SESSION TWO:

How Secure is Your PHI?

Best Practices in Breach Prevention
- Minimizing the Risk of a Breach

Objectives:

HIPAA Privacy and Security

- Understand the 2009 and 2013 Modifications
- Conduct security risk analysis to identify threats and risks.
- Document and monitor security measures
- Develop a risk mitigation plan

Best Practices in Breach Prevention

- Develop appropriate security measures
- Monitor compliance with required measures
- Comply with reporting requirements

Today's Agenda

- A Look at the Security Rule
- Security Risk Analysis
- Breaches and Notification
- OCR Audit Program

What is Security?

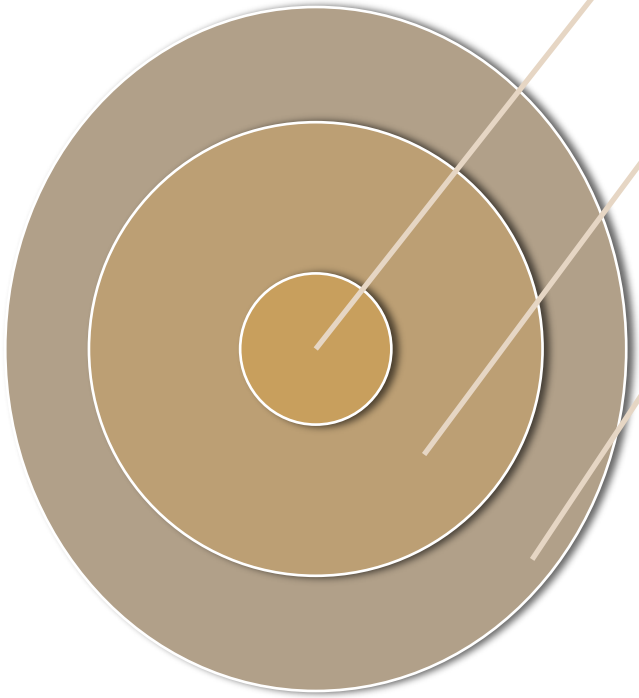
se·cu·ri·ty: [si-kyoor-i-tee] Show IPA noun, plural se·cu·ri·ties, adjective

noun

- 1. freedom from danger, risk, etc.; safety.
- 2. freedom from care, anxiety, or doubt; well-founded confidence.
- 3. something that secures or makes safe; protection; defense.
- 4. freedom from financial cares or from want: The insurance policy gave the family security.
- 5. precautions taken to guard against crime, attack, sabotage, espionage, etc.: The senator claimed security was lax and potential enemies know our plans.

Source: dictionary.reference.com

Privacy, Confidentiality, Security



Privacy – The right of an individual to limit access about his or her person

Confidentiality – Expectation that information will only be shared for its intended purpose

Security – Protection measures or tools for safeguarding information

The Security Rule

- Enforceable on April 21, 2005
- Pertains to electronic PHI (e-PHI)
- Applicable to all Covered Entities and under HITECH/ Omnibus, ***extended to Business Associates and Subcontractors under HITECH/Omnibus Rule*** Δ 2013
- Standards and Implementation Specifications
  - Required 14
  - Addressable 22
    - Implement
    - Equivalent
    - Not Implement
    - Documentation

Security Rule

- 164. 302 Applicability Δ 2013
- 164. 304 Definitions Δ 2013
- Business Associates Δ 2013
- 164. 306 General Rules Δ 2013
- 164. 308 Administrative Safeguards Δ 2013
- 164. 310 Physical Safeguards Δ 2013
- 164. 312 Technical Safeguards
- 164. 314 Organizational Requirements Δ 2013
- 164. 316 Policies and Procedures and Documentation Requirements Δ 2013
- 164. 318 Compliance Dates for the Initial Implementation of the Security

Security Standards: General Rules

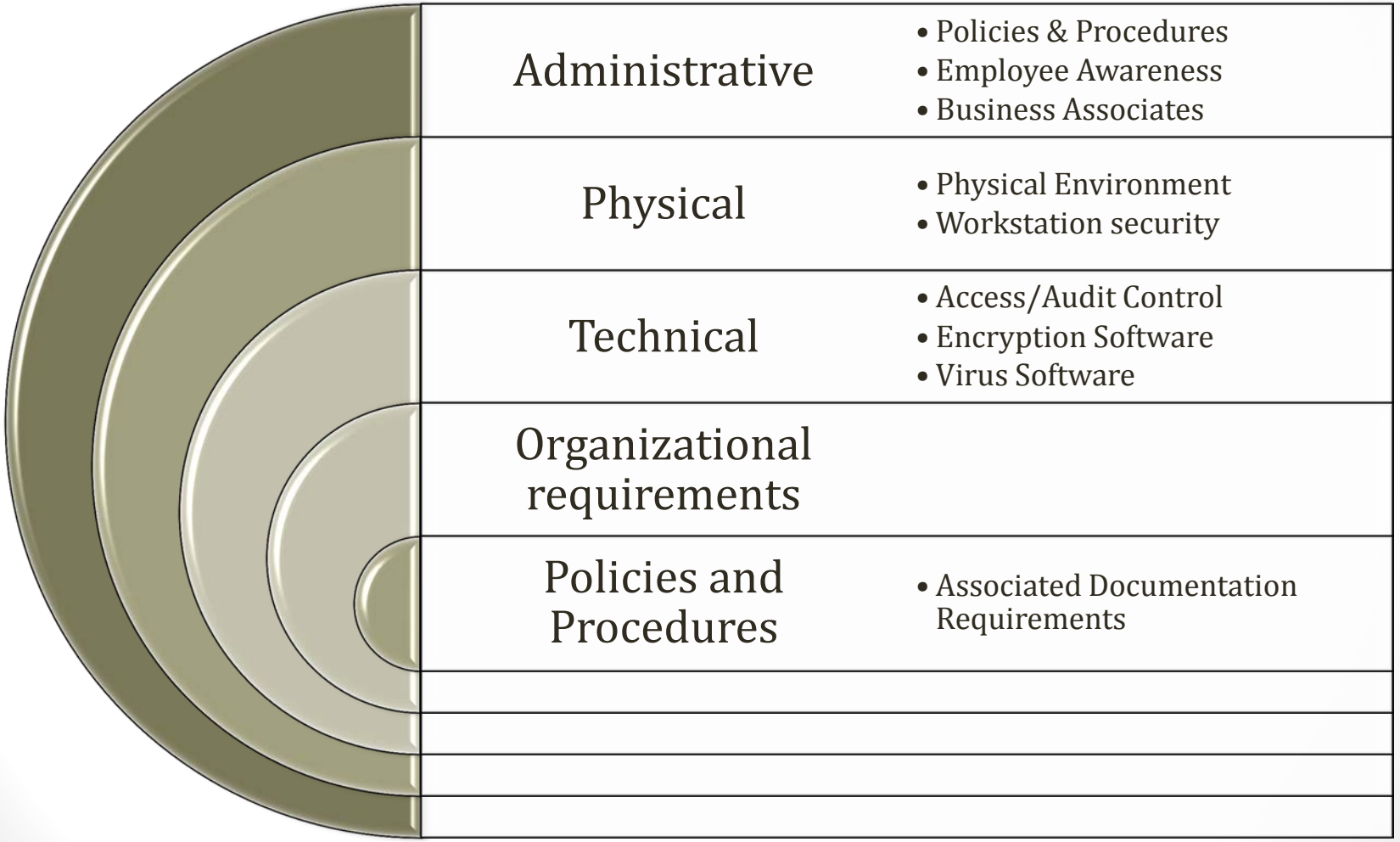
Covered Entities Must:

