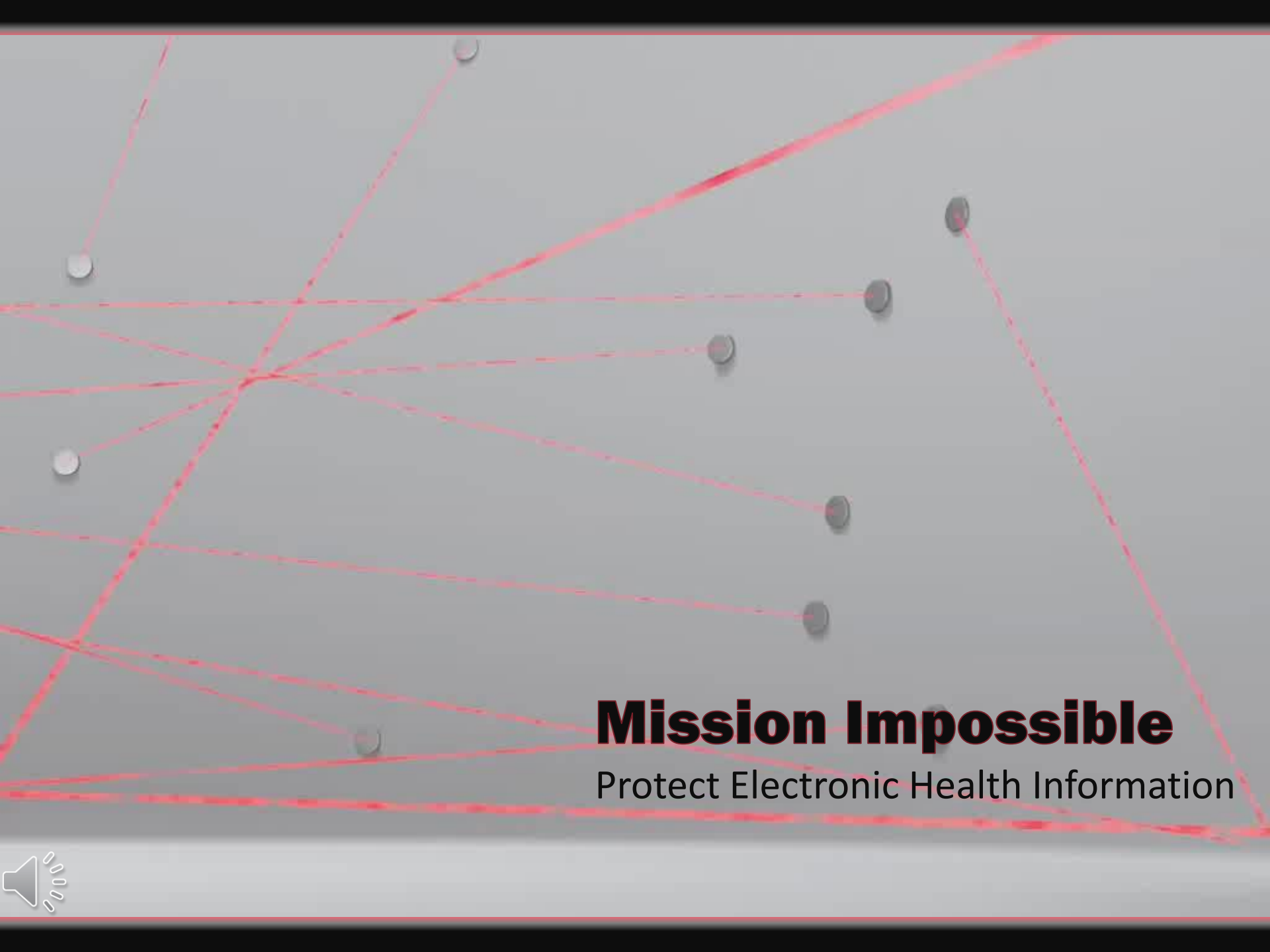
HIPAA and Meaningful Use

Protect Electronic Health Information

HIMSS
CENTRAL & SOUTHERN OHIO *Chapter*


Mission Impossible
Protect Electronic Health Information

Presenter Today:
Jim Carroll

- Over 40 years of IT experience in Healthcare, Manufacturing & Distribution, Facilities & Management, Insurance and Consulting
- Former CIO for a group of 3 hospitals in northeast Ohio
- Currently directing the Regional Extension Center, a program of the Akron Regional Hospital Association
- Lead and facilitate the CMS Privacy & Security Community of Practice

We will review:

- The requirements from CFR 164,
- Examples of the resources available for a provider or hospital,
- Basic guidelines to assist in completing a Risk Analysis and Management Plan.

