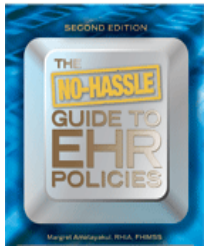
- www.mgma.org

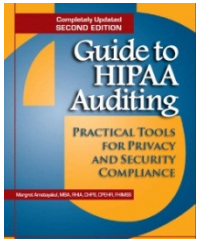



Electronic Health Records: A Practical Guide for Professionals and Organizations, Fifth Edition, Chicago: American Health Information Management Association, 2012

- www.ahima.org



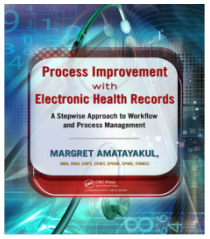




*The No-Hassle Guide to EHR Implementation*, 2007

*The No-Hassle Guide to EHR Policies*, 2010

*Guide to HIPAA Auditing: Practical Tools for Privacy and Security Compliance*, 2nd Ed, 2009

Published by HCPro, Inc. • www.hcmarketplace.com




Process Improvement with Electronic Health Records: A Stepwise Approach to Workflow and Process Management, Boca Raton, FL: CRC Press, 2012

- www.crcpress.com