- Ensure ***confidentiality, integrity,*** **and** ***availability*** **(CIA)** of all e-PHI created, received, maintained, or transmitted
- Protect against any reasonably anticipated threats or hazards to the security and integrity of PHI, e.g., hackers, virus, data back-ups
- Protect against any reasonably anticipated uses and disclosures that are not permitted or required under the Privacy Rule
- Ensure compliance by its workforce

Security Standards: General Rules

- Covered Entities May
- Use any security measures that allow it to reasonably and appropriately implement the standards (flexible, scalable, technology neutral)
  - Size, complexity, and capabilities of CE
  - Technical infrastructure, hardware, and software security capabilities (malware)
  - Probability and criticality of potential risks to e-PHI
  - Costs of security measures
  - **NOTE: Preamble states "Cost is not meant to free covered entities from responsibility"**

What is PHI Security?



Administrative Safeguards

ADMINISTRATIVE SAFEGUARDS			
Standards	**Sections**	**Implementation Specifications §164.306(d) (R) = Required; (A) = Addressable**	
Security Management Process	§164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	§164.308(a)(2)		(R)
Workforce Security	§164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	§164.308(a)(4)	Isolating Healthcare Clearinghouse Functions	(R)
		Access Authorization	(A)
		Access Establishment and Modifications	(A)

Administrative Safeguards

ADMINISTRATIVE SAFEGUARDS (continued)			
Security Awareness and Training	§164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	
Security Incident Procedures	§164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	§164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedures	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	§164.308(a)(8)		(R)
Business Associate Contracts and Other Arrangements	§164.308(b)(1)	Written Contract or Other Arrangement	(R)

Physical Safeguards

PHYSICAL SAFEGUARDS			
Standards	Sections	Implementation Specifications §164.306(d) (R) = Required; (A) = Addressable	
Facility Access Controls	§164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	§164.310(b)		(R)
Workstation Security	§164.310(c)		(R)
Device and Media Controls	§164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

Technical Safeguards

TECHNICAL SAFEGUARDS			
Standards	**Sections**	**Implementation Specifications (§164.306(d)) (R) = Required; (A) = Addressable**	
Access Control	§164.312(a)(1)	User Unique Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	§164.312(b)		
Integrity	§164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	§164.312(d)		
Transmission Security	§164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

Organization, Policies, and Documentation Requirements

ORGANIZATIONAL REQUIREMENTS			
Standards	**Sections**	**Implementation Specifications §164.306(d) (R) = Required; (A) = Addressable**	
Business Associate Contracts or Other Arrangements	§164.314(a)(1)	Business Associate Contracts	(R)
		Other Arrangements	(R)
Requirements for Group Health Plans	§164.314(b)(1)	Implementation Specifications	(R)
POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS			
Standards	**Sections**	**Implementation Specifications §164.306(d) (R) = Required; (A) = Addressable**	
Policies and Procedures	§164.316(a)		(R)
Documentation	§164.308(b)(1)	Time Limit	(R)
		Availability	(R)
		Updates	(R)

Business Associates

Under new Rule effective March 26, 2013 enforceable September 23, 2013

- Security rule safeguards apply
- Privacy rule use and disclosure rule apply
- Use PHI only as stated in contract/agreement
- PENALTIES now apply to Bas
- BA's are now responsible for having BAAs
- Subcontractors are now treated as BA and held to same standards as BA
- BAs must have agreement with Subs

There is NO requirement of the CE to monitor the BA

Business Associates

- Required elements of BAA
  - Start/expiration/review dates and signatures
  - Terms and conditions (how to use or disclose PHI, data rights, security, et)
  - P&P for data retention and destruction
  - Recording of breaches
  - Reporting of breaches to CE
  - Penalties for breaches

Transition to new BAA

- Existing agreements that confirmed to HITECH regulation executed/renewed before 1/25/13
  - Allowed 240 days + 1 year transition
  - Compliance required by 9/23/14
- New BAAs executed/renewed after 1/25/13
  - Must conform to new rules
  - Compliance required by 9/23/13

Sample BAA:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

How to ensure compliance

Has your organization conducted an assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information?

OCR Guidance for Risk Analysis

- Identified as first step in implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule
- Evaluate risks and vulnerabilities in their environments
- Implement reasonable and appropriate security measures to protect against threats or hazards to the security or integrity of PHI

Source: Guidance on Risk Analysis Requirements under the HIPAA Security Rule

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalintro.html

Items to Consider

Sample questions:

- Have you identified the e-PHI within your organization? This includes e-PHI that you create, receive, maintain or transmit.
- What are the external sources of e-PHI? For example, do vendors or consultants create, receive, maintain or transmit e-PHI?
- What are the human, natural, and environmental threats to information systems that contain e-PHI?

Source: Guidance on Risk Analysis Requirements under the HIPAA Security Rule

http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

Security Risk Analysis (Administrative Safeguards)

Security Management Process

- **Risk Analysis** (R) - §164.308(a)(1)(ii)(A)

  "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity"

- **Risk Management** (R) - §164.308(a)(1)(ii)(A

  "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable appropriate level…"

Security Risk Analysis (Meaningful Use)

(Core Requirement - EP/HOSP)

- **Objective:** *"Protect electronic health information created or maintained by* ***certified EHR technology*** *through the implementation of appropriate technical capabilities."*

- **Measure:** *"Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of the risk management process."*

What is Risk?

Adapted definition from NIST SP 800-30…

"The net mission impact considering (1) the probability that a particular [threat] will accidentally trigger or intentionally exploit a particular [vulnerability] and (2) the resulting impact if this should occur… [R]isks arise from legal liability or mission loss due to:

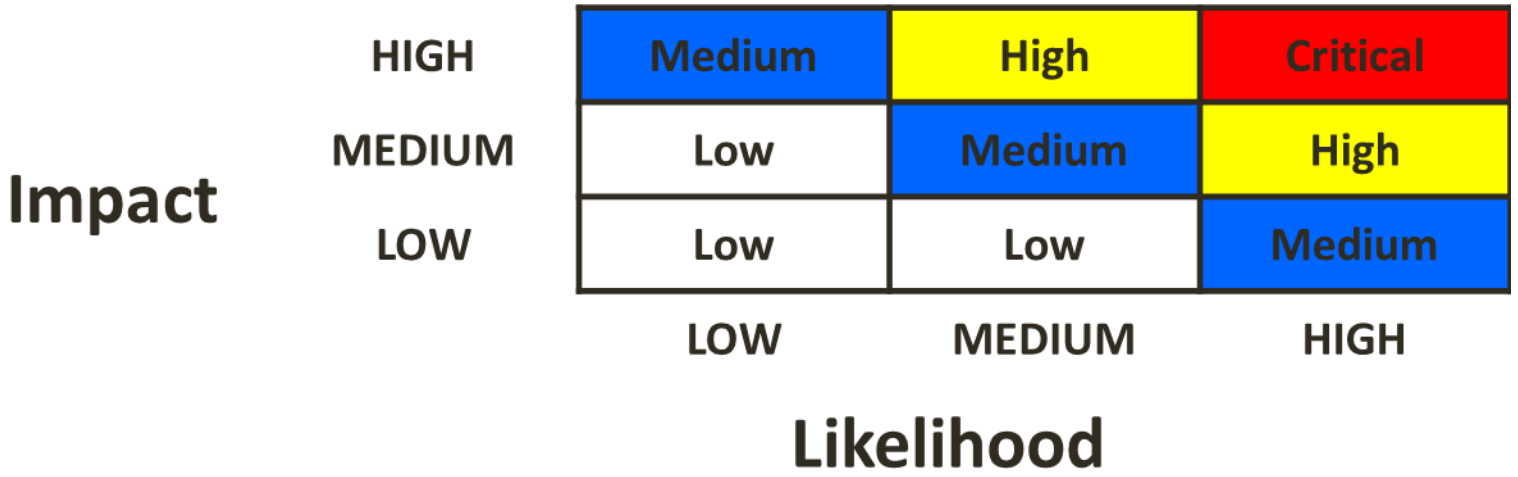
1. Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
2. Unintentional errors and omissions
3. IT disruptions due to natural or man-made disasters
4. Failure to exercise due care and diligence in the implementation and operation of the IT system."

Available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf

.

What is Risk?

Risk = Impact * Likelihood



Goal = Understanding the probability of a threat occurrence being caused by a vulnerability and how to classify it… Low, Medium, High, Critical

Risk Example - Personal

Personal Asset = House, Apartment, Condo

Threat Source

- Burglar

Vulnerability

- No deadbolt
- Empty during the day
- Windows left open
- Lots of plants surrounding the front yard

Controls

- Awareness
- Deadbolts on doors
- Decorative bars around windows
- Alarm Systems
- Neighborhood watch
- Gated Community

Risk Example to PHI

Information Asset = Laptop with ePHI

Threat Source

- Theft of a laptop

Vulnerability

- Device is portable
- Password is weak
- ePHI is not encrypted
- ePHI is not backed up

Controls

- Policies and Procedures
- Training and Awareness
- Cable lockdown
- Strong passwords
- Encryption
- Data Backup

HHS (9) Essential Elements of a Risk Analysis

1. Scope of the Analysis
   - All systems containing ePHI
   - Certified EHR Technology (meaningful use)
2. Data Collection
   - Identify where ePHI is stored, received, maintained or transmitted
3. Identify and Document Potential Threats and Vulnerabilities
   - External and Internal
4. Assess Current Security Measures
   - Document current processes that may limit risks

HHS (9) Essential Elements of a Risk Analysis

5. Determine the likelihood of threat occurrence
   - NIST guidelines provide a qualitative analysis that ranks likelihood (probability) as High, Medium, Low
6. Determine potential impact of threat occurrence
   - NIST guidelines provide definitions for High, Medium, Low; Severe or Catastrophic, Serious, Limited events

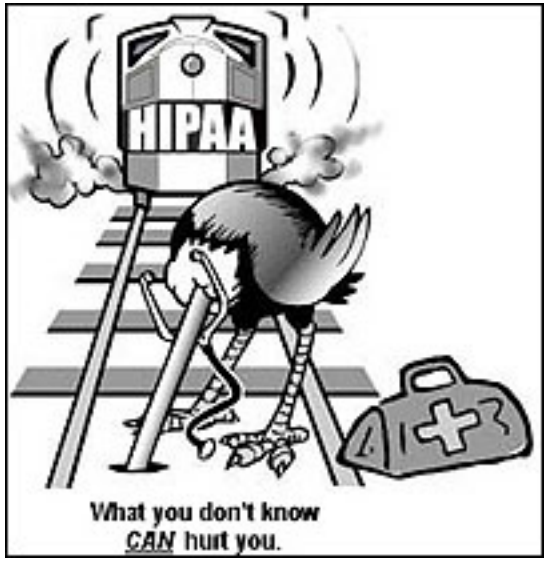
HHS (9) Essential Elements of a Risk Analysis

Calculate the probability of an event

Calculating a Risk Score			
	Low Impact (10)	Medium Impact (50)	High Impact (100)
High Likelihood (1)	Low (10)	Medium (50)	High (100)
Medium Likelihood (.5)	Low (5)	Medium (25)	Medium (50)
Low Likelihood (.1)	Low (1)	Low (5)	Low (10)

HHS (9) Essential Elements of a Risk Analysis

7. Determine and prioritize the level of risk
8. Identify potential security measures and finalize documentation
9. Period Review and Update to Risk Assessment



Risk Analysis Sample

Prioritized Risks

The risk meeting results on the previous sheet are copied and pasted here and organized in order of priority, using menu item **Data - Sort...,** selecting the **Risk Level column** to sort by, and clicking the **Descending** button**.** Following this sheet is the **Summary and Next Steps** sheet, a summary of issues and recommendations by risk level, to be used as the guide to risk mitigation.

System or Flow, or Physical Security Item	Risk Issue	Recommendation	Policy Review	Tech Review	Impact to C., I., or A.	Likelihood	Risk Level
1. Local User Access of practice-based and remote services	Improper Access	PC and Network Configuration Review and Vulnerability Scan		Needed	C: 3 I: 3 A: 3	2	6
1. Local User Access of practice-based and remote services	Improper Access of Communications	Review configuration of communications outside of Practice premises		Needed	C: 3 I: 3 A: 3	2	6
2. Remote User Access of Practice Network	EPHI Remaining on Remote Systems	Use of Encryption, Policy limitation on downloading of EPHI	Needed		C: 3 I: 1 A: 1	2	6
2. Remote User Access of Practice Network	Improper Access of Communications	Review configuration of VPN and remote devices		Needed	C: 3 I: 3 A: 3	2	6
5. Excel Files, Word Documents, Access Databases	Remote Access - PHI remaining	Encryption of portable devices containing PHI	Needed	Needed	C: 3 I: 1 A: 1	2	6
5. Excel Files, Word Documents, Access Databases	Remote Access - Communications	Review configuration of communications regularly to ensure security		Needed	C: 3 I: 1 A: 1	2	6

A Risk Assessment is not…

- A checklist
- Privacy and Security functionality of an EHR software
- An evaluation of the hardware
- A one-time event
- A requirement ONLY for meaningful use attestation

Some tools to help

- **CalOHII** – California Office of Health Information Integrity
  - Security Toolkit

  http://www.ohii.ca.gov/calohi/PrivacySecurity/ToolstoHelpYou.aspx
- **NIST** – National Institute of Standards and Technology
  - HIPAA Security Rule Toolkit

  http://scap.nist.gov/hipaa/
- **HHS Audit Program Protocol**
  - Covers Privacy, Security and Breach Notification Rule Requirements

  http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
- **ONC: Guide to Privacy and Security of Health Information**

  http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Breakout Time

What are some suggested Security Measures to track, trend, and monitor as part of a Security Management Program?