REQUIREMENTS

HIMSS
CENTRAL & SOUTHERN OHIO *Chapter*

HIPAA Security Rule

- Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

- The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164. *http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf*

Meaningful Use Objective for 2015

- **Objective:** Protect electronic health information created or maintained by the CEHRT through the implementation of appropriate technical capabilities.
- **Measure:** Conduct or review a security risk analysis in accordance with the requirements in **45 CFR 164.308(a)(1)**, including addressing the security (to include encryption) of ePHI created or maintained in CEHRT in accordance with requirements in 45 CFR **164.312(a)(2)(iv)** and **45 CFR 164.306(d)(3)**, and implement security updates as necessary and correct identified security deficiencies as part of the EP's risk management process.

The Following Identifiers Are Key
for de-identification of data

removed:

(A) Names	
(B) All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000	
(C) All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older	
(D) Telephone numbers	(L) Vehicle identifiers and serial numbers, including license plate numbers
(E) Fax numbers	(M) Device identifiers and serial numbers
(F) Email addresses	(N) Web Universal Resource Locators (URLs)
(G) Social security numbers	(O) Internet Protocol (IP) addresses
(H) Medical record numbers	(P) Biometric identifiers, including finger and voice prints
(I) Health plan beneficiary numbers	(Q) Full-face photographs and any comparable images
(J) Account numbers	(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and
(K) Certificate/license numbers	

The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

Did You Know?

- It has been estimated that the combination of a patient's Date of Birth, Gender, and 5-Digit ZIP Code is unique for over 50% of residents in the United States. This means that over half of U.S. residents could be uniquely described just with these three data elements.
- It has been estimated that the combination of Year of Birth, Gender, and 3-Digit ZIP Code is unique for approximately 0.04% of residents in the United States. This means that very few residents could be identified through this combination of data alone.
- **May parts or derivatives of any of the listed identifiers be disclosed consistent with the Safe Harbor Method?**
  - No. For example, a data set that contained patient initials, or the last four digits of a Social Security number, would not meet the requirement of the Safe Harbor method for de-identification.

AVAILABLE RESOURCES

HIMSS
CENTRAL & SOUTHERN OHIO *Chapter*

Published CFRs

164.306 Security standards: General Rules.

(a) General requirements. Covered entities and business associates must do the following:

(1) **Ensure the confidentiality, integrity, and availability** of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

(2) Protect against any **reasonably anticipated threats or hazards** to the security or integrity of such information.

(3) Protect against any **reasonably anticipated uses or disclosures** of such information that are not permitted or required under subpart E of this part.

(4) **Ensure compliance with this subpart by its workforce**.

164.306 Security standards: General Rules.

(b) Flexibility of approach.

(1) **Covered entities and business associates** may use **any security measures that allow the covered entity or business associate to reasonably and appropriately** implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

(i) The **size, complexity, and capabilities** of the covered entity or business associate.

(ii) The covered entity's or the business associate's **technical infrastructure, hardware, and software security capabilities**.

(iii) The **costs** of security measures.

– (iv) The probability and criticality of potential risks to electronic protected health information.

164.306 Security standards: General Rules.

(c) Standards. A covered entity or business associate **must comply with the applicable standards** as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314 and § 164.316 with respect to all electronic protected health information.

164.306 Security standards: General Rules.

(d) Implementation specifications. In this subpart:

(1) Implementation specifications are required or addressable. If an implementation specification is required, the word “Required” appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word “Addressable” appears in parentheses after the title of the implementation specification.

(2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes **required** implementation specifications, a covered entity or business associate **must implement** the implementation specifications.

(3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity or business associate must—

(i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and

164.306 Security standards: General Rules.

(ii) As applicable to the covered entity or business associate—

(A) Implement the implementation specification if reasonable and appropriate; or

(B) If implementing the implementation specification is not reasonable and appropriate—

(1) Document why it would not be reasonable and appropriate to implement the implementation specification; and

(2) Implement an equivalent alternative measure if reasonable and appropriate.

