

**AUDITING TECHNIQUES TO ASSESS  
FRAUD RISKS IN ELECTRONIC  
HEALTH RECORDS**

## OBJECTIVE

Increase your IT vocab so that you can assess the risks related to your audits of EHRs and/or EHR related data

## AGENDA

What is an EHR?

challenges facing ALL auditors and assessing risks

copy&paste / cloning

electronic signatures

versioning

access (password) controls

logging

## BACKGROUND

2009 American Recovery &  
Reinvestment Act

HITECH ACT

electronic health  
records

meaningful use

incentive payments \$\$\$



IT'S AN EHR! DUH!

HITECH ACT

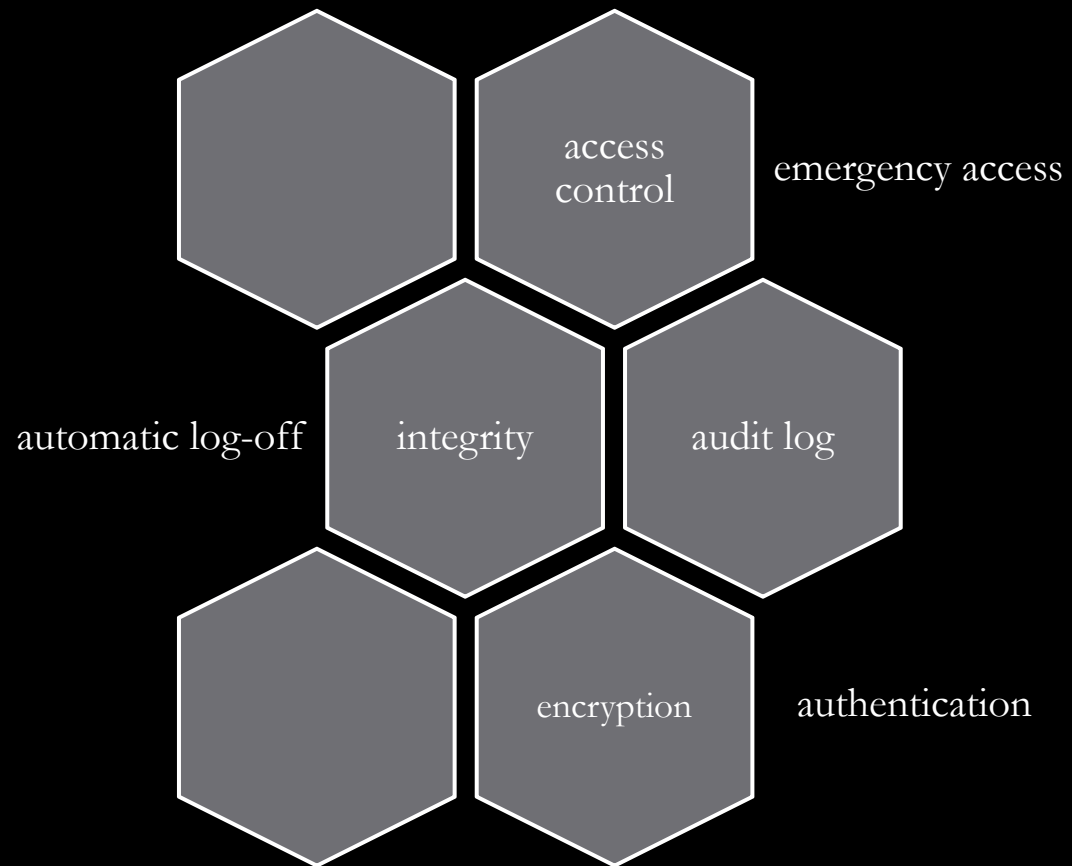
○ electronic health record

meaningful use/incentive payments

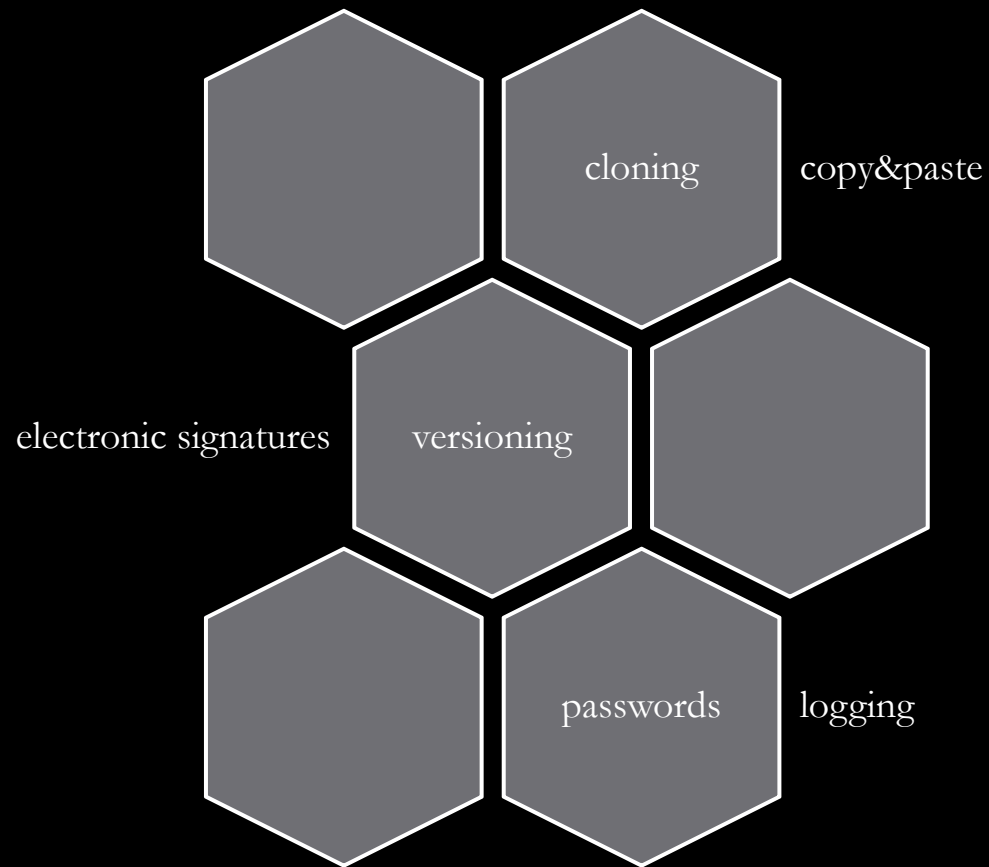
improve health care



# SECURITY REQUIREMENTS



# CHALLENGES



## POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

Security Objective	LOW	MODERATE	HIGH
<p style="text-align: center;">Confidentiality</p> <p>Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.</p>	<p>The unauthorized disclosure of information could be expected to have a <i>limited adverse effect</i> on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a <i>serious adverse effect</i> on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a <i>severe or catastrophic</i> adverse effect on organizational operations, organizational assets, or individuals.</p>
