AMA
AMERICAN MEDICAL
ASSOCIATION

# Welcome to the AMA's SL2 Series: Security Risk Analysis

**September 13, 2017**

Your MISSION is Our MISSION

# Transforming Clinical Practice Initiative

- The Transforming Clinical Practice Initiative is designed to help clinicians achieve large-scale health transformation.

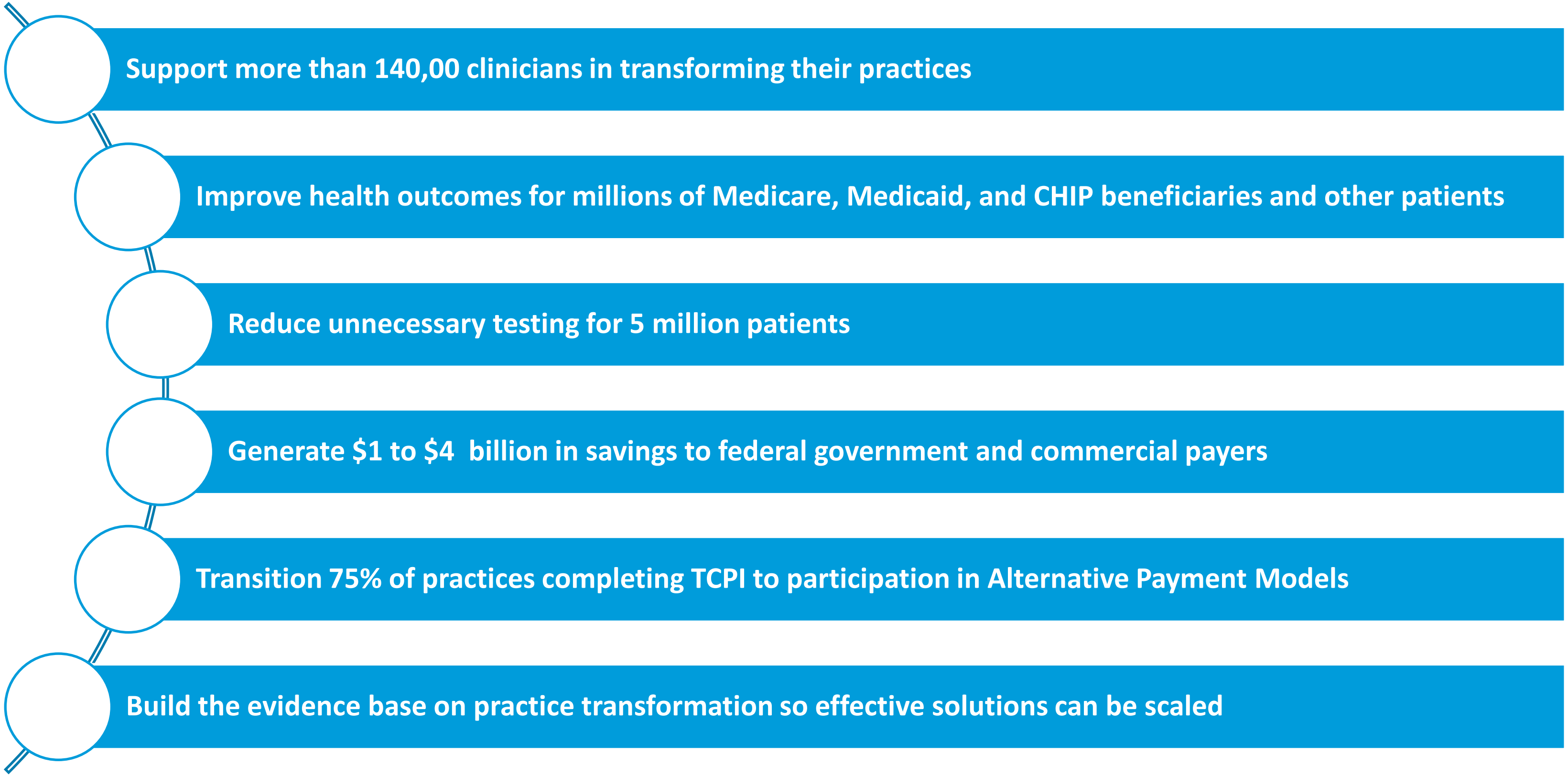
- The initiative is designed to support more than 140,000 clinician practices over the next four years in sharing, adapting and further developing their comprehensive quality improvement strategies.

- [https://innovation.cms.gov/initiatives/Transforming-Clinical-Practices/](https://innovation.cms.gov/initiatives/Transforming-Clinical-Practices/)

*AMA's TCPI work is supported by Funding Opportunity Number CMS-1L1-15-002 from the U.S. Department of Health & Human Services, Centers for Medicare & Medicaid Services.*

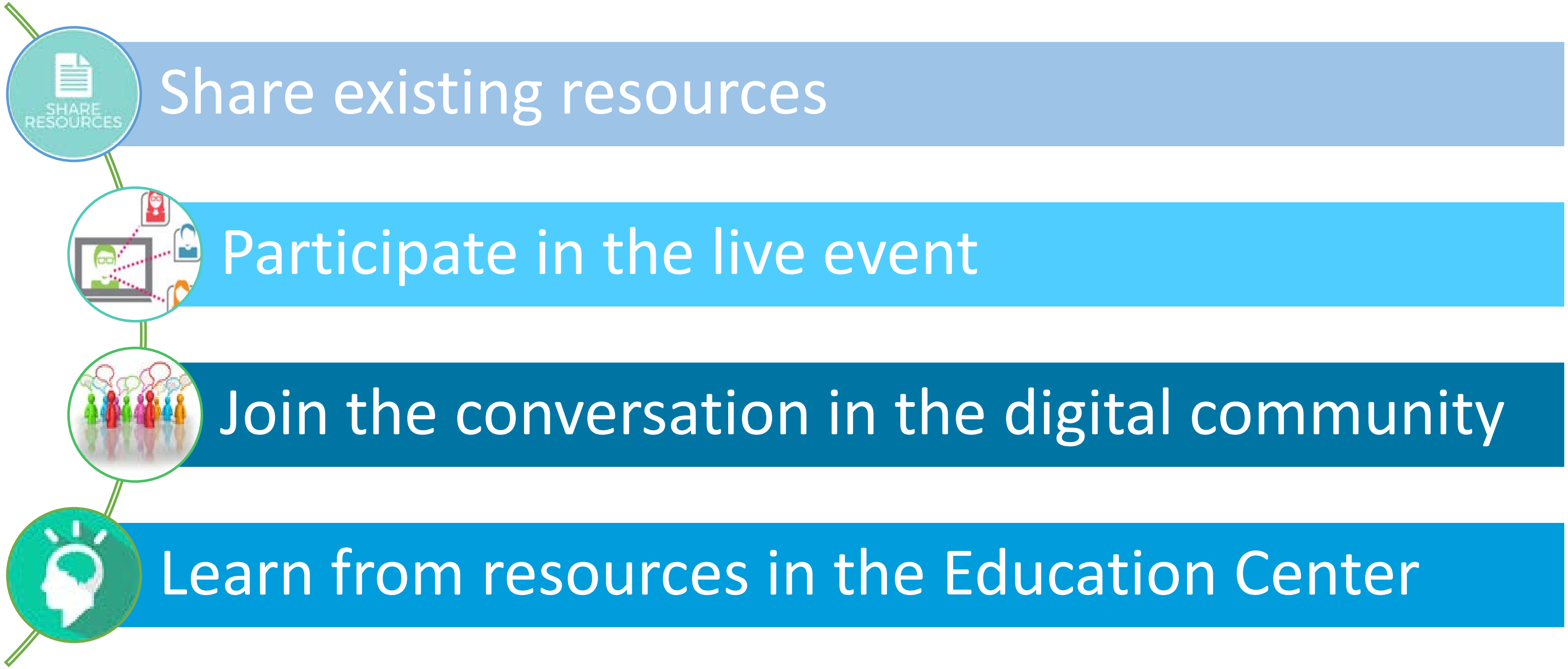
*The content provided is solely the responsibility of the AMA and faculty and do not necessarily represent the official views of HHS or any of its agencies*