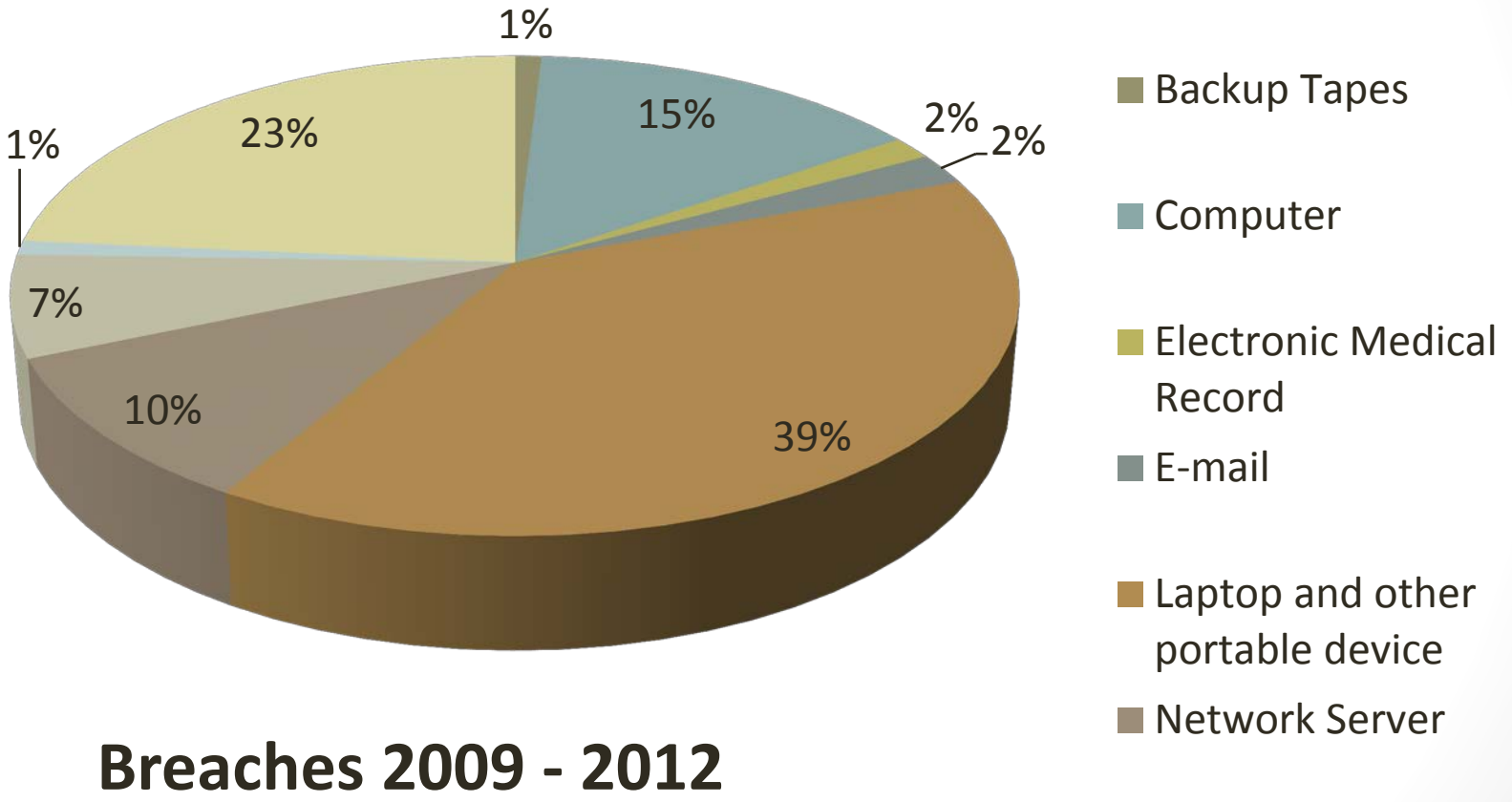
Some Suggested Examples

5 Security Components for Risk Management		
Security Components	**Examples**	**Examples of Security Measures**
Physical Safeguards	• Your facility and other places where patient data is accessed • Computer equipment • Portable devices	• Building alarm systems • Locked offices • Screens shielded from secondary viewers
Administrative Safeguards	• Designated security officer • Workforce training and oversight • Controlling information access • Periodic security reassessment	• Staff training • Monthly review of user activities • Policy enforcement
Technical Safeguards	• Controls on access to EHR • Use of audit logs to monitor users and other EHR activities • Measures that keep electronic patient data from improper changes • Secure, authorized electronic exchanges of patient information	• Secure passwords • Backing-up data • Virus checks • Data encryption
Policies & Procedures	• Written policies and procedures to assure HIPAA security compliance • Documentation of security measures	• Written protocols on authorizing users • Record retention
Organizational Requirements	• Breach notification and associated policies • Business associate agreements	• Agreement review and updates

Source: ONC Guide to Privacy and Security of Health Information

Privacy and Security Incidents (Breaches and Violations)

Some Statistics



Breaches 2009 - 2012

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Some Statistics

Table 4: PHI Data Breach by Source / Device

	Pre-2012		2012	
Laptop and other portable device	151	39.2%	55	37.7%
Paper	92	23.9%	31	21.2%
Computer	56	14.5%	20	13.7%
Server	38	9.9%	15	10.3%
Other	18	4.7%	18	12.3%
Email	7	2%	4	2.7%
Electronic Health Record	6	1.6%	2	1.4%
X-Ray	5	1.3%	0	0
Back-up Tapes	4	1%	1	0.6%
Hard Drives	3	0.8%	0	0
Mail, Postcards	3	0.8%	0	0
CD	2	0.5%	0	0
Total	385	100%	146	100%

Source: Redspin Breach Report 2012
http://www.redspin.com/docs/Redspin_Breach_Report_2012.pdf

By the numbers…

- **21.5%** increase in # of large breaches in 2012 over 2011… but a 77% decrease in number of patient records impacted
- **67%** of all breaches have been result of a theft or loss
- **57%** of all patient records involved a business associate
  - Historically breaches at business associates have impacted 5 times **(5X)** as many patient records as those of CE
- **38%** of incidents result of unencrypted laptop or other portable device

Source: Redspin Breach Report 2012
http://www.redspin.com/docs/Redspin_Breach_Report_2012.pdf

Breach defined…

California State Law

"Unlawful or unauthorized access to, and use or disclosure of patients' medical information whether electronic, paper, or oral"

Federal Regulations

" the acquisition, access, use, or disclosure of Protected Health Information (PHI) in manner not permitted by the Privacy Rule which compromises the security or privacy of the PHI"

What is a Breach?