<p style="text-align: center;">Integrity</p> <p>Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.</p>	<p>The unauthorized modification or destruction of information could be expected to have a <i>limited adverse effect</i> on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a <i>serious adverse effect</i> on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a <i>severe or catastrophic adverse effect</i> on organizational operations, organizational assets, or individuals.</p>
<p style="text-align: center;">Availability</p> <p>Ensuring timely and reliable access to and use of information.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a <i>limited adverse effect</i> on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a <i>serious adverse effect</i> on organizational operations, organizational assets, or individuals.</p>	<p>The disruption of access to or use of information or an information system could be expected to have a <i>severe or catastrophic adverse effect</i> on organizational operations, organizational assets, or individuals.</p>



## CLONING

09.24.2012 President's Warning  
Letter

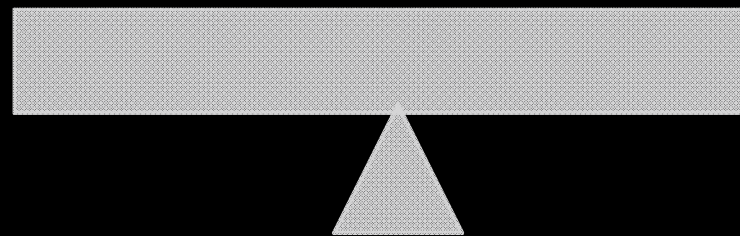
02.13.13 AHIMA acknowledged  
non-compliance remained an issue