# Transforming Clinical Practice Initiative Goals



- Support more than 140,00 clinicians in transforming their practices
- Improve health outcomes for millions of Medicare, Medicaid, and CHIP beneficiaries and other patients
- Reduce unnecessary testing for 5 million patients
- Generate $1 to $4  billion in savings to federal government and commercial payers
- Transition 75% of practices completing TCPI to participation in Alternative Payment Models
- Build the evidence base on practice transformation so effective solutions can be scaled

# AMA-SAN: Share, Listen, Speak, Learn (SL2) Series



Share existing resources

Participate in the live event

Join the conversation in the digital community

Learn from resources in the Education Center

# Presenter: Laura G. Hoffman

- Assistant Director, Department of Federal Affairs
  - Health information technology
  - HIPAA privacy and security
  - MACRA/Quality Payment Program
  - Cybersecurity

# Disclaimer

- This webinar has been prepared by the American Medical Association (AMA). The advice expressed during this webinar is solely the AMA's view and not necessarily the view of any other organization or association.  Neither the AMA nor the presenter are engaged in providing legal or other professional services.

# Today’s Presentation: Objectives

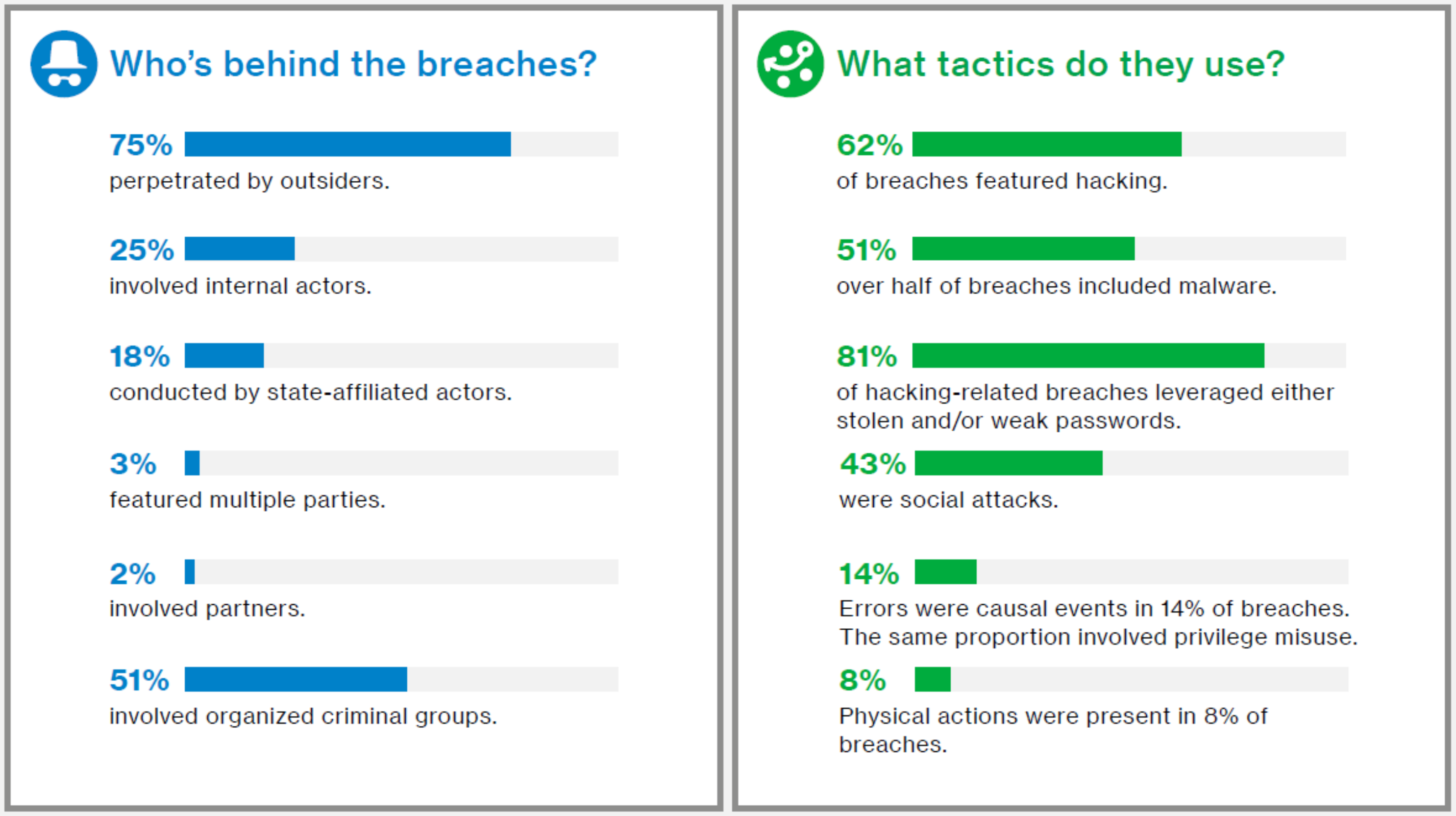
1. Understand why you should conduct a risk analysis.
2. Review requirements of the HIPAA Security Rule.
3. Identify critical elements of a comprehensive security risk analysis.

# Why Conduct a Risk Analysis?

# Why Conduct a Risk Analysis?

✓ Protect your patients’ health information.