(e) Maintenance. A covered entity or business associate must review and modify the security measures implemented under this subpart as needed to continue provision of reasonable and appropriate protection of electronic protected health information, and update documentation of such security measures

Administrative Safeguards

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Administrative Safeguards		
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 Health care Clearinghouse Function (R)
		Access Authorization (A)
		Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A)
		Protection from Malicious Software (A)
		Log-in Monitoring (A)
		Password Management (A)
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 Procedure (A)
		Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)

Physical Safeguards

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Physical Safeguards		
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

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

HHS Resources

- HealthIT.gov Privacy and Security Resources
  - http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources
- HHS.gov For Small Providers, Health Plans
  - http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/smallbusiness.html
- HHS.gov Summary HIPAA Security Rule
  - http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
- HHS.gov Security Rule Guidance
  - http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

HHS Resources

- HealthIT.gov Model Notices of Privacy Practices
  - http://www.healthit.gov/providers-professionals/model-notices-privacy-practices
- HealthIT.gov Guide to Privacy and Security PDF
  - http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
    - - Good document to keep on hand
- HealthIT.gov Security Risk Assessment Tool
  - http://www.healthit.gov/providers-professionals/security-risk-assessment-tool

HHS Resources

- HealthIT.gov Model Notices of Privacy Practices
  - http://www.healthit.gov/providers-professionals/model-notices-privacy-practices
- HealthIT.gov Guide to Privacy and Security PDF
  - http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
    - - Good document to keep on hand
- HealthIT.gov Security Risk Assessment Tool
  - http://www.healthit.gov/providers-professionals/security-risk-assessment-tool

RISK ANALYSIS & MANAGEMENT PLAN

HIMSS
CENTRAL & SOUTHERN OHIO *Chapter*

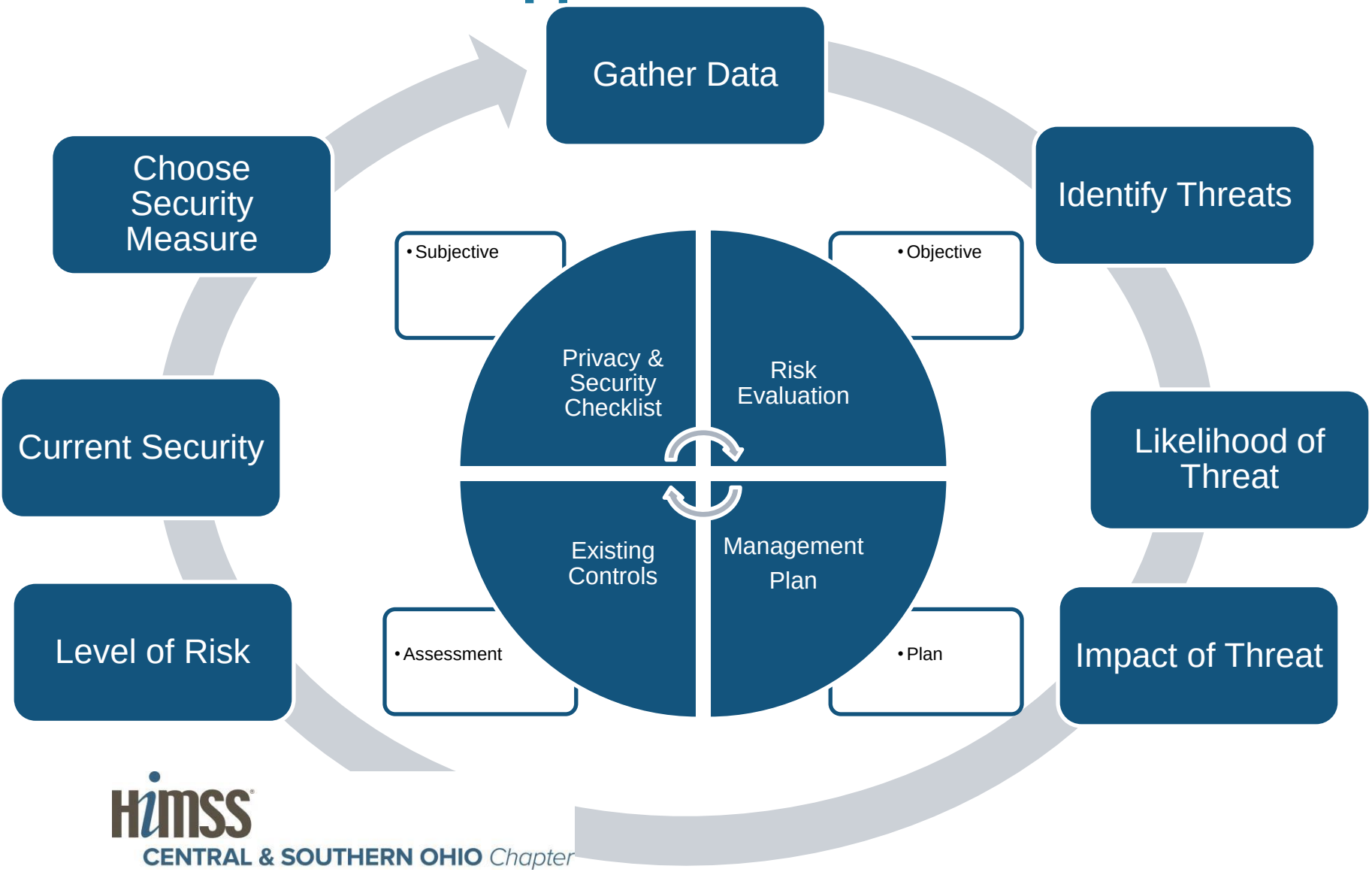
Is there a specific risk analysis method that I must follow?