- make me the author
- copying vital signs
- templates

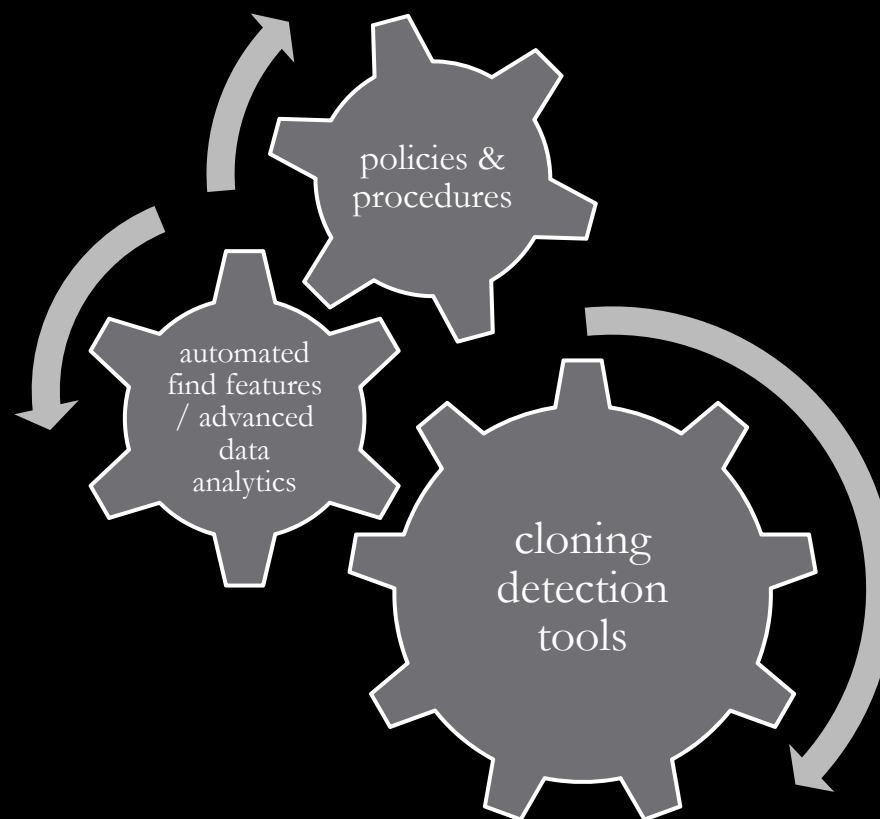
## AUDIT CHALLENGES: CLONING

Document  
Review

Legitimate Rate  
of Frequency



## RISK ASSESSMENT: CLONING



## PASSWORDS



EHR Audit Findings



What type of lock do you have?

## PASSWORDS



minimum 8 characters, complex



unable to reuse passwords



prohibit group/shared passwords

## RISK ASSESSMENT: PASSWORDS



start with p&ps

crack the sam file

test: ask someone to reset his/her password

# EHR SIGNATURES


digitized signatures

button, PIN, Biometric

digital signature

# DIGITAL SIGNATURE

Signature Properties

 Signature is VALID, signed by John B. Harris <jbharris@adobe.com>.




Summary | Document | Signer | Date/Time | Legal

Signed by: John B. Harris <jbharris@adobe.com> [Show Certificate...](#)

Reason: Not available

Signing Time: 2010/06/09 11:19:46 -05'00' Location: Not available

Validity Summary

-  The Document has not been modified since this signature was applied.
-  The document is signed by the current user.
-  The signature includes an embedded timestamp. Timestamp time: 2010/06/09 11:19:50 -05'00'

Signature was created using Adobe Acrobat 9.3.2.  
Signature was validated as of the secure (timestamp) time:  
2010/06/09 11:19:50 -05'00'

[Close](#) [Validate Signature](#)