- **§164.402 defines "breach"** as *the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information*. ~~**(i.e. which poses a significant risk of financial, reputational, or other harm to an individual)**~~
- **Δ 2013 Final Rule:** an impermissible use or disclosure of PHI is ***presumed*** to be a breach [and notification necessary] unless the covered entity or business associate, as applicable, demonstrates that there is a *low probability* that the PHI has *been compromised* by demonstrating a thorough risk assessment
- Risk assessment is to include four factors

Exceptions

- Unintentional acquisition, access or use of PHI by a workforce member or a person acting under the authority of the covered entity (CE) or business associate (BA), if it was in good faith, within scope of authority, and does not result in further use or disclosure that violates HIPAA
- Inadvertent disclosure to another at the CE or BA (or within an organized health care arrangement in which the CE participates), if the recipient is authorized to see PHI and it does not result in further use or disclosure that violates HIPAA
- Good faith belief that recipient would not reasonably have been able to retain the PHI

Other

Δ 2013 Final Rule: Limited Data Set

- No longer an exception if a breach if the information does not include direct identifiers (at 45 CFR 164.514(e)(2)), date of birth, or zip code
- Risk assessment that evaluates the four factors to determine if breach notification is not required.
- Encourage CE and BA to take advantage of "safe harbor" provision of breach notification rule

Compromise Standard

- Complete a **Risk Assessment** to determine if there is a low probability of compromise
- Factors to include:
  - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
  - The unauthorized person who used the PHI or to whom the disclosure was made:
  - Covered entities must determine whether or not the PHI was actually acquired or viewed or whether there was an opportunity for the PHI to be acquired or viewed.
  - The extent to which the risk to the PHI has been mitigated

Notification

- CE and BA must only provide the required notice ***if*** the breach involve ***unsecured*** protected health information

What is Unsecured PHI?

- Unsecured PHI is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance.
- HHS issued guidance on April 17, 2009 and updated guidance in the August 24, 2009 breach reporting regulations (74 Fed. Reg. 42740)
- Secured PHI is **encrypted** according to NIST standards (or if paper, destroyed)
- Encryption is not required, but works as ***"safe harbor"*** to reporting requirement

Safe Harbor is…

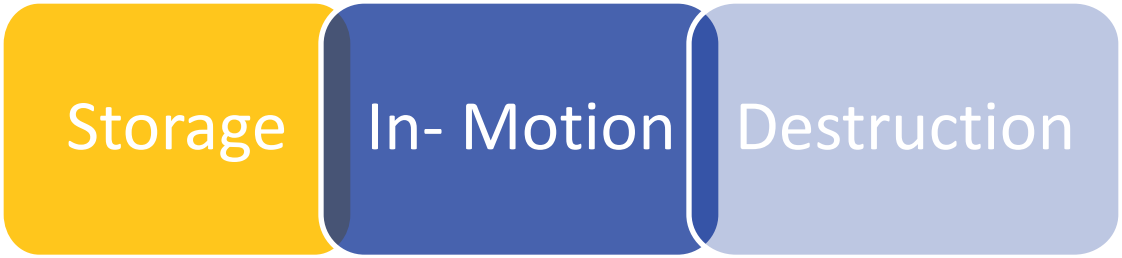
PHI that is rendered unusable, unreadable, or indecipherable using specified technologies and methodologies pursuant to the rules' guidance for **data-at-rest, data-in-motion, and data destruction**

Safe Harbor Guidance

- Providers are not required to follow guidance as specified in the Security Rule for encryption; however,
- ***If specified methodologies ARE used***, no breach notification exists or is required creating the functional equivalent of a **"Safe Harbor"**
- Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals

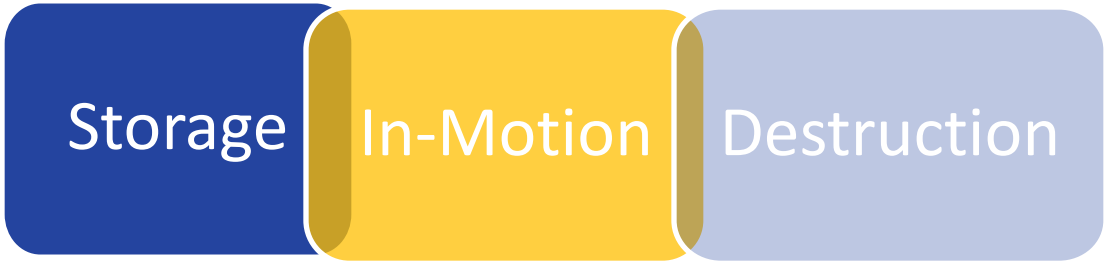
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html

Encryption Guidance



- **Data at Rest:** includes data that resides in databases, file systems, flash drives, memory and any other structured storage method
  - SP 800-111 Guide to Storage Encryption Technologies for End User Devices

Encryption Guidance



- **Data in Motion:** includes data that is moving through a network, including wireless transmission, whether by email or structured electronic interchange
  - NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

Destruction Guidance

- Data Disposed: includes discarded paper records or recycled electronic media.
  - SP 800-88, Guidelines for Media Sanitization

Reporting requirements

SB 541

Facility must report within **5 business days** of detection of the incident-$100 per day fine for failure to report (Any lawful or unauthorized access to, or use or disclosure of a patient's medical information)

- **HITECH (Breaches on or after September 23, 2009)**

- Facilities must report to the patient **within 60 days** of the incident, the date and discovery of the breach, what happened, what PHI was involved, steps taken to investigate and protect them from harm and contact numbers

- Reports to media also required if breach involve > 500 patients

- Reports to DHHS required **annually or within 60 days** if breach involved PHI > 500 patients

Breach Scenarios

A hospital employee left a message with the daughter of a patient that detailed the medical condition and treatment plan…

OCR Resolutions

Minimum Necessary (164.514(d))

Confidential Communications (164.522(b))

- OCR identified that confidential communications requirements not followed (employee left message at home despite request to contact her through work
- Too much information over telephone
- Hospital developed and implemented new procedures
  - Issue of minimum necessary over telephone
  - Employees trained to review registration information for patient contact directives
  - New policies incorporated into staff privacy training and yearly update

Breach Scenarios

Massachusetts provider settles HIPAA case for $1.5M

"Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. (collectively referred to as "MEEI") has agreed to pay the U.S. Department of Health and Human Services (HHS) **$1.5 million** to settle potential violations of the HIPAA Privacy and Security Rules. MEEI has also agreed to take corrective action to improve policies and procedures to safeguard the privacy and security of their patients' protected health information and retain an independent monitor to report on MEEI's compliance efforts."