# 2017 Data Breach Investigation Analysis*



## Who's behind the breaches?

**75%**
perpetrated by outsiders.

**25%**
involved internal actors.

**18%**
conducted by state-affiliated actors.

**3%**
featured multiple parties.

**2%**
involved partners.

**51%**
involved organized criminal groups.

## What tactics do they use?

**62%**
of breaches featured hacking.

**51%**
over half of breaches included malware.

**81%**
of hacking-related breaches leveraged either stolen and/or weak passwords.

**43%**
were social attacks.

**14%**
Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

**8%**
Physical actions were present in 8% of breaches.

* Verizon 2017 Data Breach Investigations Report - Executive Summary

# Why Conduct a Risk Analysis?

- ✓ Protect your patients’ health information.
- ✓ **Comply with federal law and regulation.**

# Risk Analysis Required by HIPAA – 45 CFR §164.308(a)

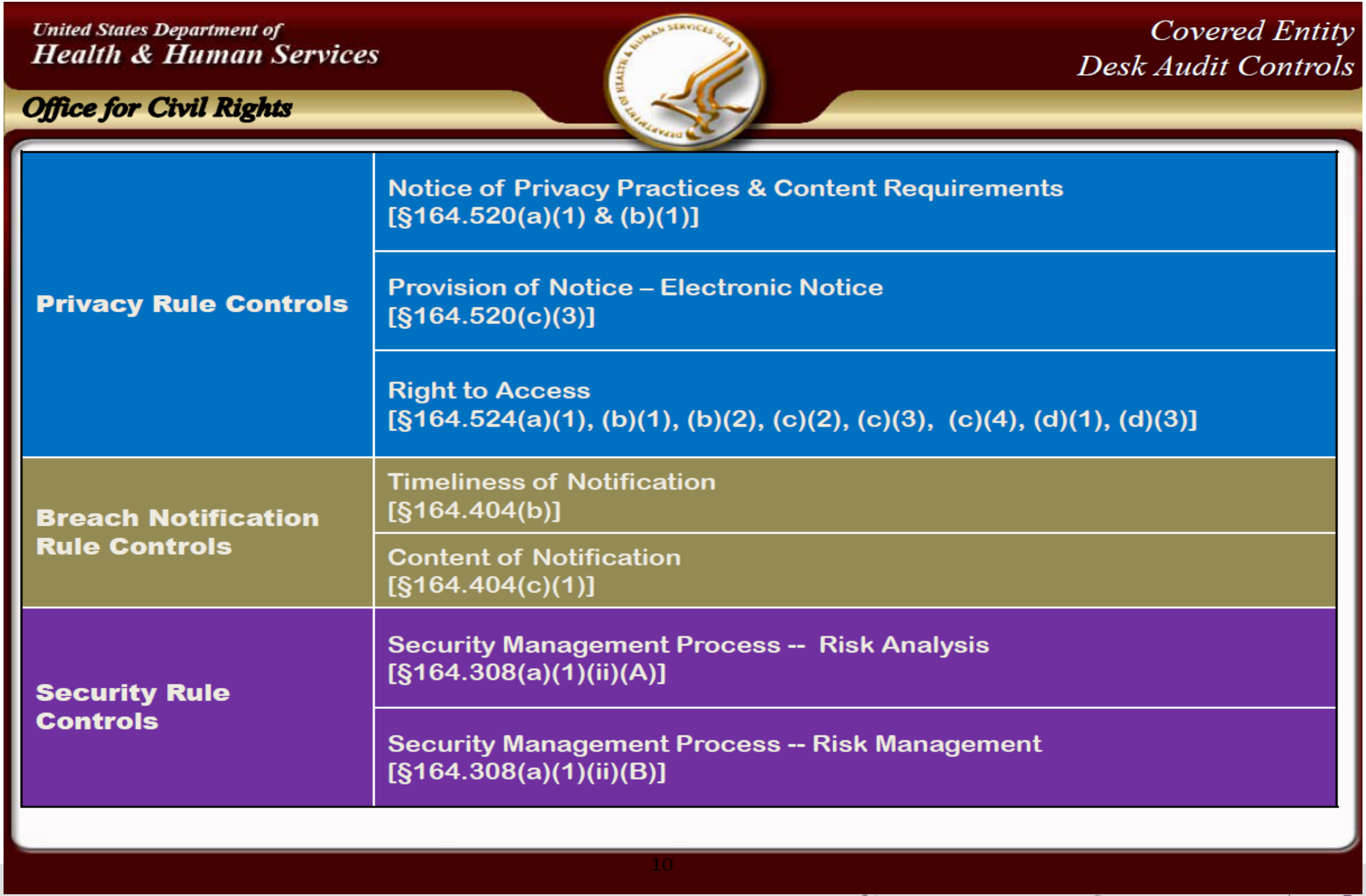
- **(a)** A covered entity or business associate must, in accordance with § 164.306:
- **(1) (i)*Standard: Security management process.*** Implement policies and procedures to prevent, detect, contain, and correct security violations.
- **(ii) *Implementation specifications:***
  - **(A)*Risk analysis (Required).*** 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 or business associate.

# OCR Investigations

- To date, the compliance issues investigated most are, in order of frequency:
  - Impermissible uses and disclosures of protected health information;
  - **Lack of safeguards of protected health information;**
  - Lack of patient access to their protected health information;
  - Use or disclosure of more than the minimum necessary protected health information; and
  - Lack of administrative safeguards of electronic protected health information.

# Examples from OCR

- Adult & Pediatric Dermatology – $150,000
  - Stolen unencrypted thumb drive
- Concentra Health Services – $1,725,220
  - Stolen laptops
- Affinity Health Plan – over $1.2 million
  - ePHI left on photocopier drives
- Hospice of Northern Idaho – $50,000
  - Unencrypted laptop stolen



United States Department of
Health & Human Services

Office for Civil Rights

## Covered Entity
## Desk Audit Controls

| | |
|---|---|
| **Privacy Rule Controls** | Notice of Privacy Practices & Content Requirements<br>[§164.520(a)(1) & (b)(1)] |
| | Provision of Notice – Electronic Notice<br>[§164.520(c)(3)] |
| | Right to Access<br>[§164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)] |
| **Breach Notification Rule Controls** | Timeliness of Notification<br>[§164.404(b)] |
| | Content of Notification<br>[§164.404(c)(1)] |
| **Security Rule Controls** | Security Management Process -- Risk Analysis<br>[§164.308(a)(1)(ii)(A)] |
| | Security Management Process -- Risk Management<br>[§164.308(a)(1)(ii)(B)] |

10

# Why Conduct a Risk Analysis?

- ✓ Protect your patients’ health information.
- ✓ Comply with federal law and regulation.
- ✓ **Position yourself for success in ACI component of the Quality Payment Program.**

# ACI performance category scoring: required measures (50% score)

| Objective | ACI Measure | Reporting Requirement |
|---|---|---|
| Protect patient health information | Security risk analysis | Yes/No statement |
| Electronic prescribing | E-prescribing | Numerator/ denominator |
| Patient electronic access | Provide patient access | Numerator/ denominator |
| Health information exchange | Send summary of care | Numerator/ denominator |
| Health information exchange (2015 CEHRT only) | Request/ accept summary of care | Numerator/ denominator |

# MU/ACI Requirement: Protect Patient Health Information

- Objective: Protect electronic protected health information (ePHI) **created or maintained by the CEHRT** through the implementation of appropriate technical, administrative, and physical safeguards.

- Security Risk Analysis Measure: In accordance with HIPAA…
  - Conduct or review a security risk analysis, including addressing the security of ePHI created or maintained by CEHRT
  - Implement security updates as necessary, and
  - Correct identified security deficiencies as part of the MIPS eligible clinician's risk management process.

# Why Conduct a Risk Analysis?

✓ Protect your patients' health information.

✓ Comply with federal law and regulation.