- NO.
  - A risk analysis can be performed in countless ways. OCR has issued Guidance on Risk Analysis Requirements of the Security Rule.
  - Excerpt from 'Guidance on Risk Analysis Requirements under the HIPAA Security Rule'. Posted 7/14/2010.
    - "We understand that the Security Rule does not prescribe a specific risk analysis methodology, recognizing that methods will vary dependent on the size, complexity, and capabilities of the organization. Instead, the Rule identifies risk analysis as the foundational element in the process of achieving compliance, and it establishes several objectives that any methodology adopted must achieve."

Basic Steps to Meeting Regulation

- Establish “Culture of Compliance”
  - Leadership Is Critical
  - Training & Education
- Create An Audit File
- Create An Inventory Of All ePHI
  - Thorough & Accurate
  - Basis of Risk Analysis
- Conduct Full Scale Security Risk Analysis
- Develop Management Action Plan To Address Security Risk Analysis
  - Policies & Procedures Are Critical
- Communication Plan
  - Patients, Staff And Vendors
- Business Associate Agreements

Completing A Risk Analysis & Management Plan Modified SOAP Approach



HIMSS CENTRAL & SOUTHERN OHIO Chapter

An Accurate Inventory of all EPHI is Critical
-Potential Sources for EPHI

Document Imaging System	Operating Room / Surgery Management System	Billing System
Document Management System	Patient or Member Portal	Claims Collection
Email	Perinatal Care System	Claims System
Fax System	Pharmacy Management	3rd Party Clearinghouse / Interface System
File Servers	Pharmacy System	Complaints and Quality Events
MS Exchange Email	Picture Archiving and Communication System	Member or Patient Eligibility System
Network File Shares	Portal	Financial / General Accounting System
Authorization System	Privacy Breach Records	Internal Intranet Based Member Look up
Case Management	Provider Data Management System	Online Billing/Statements
Cath labs monitoring and reporting systems	Provider Portal	Payor Contract Management System
CPOE	Radiology Information System	Practice Management Software
EDI Transactions	Reporting System	Reinsurance Broker
EHR - Data Repository	Transcription System	Reinsurance Carrier
EHR System - Ambulatory	Vascular Studies	Transaction Services (EDI)
EKG Storage and Interpretation	Patient or Member Stratification System	Workflow Management
Endoscopy Information System	Materials Management System	Customer Relationship Management (CRM) System
Enterprise Medical Record System	Geriatric Health Management System	Interactive Voice Response (IVR) Eligibility
Geriatric Health Management System	Data Warehouse	
Emergency Department System	EHR System - Hospital	
ICU System	Health Information Management	
Laboratory Information System	Informatics	
Oncology Management System	Medical Informatics	
	Enterprise Resource Planning (ERP) System	
	Analysis and Reporting System (e.g., SAS)	