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement.html

OCR Findings

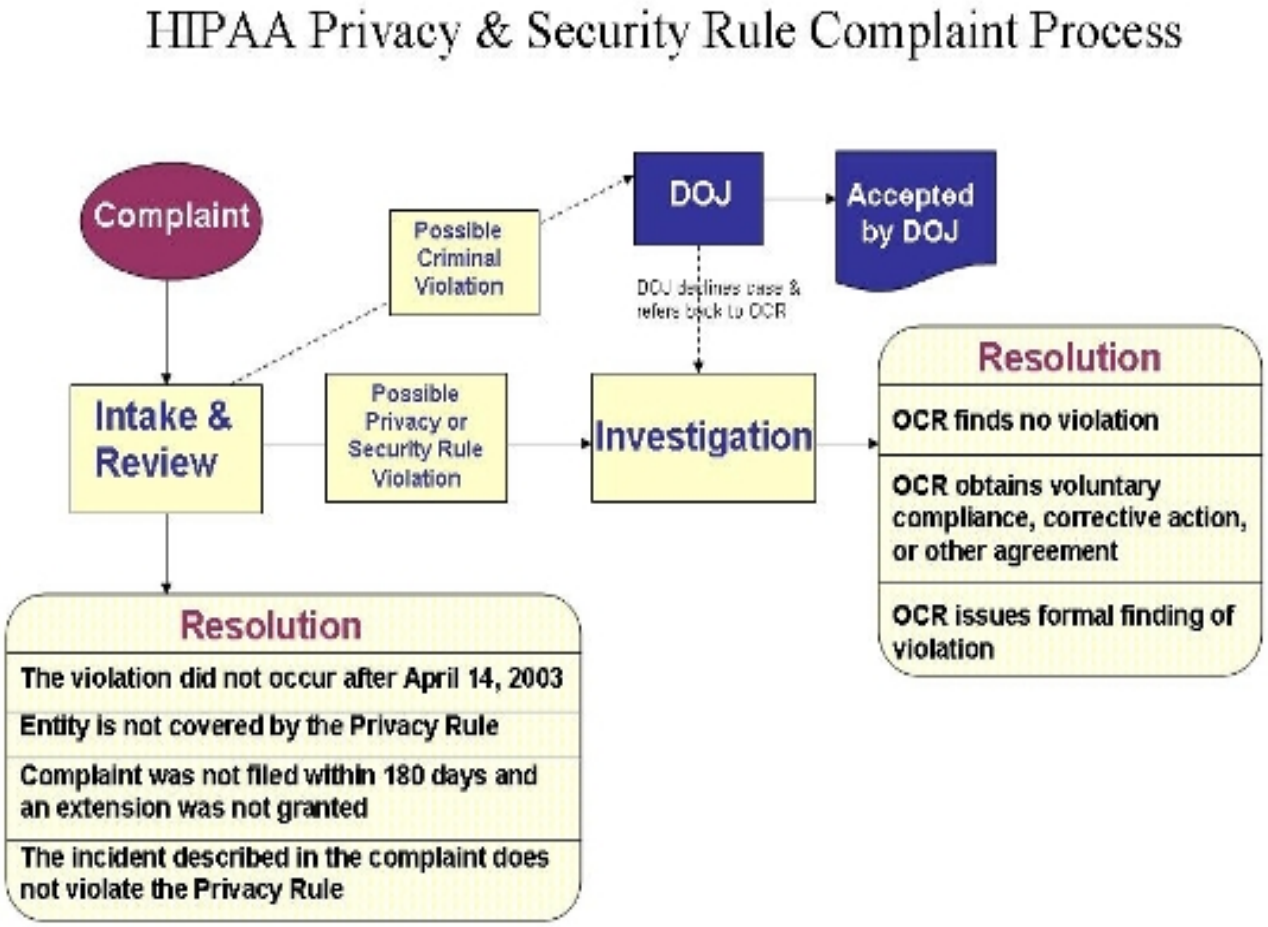
- Failure to conduct a thorough risk analysis to evaluate confidentiality of ePHI maintained on portable devices
- Failure to implement appropriate security measures sufficient to ensure confidentiality of ePHI created, maintained and transmitted using portable devices
- Failure to adopt and implement policies to restrict access to ePHI to authorized users of portable devices
- Failure to implement policies and procedure to address security incident identification, reporting and response.
- Failure to implement appropriate safeguards on mobile devices