✓ Position yourself for success in ACI component of the Quality Payment Program.

✓ **Identify and prioritize areas of focus and risk (both internal and external) in your privacy and security program.**

✓ **Conserve resources.**

✓ **Practice sound management.**

✓ **Improve operational efficiency.**

✓ **Use as the basis for determining audit areas.**

# HIPAA Security Rule

# Important Definitions

- Electronic Protected Health Information (ePHI)
    - Individually identifiable health information;
    - Created, received, maintained, or transmitted;
    - By or on behalf of a covered entity; and
    - Relates to health care or payment.
- Covered entity: Health care providers, insurers, clearinghouses.
- Business associate: a person or entity who performs functions or activities on behalf of, or certain services for, a covered that involve the use or disclosure of PHI.

# Important Definitions: Vulnerability

- “*[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.*”
  - NIST Special Publication 800-30

- May be technical or non-technical.

# Important Definitions: Threat

- “*[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.*”
    - NIST Special Publication 800-30

- Threats can be natural, human, or environmental.

# Important Definitions: Risk

- *“The net mission impact considering (1) the probability that a particular [threat] will exercise (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 –*
  - *Unauthorized (malicious or accidental) disclosure, modification, or destruction of information*
  - *Unintentional errors and omissions*
  - *IT disruptions due to natural or man-made disasters*
  - *Failure to exercise due care and diligence in the implementation and operation of the IT system.”*
    - NIST Special Publication 800-30

# HIPAA Security Rule

- Covered entities must maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI:
  - Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  - Protect against reasonably anticipated, impermissible uses or disclosures; and
  - Ensure compliance by their workforce.

# Security Rule Standards: Administrative

- *Security Management Process –*
  45 CFR §164.308(a)(1)
  - Risk Analysis (R)
  - Risk Management (R)
  - Sanction Policy (R)
- *Workforce Security –*
  45 CFR §164.308(a)(3)(i)
  - Authorization and/or Supervision (A)
- *Security Awareness and Training –*
  45 CFR §164.308(a)(5)(i)
  - Password Management (A)
- *Contingency Plan –*
  45 CFR §164.308(a)(7)(i)
  - Data Backup Plan (R)
- *Business Associate Contracts –*
  45 CFR §164.308(b)(1)
  - Written Contract or Other Arrangement (R)

# Security Rule Standards: Physical

- *Facility Access Controls* – 45 CFR §164.310(a)(1)
    - Facility Security Plan (A)
    - Maintenance Records (A)
- *Workstation Use* – 45 CFR §164.310(b)
- *Device and Media Controls* – 45 CFR §164.310(d)(1)
    - Disposal (R)
    - Data Backup and Storage (A)

# Security Rule Standards: Technical

- *Access Controls* – 45 CFR §164.312(a)(1)
  - Unique User Identification (R)
  - Automatic Logoff (A)
- *Person or Entity Authentication* – 45 CFR §164.312(d)
- *Transmission Security* – 45 CFR §164.312(e)(1)
  - Encryption (A)

# Standards & Implementation Specifications

- Standards are requirements (18 of them)
- Implementation Specifications (ISs) are more detailed descriptions of methods or approaches Covered Entities can use to meet the standards
- ISs are either required or addressable –
    - Required: Must implement policies and/or procedures that meet what the implementation specification requires.
    - Addressable: Must assess whether it is a reasonable and appropriate safeguard in the entity’s environment
- If the covered entity chooses not to implement an addressable specification based on its assessment, it must document the reason and, if **reasonable and appropriate**, implement an equivalent alternative measure

# A Note on “Reasonable and Appropriate”

- Important: An addressable implementation specification is **not** optional.
- If a given addressable implementation specification is determined to be reasonable and appropriate, the covered entity must consider options for implementing it.
- Deciding which security measures to implement to address the standards and implementation specifications will depend on a variety of factors, including:
    - The entity's **risk analysis** – What current circumstances leave the entity open to unauthorized access and disclosure of ePHI?
    - The entity’s **security analysis** - What security measures are already in place or could reasonably be put into place?
    - The entity’s **financial analysis** - How much will implementation cost?

# How to Conduct a Risk Analysis

# Elements of a Risk Analysis

1. Identify the Scope
2. Assess the Risk
   - Collect Data
   - Identify and Document Potential Vulnerabilities
   - Assess Current Security Measures
3. Evaluate the Risk
   - Determine the Likelihood of Threat Occurrence
   - Determine the Potential Impact of Threat Occurrence
   - Determine the Level of Risk
   - Rank the Risk
4. Create a Plan to Address the Risk
5. Periodic Review and Updates to the Risk Analysis

# Elements of a Risk Analysis

1. **Identify the Scope**
2. Assess the Risk
   - Collect Data
   - Identify and Document Potential Vulnerabilities
   - Assess Current Security Measures
3. Evaluate the Risk
   - Determine the Likelihood of Threat Occurrence
   - Determine the Potential Impact of Threat Occurrence
   - Determine the Level of Risk
   - Rank the Risk
4. Create a Plan to Address the Risk
5. Periodic Review and Updates to the Risk Analysis

# Identify the Scope: What's in Your Network?

- CEHRT
- Medical devices
- Copiers
- Mobile devices
- Others?

# Identify the Scope: Administrative Safeguards

- **Standard: Security Management Process**
  - 45 CFR §164.308(a)(1): "*Implement policies and procedures to prevent, detect, contain and correct security violations.*"
- **IS: Risk Analysis (Required)**
  - 45 CFR §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 [ePHI] held by the covered entity.*"
- **Consider: Have you identified the ePHI within your organization?**

# Identify the Scope: Physical Safeguards

- **Standard: Facility Access Controls**
  - 45 CFR §164.310(a)(1): "*Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.*"
- **IS: Facility Security Plan (Addressable)**
  - 45 CFR §164.310(a)(2)(ii): "*Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.*"
- **Consider: Do your office policies and procedures identify controls to prevent unauthorized physical access, tampering, and theft of ePHI?**

# Identify the Scope: Technical Safeguards

- **Standard: Transmission Security**
  - 45 CFR §164.312(e)(1): "*Implement technical security measures to guard against unauthorized access to [ePHI] that is being transmitted over an electronic communications network.*"
- **IS: Encryption (Addressable)**
  - 45 CFR §164.312(e)(2)(ii): "*Implement a mechanism to encrypt [ePHI] whenever deemed appropriate.*"
- **Consider: Based on your required risk analysis, is encryption needed to protect the transmission of ePHI between your office and outside organizations? If not, what measures do you have in place to ensure the protection of this information?**

# Elements of a Risk Analysis

1. Identify the Scope
2. **Assess the Risk**
   - **Collect Data**
   - **Identify and Document Potential Vulnerabilities**
   - **Assess Current Security Measures**
3. Evaluate the Risk
   - Determine the Likelihood of Threat Occurrence
   - Determine the Potential Impact of Threat Occurrence
   - Determine the Level of Risk
   - Rank the Risk
4. Create a Plan to Address the Risk
5. Periodic Review and Updates to the Risk Analysis

# Assess the Risk: Internal Sources of Information

- Interviews with key personnel
  - Clinicians
  - Practice manager
  - HIPAA privacy officer
  - In-house counsel