Asset Name	Location	creates, receives, maintains, or transmits	Encrypted	Critical	Cloud	Local

Facility Walk Through

Example

	Site	Practice 1 Name	Date:
	Contact:		Completed By:
ITEM	YES/ NO	CONTROL DESCRIPTION	NOTES
Physical Authentication		Method to determine who is authorized to access secure area of the office (e.g. badges, swipe cards, biometrics)	
Visitor Sign-In		Physical access authorization for visitor access to secure area of office (e.g. sign-in sheet, ID verification)	
Visitor Authentication		Verify access authorization before granting access to secure area (e.g. must have appointment)	
Secure Area Physically Protected		Access to secure access physically monitored or protected (e.g. receptionist monitors entry, locked door, or security camera)	

Completing A Risk Analysis & Management Plan Privacy & Security Assessment Example

164.308(a)(1)(ii)(C) TVS003	**Do you have formal sanctions against employees who fail to comply with security policies and procedures? (R)**	❑Complete ✓ Not Complete ❑ In Progress ❑ Unknown ❑ N/A

A formal sanction policy should include (not a complete list):

- Types of violations that require sanctions, including:
  - Accessing information that you do not need to know to do your job.
  - Sharing computer access codes (user name & password).
  - Leaving computer unattended while you are logged into PHI program.
- Recommended disciplinary actions include
  - Verbal or written reprimand
  - Retraining on privacy/security awareness, policies, HIPAA, HITECH, and civil and criminal prosecution
  - Letter of reprimand or suspension
  - Termination of employment or contract

Completing A Risk Analysis & Management Plan
Risk Analysis Example

164.308(a)(1)(ii)(C) TVS003	Do you have formal sanctions against employees who fail to comply with security policies and procedures? (R)	❑Complete ✓ Not Complete ❑ In Progress ❑ Unknown ❑ N/A

Risk	Risk Level	Recommended Controls	Priority	Selected Controls
No formalized sanction process for employees.	High	Information Security Policies . Develop training materials	Med	Use the Information Security Policies template.
Required Resources	**Respon-sible**	**Start/End Date**		**Comments / Maintenance**
2 weeks for development of policy	Practice Manager	9/22/15 – 10/4/15		Review policy annually

For each of the safeguards that are ‘not complete’ or ‘in progress’ or ‘unknown’ document the information above

For Physicians, Compliance Will Mean:

- Conducting and documenting a **risk analysis** of electronic protected health information (PHI) in the practice. Develop an appropriate management plan that will address the deficiencies and risks;
- Reviewing the practice's **policies and procedures** for when PHI is lost or stolen or otherwise improperly disclosed, and making sure staff members are trained in them;
- Ensuring that the electronic PHI practice holds is **encrypted** so that it cannot be accessed if it is lost or stolen ;

For Physicians, Compliance Will Mean:

- Modifying the practice's electronic health record (EHR) system so they can **flag information** a patient does not want shared with an insurance company;
- Having the ability to send patients their health information in an **electronic format**;
- Reviewing contracts with any vendors that have access to practice PHI; and
- Updating practice's notice of privacy practices.

QUESTIONS?

Contact:

Jim Carroll, Director

Northeast Central Ohio Regional Extension Center

Program of the Akron Regional Hospital Association

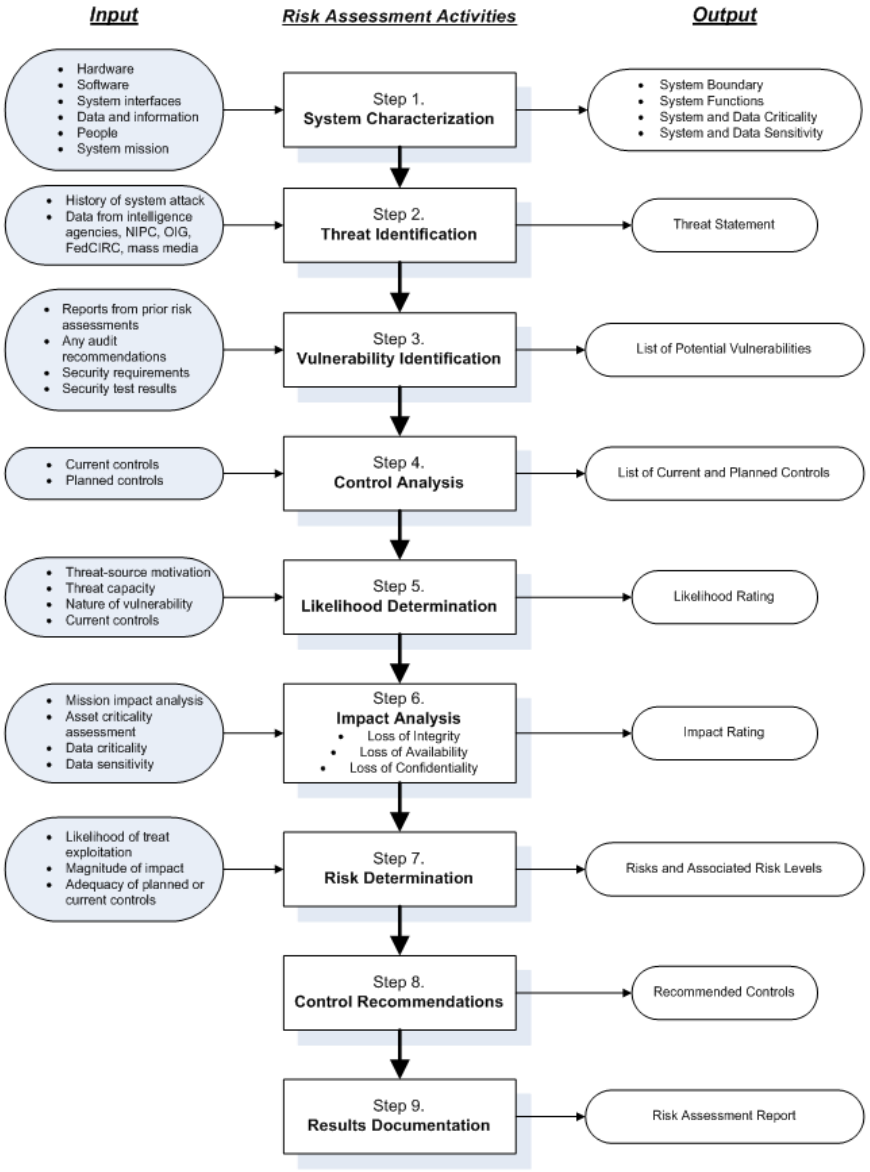
330-873-1500

jcarroll@arha.org

HIMSS CENTRAL & SOUTHERN OHIO *Chapter*

Risk Assessment Methodology Flowchart

NIST SP 800-30



This flowchart was taken directly from NIST SP 800-30

Information System Activity Review

164.308(a)(1)(ii)(D)
TVS014, TVS017, TVS019
	• Ensure EMR and other audit logs are enabled and monitored regularly. Email alerts also should be setup for login failures and other events.
	• Enabling and monitoring of Windows Security Event Logs (workstation and servers). It is also important to monitor the other Event Logs as well (Application and System Logs).
	• Monitoring of logs from networking equipment, i.e. switches, routers, wireless access points, and firewalls
	• Audit reduction, review, and reporting tools (i.e. a central syslog server) supports after-the-fact investigations of security incidents without altering the original audit records.
	• Continuous monitoring of the information system by using manual and automated methods.
	  ○ Manual methods include the use of designated personnel or outsourced provider that manually reviews logs or reports on a regular basis, i.e. every morning.
	  ○ Automated methods include the use of email alerts generated from syslog servers, servers and networking equipment, and EMR software alerts to designated personnel.
	• Track and document information system security incidents on an ongoing basis
	• Reporting of incidents to the appropriate personnel, i.e. designated Privacy Officer or Information Security Officer (ISO)
	• Use of central syslog server for monitoring and alerting of audit logs and abnormalities on the network, including:
	  ○ Account locked due to failed attempts
	  ○ Failed attempts by unauthorized users
	  ○ Escalation of rights
	  ○ Installation of new services
	  ○ Event log stopped
	  ○ Virus activity	