OCR Enforcement Actives

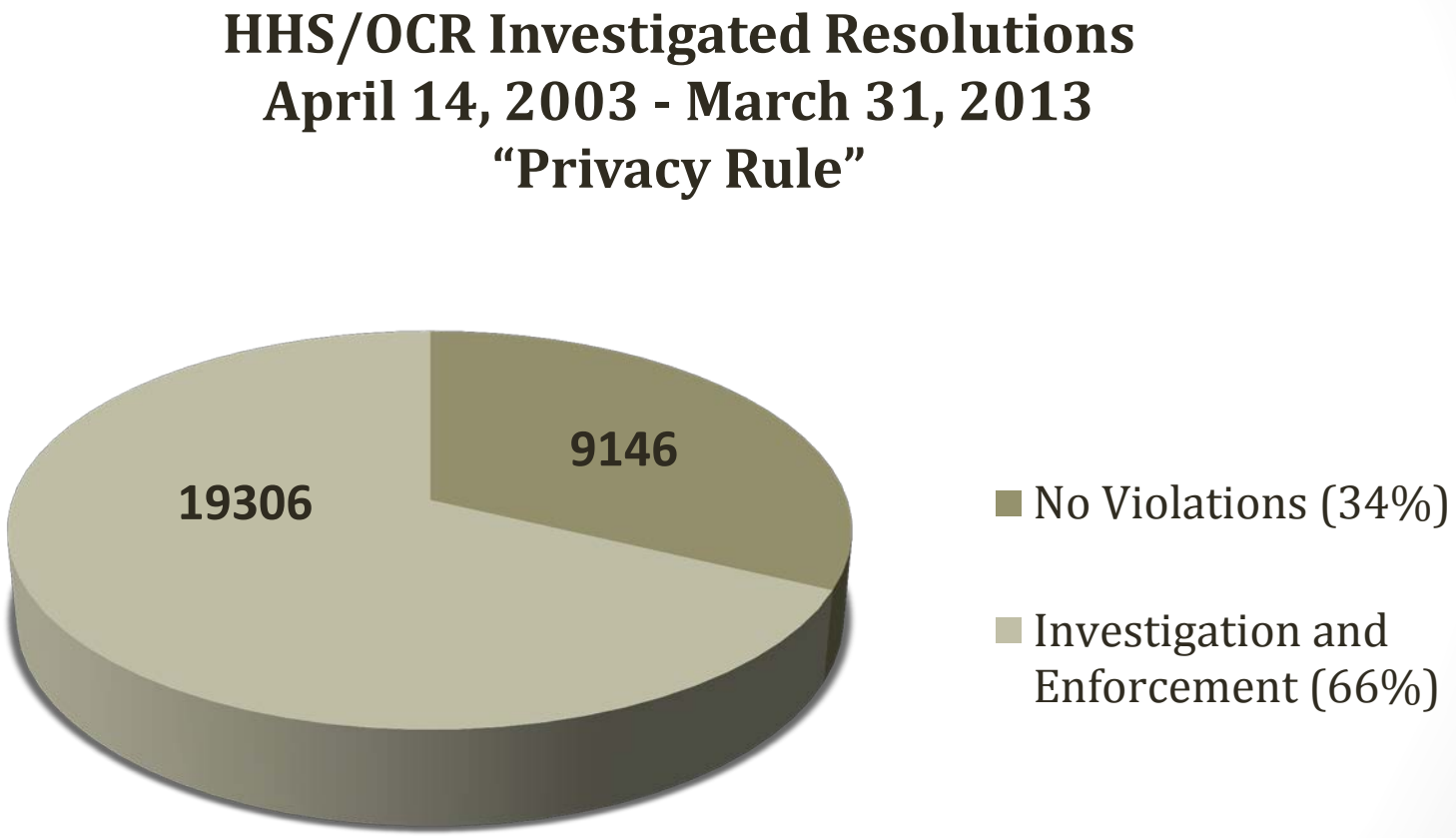
OCR Investigative Regulations

- Privacy Rule compliance and enforcement began April 14, 2003
- Security Rule compliance started April 20, 2005 and enforcement by OCR began July 27, 2009
- OCR enforces Privacy and Security Rule in several ways:
  - By investigating complaints filed
  - Conducting compliance reviews to determine if CE are in compliance
  - Performing education and outreach to foster compliance
- OCR also works with Department of Justice (DOJ) to refer possible criminal violations of HIPAA

OCR Complaint Process



HHS/OCR Investigations



HHS/OCR Compliance Issues

- Impermissible Uses and Disclosure
- Lack of Safeguards of PHI
- Lack of Patient Access to PHI
- Uses and Disclosures more than Minimally Necessary
- Lack PHI Administrative Safeguards

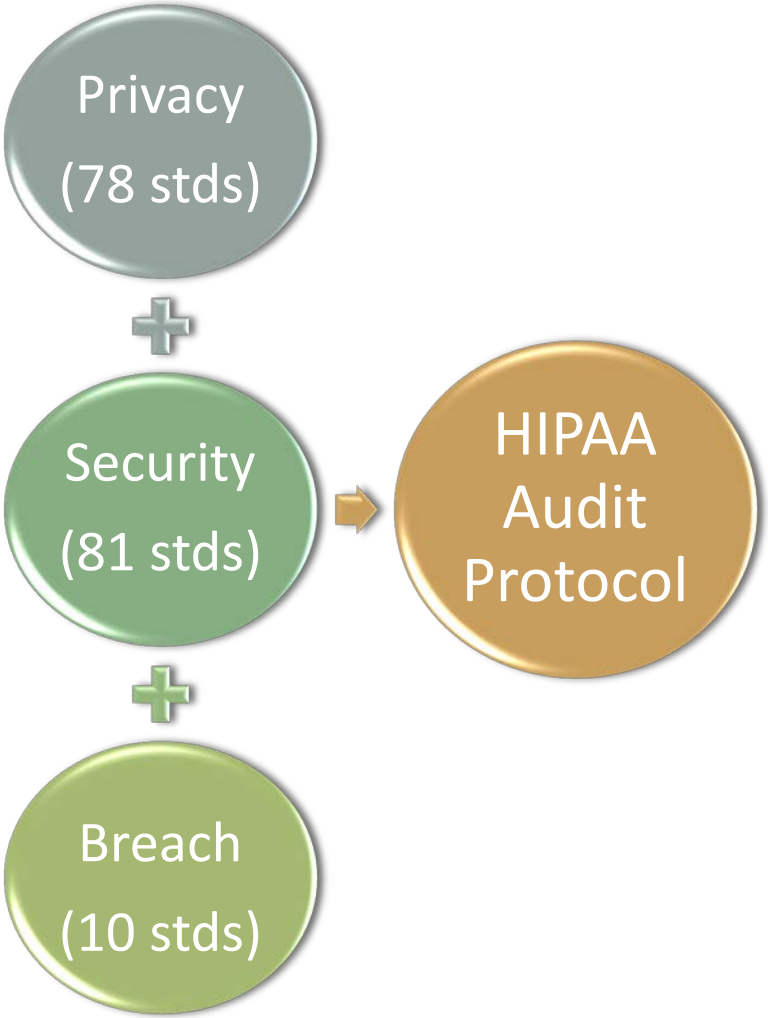
OCR Audit Program

- ARRA of 2009 requires HHS to provide periodic audits to ensure CE and BA are meeting HIPAA compliance requirements
- Serves as a new part of OCR's Health Information Privacy and Security Compliance Program
- Conducted 115 total audits through December of 2012
- Compliance with Privacy, Security, and Breach Notification Rules
- Business Associates not included in first year

Audit Process

- Audit Process 7 steps
  - Notification to CE/BA
  - 15 days to provide documentation
  - OCR reviews
  - On-site visit within 30 days
  - Draft Report 20-30 days
  - Response to draft report 10 days
  - Final Report
- Documentation
  - **So important.** Provides the burden of proof