- Review of Key Documents
  - Previous internal and external audit and consulting reports
  - Policies and procedures
  - Contracts with hospitals, physicians, vendors
  - Training course syllabi and attendance records

# Assess the Risk: External Sources of Information

- Government agency information
  - OCR enforcement alerts, guidance, bulletins, etc.
  - NIST alerts
  - ONC publications and newsletters
  - State Medicaid agency bulletins

- Professional sources
- Medical societies
- Trade associations
- Counsel and colleagues

# Elements of a Risk Analysis

1. Identify the Scope
2. Assess the Risk
   - Collect Data
   - Identify and Document Potential Vulnerabilities
   - Assess Current Security Measures
3. **Evaluate the Risk**
   - **Determine the Likelihood of Threat Occurrence**
   - **Determine the Potential Impact of Threat Occurrence**
   - **Determine the Level of Risk**
   - **Rank the Risk**
4. Create a Plan to Address the Risk
5. Periodic Review and Updates to the Risk Analysis

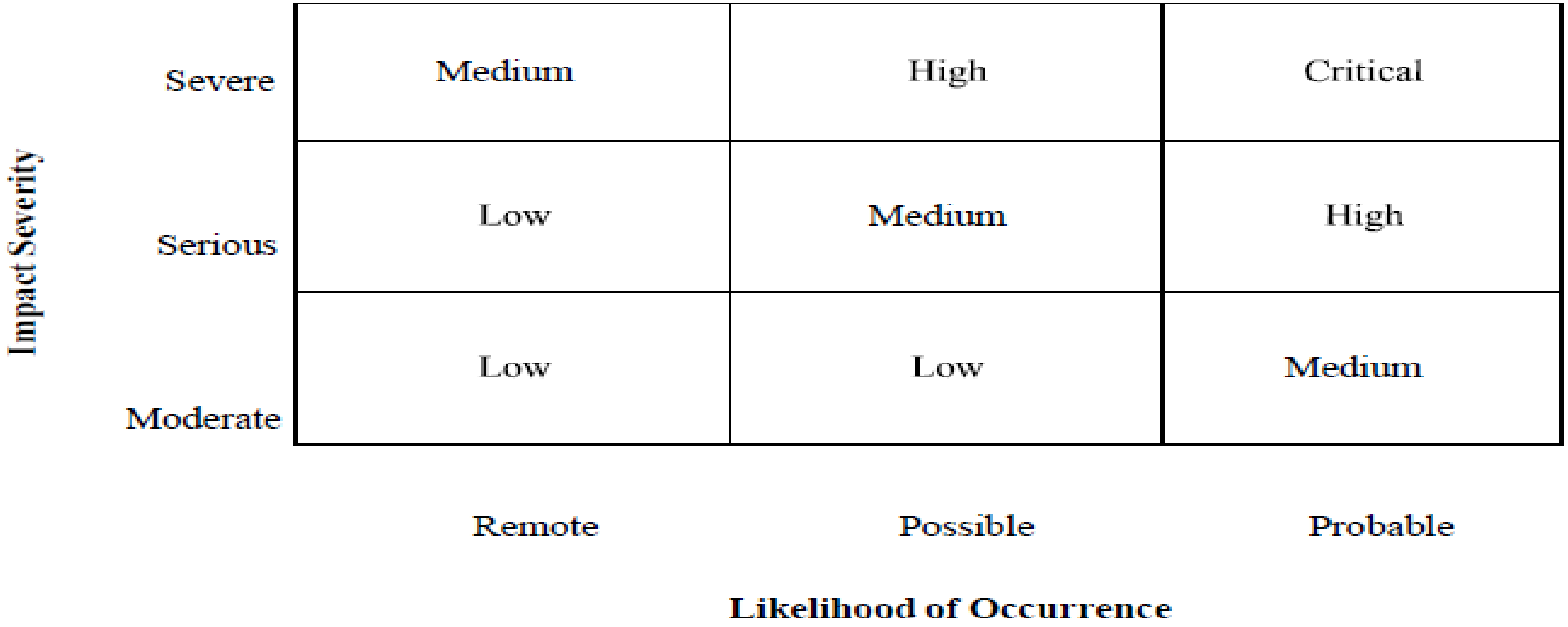
# Evaluate the Risk

Risk can be analyzed over multiple dimensions:

1) The likelihood that a violation would occur at the organization
2) The impact that a violation would have on the organization
3) The likelihood that the government would discover a violation

# Evaluate the Risk

Likelihood of Occurrence x Impact of Occurrence



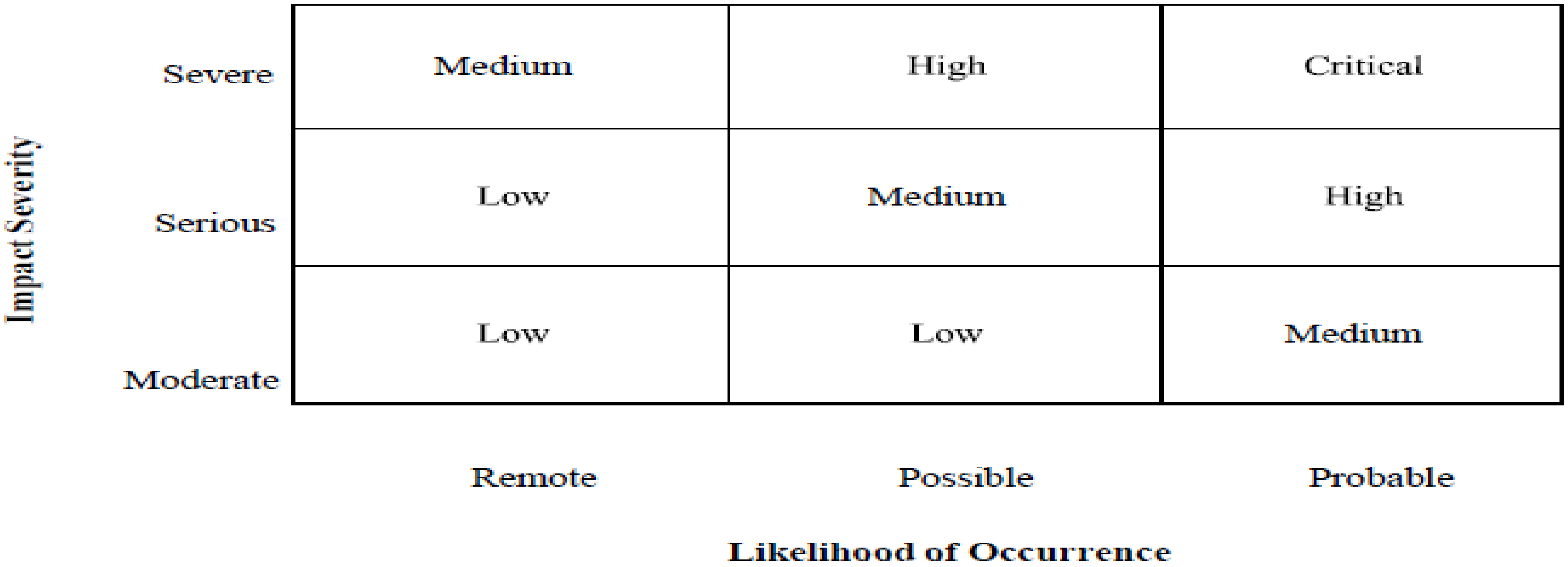
Impact Severity

| | Remote | Possible | Probable |
|---|---|---|---|
| Severe | Medium | High | Critical |
| Serious | Low | Medium | High |
| Moderate | Low | Low | Medium |