**RISK ASSESSMENT: EHR  
SIGNATURES**

Multiple, dual, co-signatures

On behalf of another

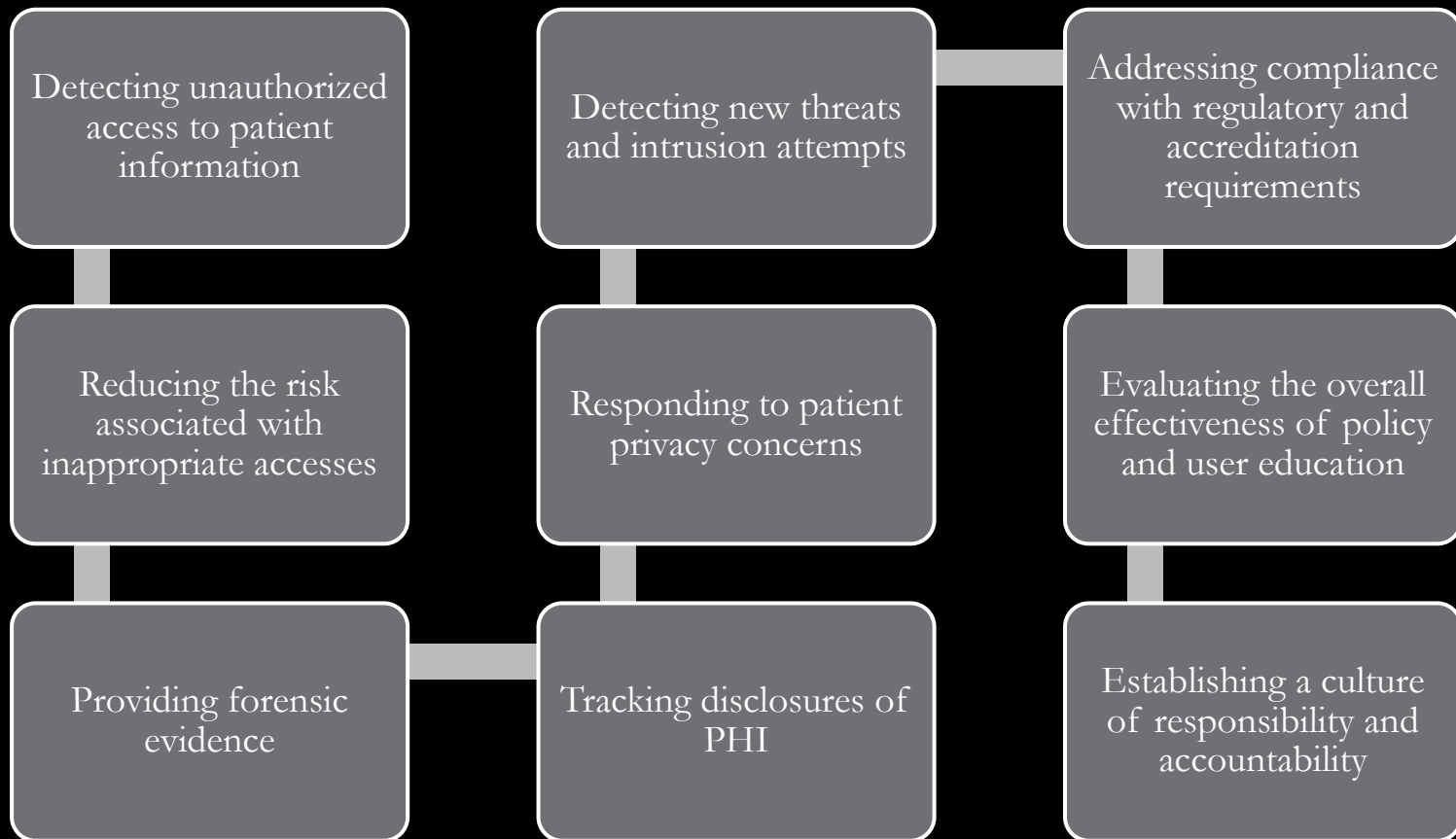
Auto-attestation

Batch signing

Scribes/ Assistants

Amendments, corrections, retractions, deletions

## 9 REASONS WHY LOGGING IS AN AUDITOR'S BFF



## AUDIT LOGGING CONTEXT

name

application

workstation id

event (e.g.  
modification,  
deletion, etc.)

## HIPAA SECURITY RULE

**Section 164.308(a)(1)(ii)(c)**, Information system activity review (required), which states organizations must "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."

**Section 164.312(1)(b)**, Audit controls (required), which states organizations must "implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

## EHR VERSIONING

What's the latest version? How many?

When was it installed?

Are there similar features for a Mac vs. Windows? Tablets? Desktops? iPhones?

## HITECH PENALTIES

Tier A -offender didn't realize he or she violated the Act and would have handled the matter differently if he or she had. **\$100 fine** for each violation, cannot exceed \$25,000 for the calendar year.

Tier B -violations due to reasonable cause, but not "willful neglect." The result is a \$1,000 fine for each violation, and the fines cannot exceed \$100,000 for the calendar year.

Tier C - violations due to willful neglect that the organization ultimately corrected. The result is a \$10,000 fine for each violation, and the fines cannot exceed \$250,000 for the calendar year.

Tier D -violations of **willful neglect** that the organization did not correct. The result is a **\$50,000 fine for each violation**, and the fines cannot exceed \$1,500,000 for the calendar year.

**QUESTIONS/COMMENTS?**