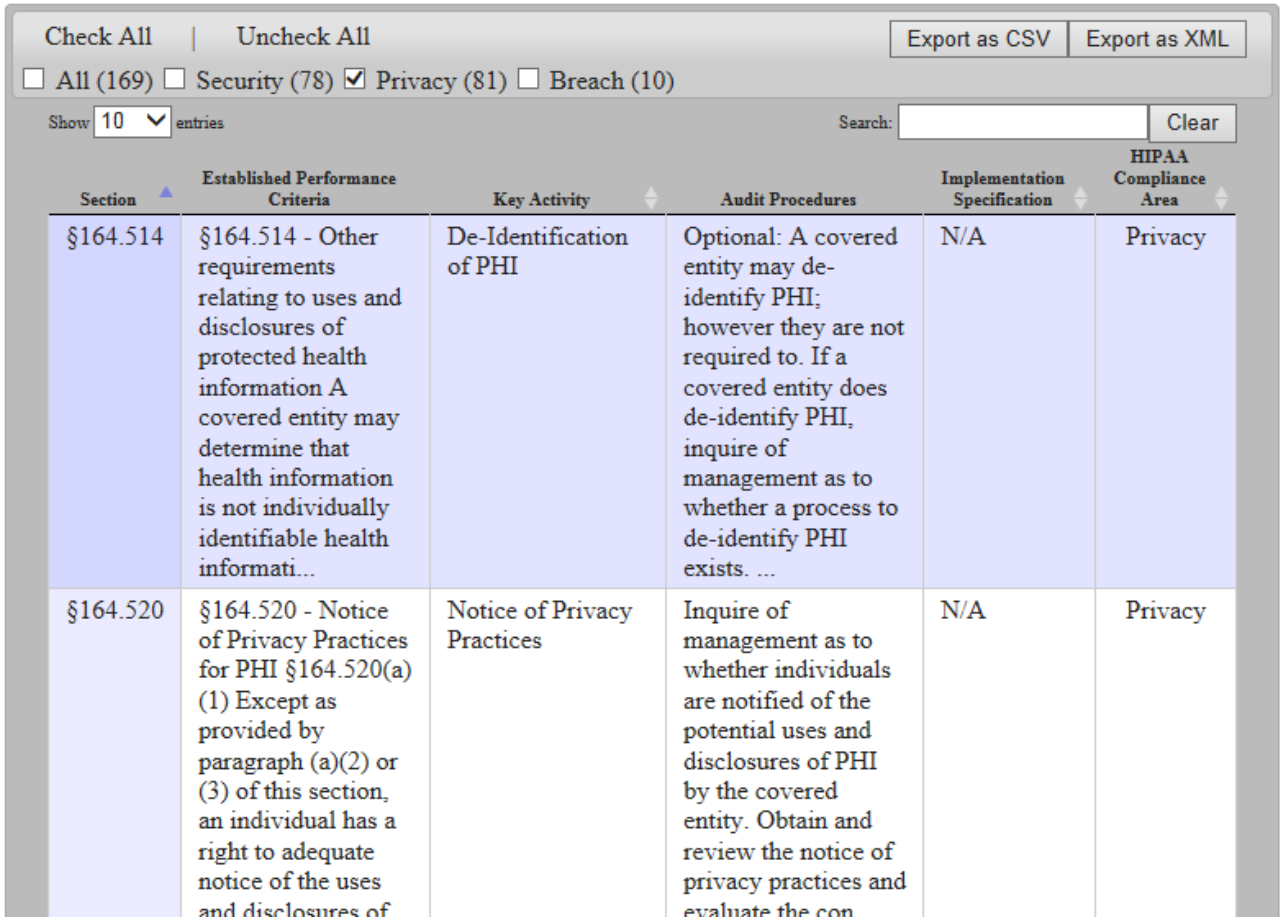
OCR Audit Program Protocol



http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

HHS HIPAA Audit Protocol

The protocol is available for public review and searchable by keyword(s) in the table below.



Check All | Uncheck All Export as CSV Export as XML

☐ All (169) ☐ Security (78) ☑ Privacy (81) ☐ Breach (10)

Show 10 entries Search: Clear

Section	Established Performance Criteria	Key Activity	Audit Procedures	Implementation Specification	HIPAA Compliance Area
§164.514	§164.514 - Other requirements relating to uses and disclosures of protected health information A covered entity may determine that health information is not individually identifiable health informati...	De-Identification of PHI	Optional: A covered entity may de-identify PHI; however they are not required to. If a covered entity does de-identify PHI, inquire of management as to whether a process to de-identify PHI exists. ...	N/A	Privacy
§164.520	§164.520 - Notice of Privacy Practices for PHI §164.520(a)(1) Except as provided by paragraph (a)(2) or (3) of this section, an individual has a right to adequate notice of the uses and disclosures of	Notice of Privacy Practices	Inquire of management as to whether individuals are notified of the potential uses and disclosures of PHI by the covered entity. Obtain and review the notice of privacy practices and evaluate the con	N/A	Privacy

Results from 2012 Findings

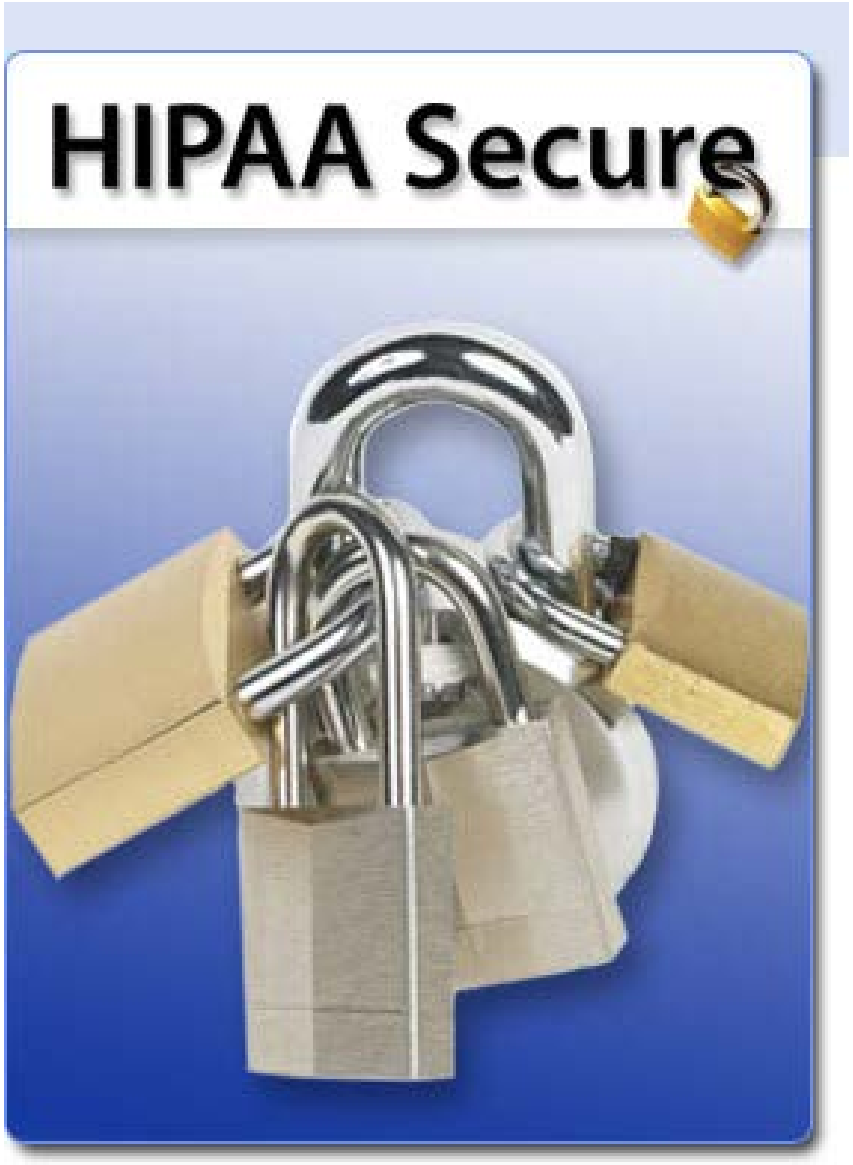
- Not published yet
- AHIMA Webinar:
  - Security accounted for more than 60% of findings
  - Smallest entities struggled the most in all three areas
  - 47/59 providers had incomplete or inaccurate risk analysis
  - Most common excuse “unaware of requirement”
  - Lack of sufficient resources
  - Incomplete implementation

Results from 2012 Findings

- AHIMA Webinar:
  - Privacy
    - Notice of privacy practices
    - Access of individuals
    - Minimum Necessary
    - Authorizations
  - Security
    - Risk Analysis
    - Access Control
    - Contigency Planning
    - Media movement and disposal
    - Audit controls and monitoring

Strategies for Success

- Read the Ominbus Rule
  - http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- Conduct a thorough independent risk analysis for privacy, security and breach
- Do a security walk through your department
- Re-visit your Business Associate agreements
- Train/educate workforce members
- Evaluate employee access control procedures
- Remember mobile devices!
- Ensure all documentation is up to date; including policies and procedures, and workforce training


HIPAA Secure

Kelly Stewart @ Kelly.Stewart@ihs.gov
Sharon Lewis @ slewis@primeauconsultinggroup.com