Likelihood of Occurrence

# Evaluate the Risk

## Example: Risk of lost laptop



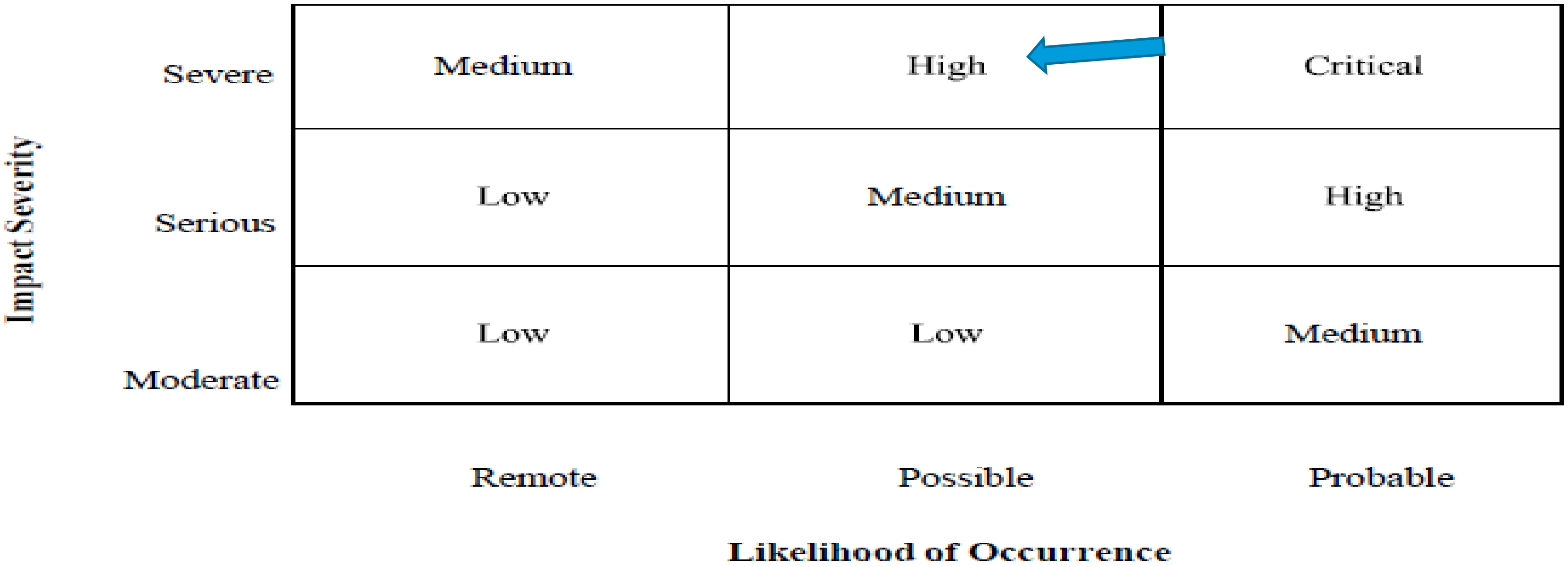
Impact Severity

|  | Remote | Possible | Probable |
|---|---|---|---|
| Severe | Medium | High | Critical |
| Serious | Low | Medium | High |
| Moderate | Low | Low | Medium |

Likelihood of Occurrence

# Evaluate the Risk

## Example: Risk of lost *unencrypted* laptop

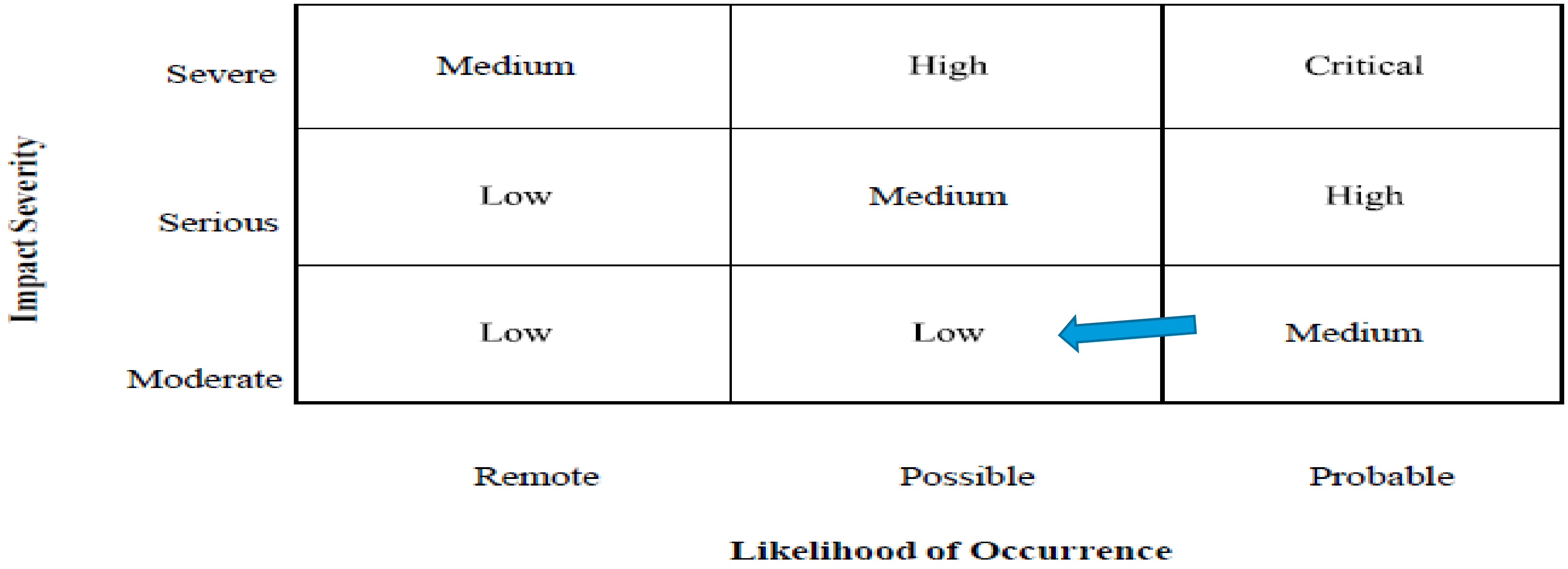


| Impact Severity | Remote | Possible | Probable |
|---|---|---|---|
| Severe | Medium | High | Critical |
| Serious | Low | Medium | High |
| Moderate | Low | Low | Medium |

Likelihood of Occurrence

# Evaluate the Risk

## Example: Risk of lost *encrypted* laptop



| Impact Severity | Remote | Possible | Probable |
|---|---|---|---|
| Severe | Medium | High | Critical |
| Serious | Low | Medium | High |
| Moderate | Low | Low | Medium |

Likelihood of Occurrence

# Ranking Risk Areas

Sample ranking:

1. Critical risks: EHR
2. High risks: Mobile devices
3. Medium: Information stored on copiers
4. Low: Theft of desktop computers

# Elements of a Risk Analysis

1. Identify the Scope

2. Assess the Risk
   - Collect Data
   - Identify and Document Potential Vulnerabilities
   - Assess Current Security Measures

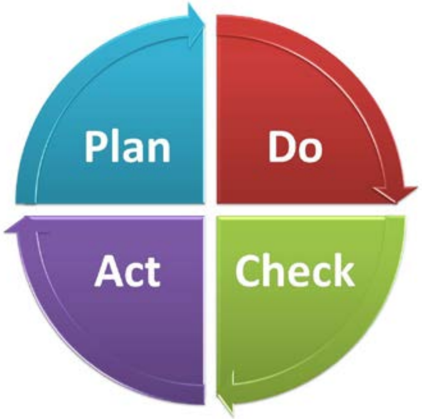
3. Evaluate the Risk
   - Determine the Likelihood of Threat Occurrence
   - Determine the Potential Impact of Threat Occurrence
   - Determine the Level of Risk
   - Rank the Risk

4. **Create a Plan to Address the Risk**

5. Periodic Review and Updates to the Risk Analysis

# What is a Work Plan?

- A work plan is a list of projects or actions that are conducted in response to a risk area.
- Objectives of a work plan can include:
    - Provision and maintenance of detailed documentation of HIPAA security.
    - Documentation of a practice's good faith effort to comply with federal and state security requirements.
    - Demonstration of the effectiveness of a security program in reducing risk.



# Contents of a Work Plan

- A work plan should contain:
  - Specific actions to be taken;
  - Party responsible for the action;
  - Resources required to complete the action;
  - Date work is scheduled, conducted, and completed; and
  - If possible, goals to measure effectiveness

# Sample HIPAA Security Work Plan

| Risk Area | Activities | Budget Request | Expected Outcomes | Person(s) Responsible | Completion Date |
|---|---|---|---|---|---|
| **Mobile Devices** | 1. Create inventory of cell phones and laptops<br>2. Review and update policy on use of mobile devices | *[$---]*<br>*[$---]* | 1. Inventory of devices to secure<br>2. Updated policy | Office manager<br>Privacy officer | Q2<br>Q1 |
| **Office Equipment** | 1. Hire contractor to erase hard drive on copier | *[$---]* | Written assurance that hard drive is clean. | Office manager | Q4 |

# A Note on Work Plan Design:
# New vs. Established Security Programs

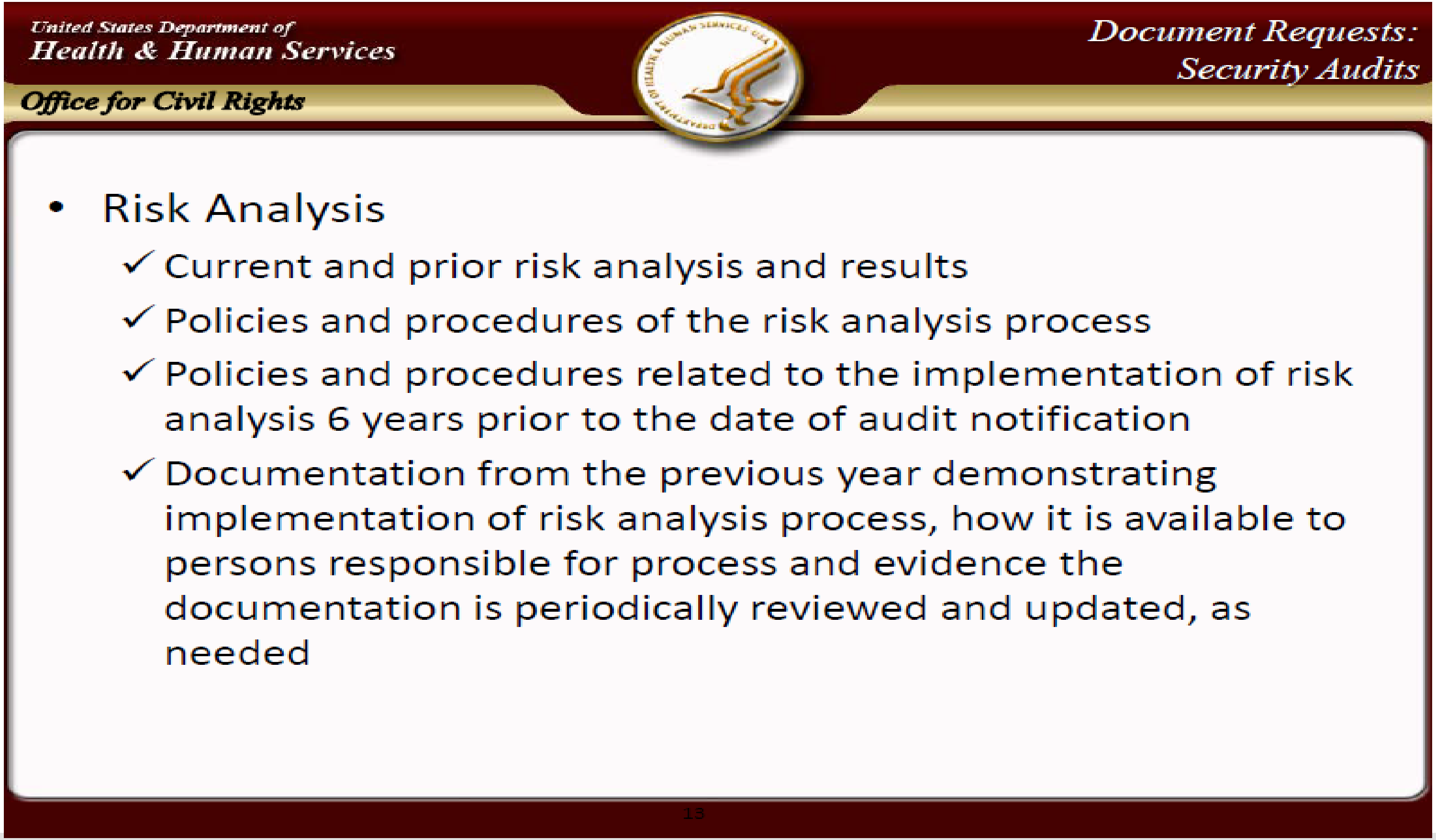
- Organizations developing a brand new security program:
  - Implement as many of the security standards as possible.
  - Create implementation timetable with available resources in mind.
- Organizations that have already implemented a security program:
  - Strengthen the effectiveness of the program.
  - Focus on risk areas.
- Organizations with a well-developed and well-functioning security program:
  - Focus on strengthening internal monitoring and auditing.
  - Focus on top risk areas.

# Elements of a Risk Analysis

1. Identify the Scope
2. Assess the Risk
   - Collect Data
   - Identify and Document Potential Vulnerabilities
   - Assess Current Security Measures
3. Evaluate the Risk
   - Determine the Likelihood of Threat Occurrence
   - Determine the Potential Impact of Threat Occurrence
   - Determine the Level of Risk
   - Rank the Risk
4. Create a Plan to Address the Risk
5. **Periodic Review and Updates to the Risk Analysis**

# Take Away Tips

# Document Requests: Phase 2 Audits



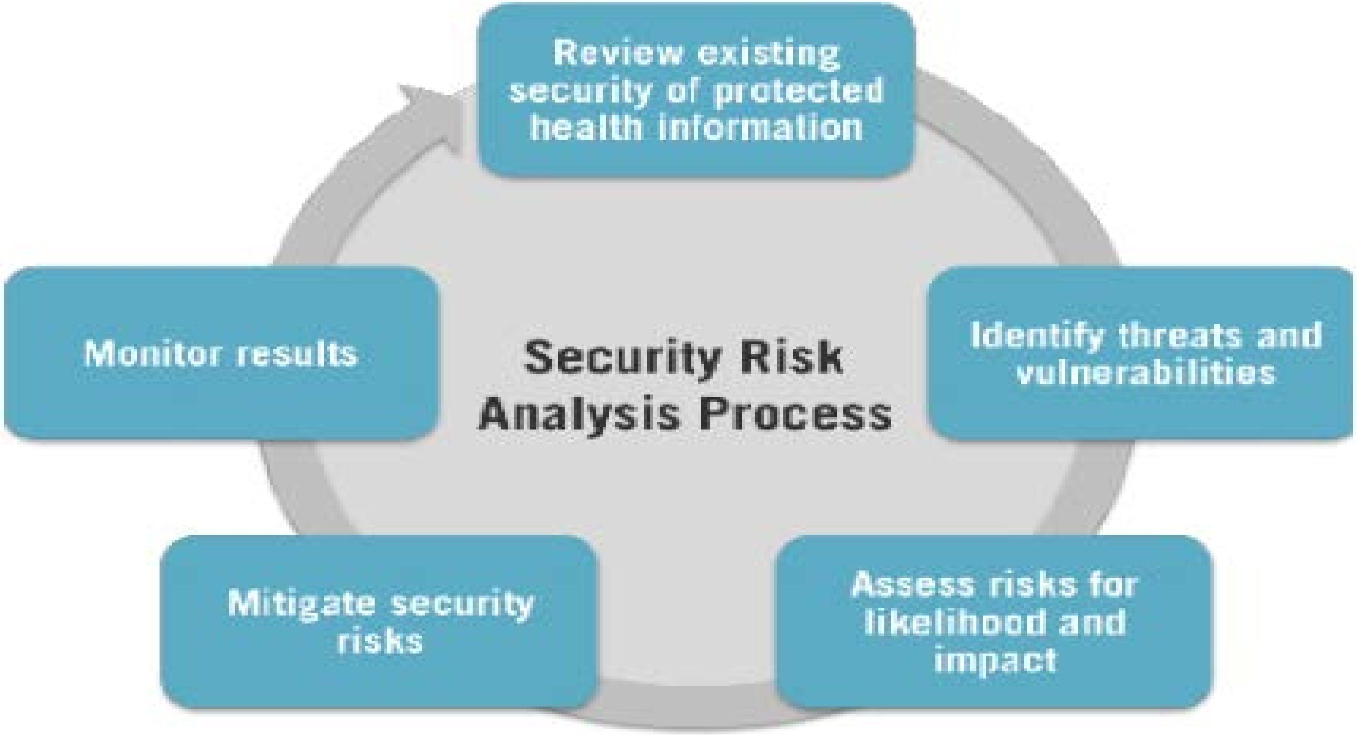
United States Department of
Health & Human Services

Office for Civil Rights

Document Requests:
Security Audits

- Risk Analysis
  - ✓ Current and prior risk analysis and results
  - ✓ Policies and procedures of the risk analysis process
  - ✓ Policies and procedures related to the implementation of risk analysis 6 years prior to the date of audit notification
  - ✓ Documentation from the previous year demonstrating implementation of risk analysis process, how it is available to persons responsible for process and evidence the documentation is periodically reviewed and updated, as needed

# Security Risk Analysis Process



Review existing security of protected health information
Identify threats and vulnerabilities
Assess risks for likelihood and impact
Mitigate security risks
Monitor results
Security Risk Analysis Process

# Recommended Security Rule Policies & Procedures (1)

- Security Officer Assigned Responsibility
- Security Risk Assessment & Evaluation
- Information System Activity Review
- Sanction Policy
- Use and Disclosure of Confidential Information Policy
- Workforce Confidentiality Agreement
- Workforce Termination Procedures
- Access Authorization and Control Policy
- Password Management
- Emergency Mode Operation
- Protection from Malicious Software
- Workforce Awareness and Training
- Security Incident Response and Report

# Recommended Security Rule Policies & Procedures (2)

- Hardware and Software Asset Inventory
- Data Backup Plan
- Disaster Recovery and Business Continuity Plan
- Applications and Data Criticality Analysis
- Business Associates Agreements
- Physical Security and Facility Maintenance Review
- Workstation Use Policy
- Disposal and Media Reuse
- User Identification and Authentication
- Technical Vulnerability Assessment and Controls
- Security Audit Policy
- Documentation
- Policies and Procedures Periodic Review

# Resources

- OCR Risk Analysis Guidance:
  - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf
- ONC Security Risk Assessment Tool:
  - https://www.healthit.gov/providers-professionals/security-risk-assessment
- AMA Security Rule and Risk Analysis webpage:
  - https://www.ama-assn.org/practice-management/hipaa-security-rule-risk-analysis :
- OCR Security Rule Guidance:
  - https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html?language=es
- OCR Security Rule FAQs:
  - ttps://www.hhs.gov/hipaa/for-professionals/faq/security-rule
- CMS Basics of Risk Analysis and Risk Management:
  - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf?language=es

# Next Steps

# ***Share, Listen,*** Speak, Learn about Security Risk Analysis

## Share

- HIPAA Security Rule & Risk Analysis
- HIPAA Privacy and Security Toolkit:  Helping Your Practice Meet New Compliance Requirements
- HIPAA Security Rule:  Frequently Asked Questions Regarding Encryption of Personal Health Information

## Listen

- Link to the recorded webinar will be provided in the post-webinar survey email

# Share, Listen, ***Speak, Learn*** about Security Risk Analysis

## Speak

- Online discussion: How to conduct a security risk*

## Learn in the AMA Education Center and other resources

- The Nuts and Bolts of Achieving HIPAA Security Rule Compliance through Effective Risk Assessment
- HIMSS Episode #46:  The Nuts and Bolts of Achieving HIPAA Security Rule Compliance through Effective Risk Assessment

** Apart of the AMA Running Your Practice online community*

# FYI…

Post-webinar evaluation:

- Complete the survey now

Next scheduled webinars:

- Thriving Under MIPS - Where to start? Breaking down the complexity of MIPS
  Wednesday, October 18th, 12 noon CST
  Registration link: https://cc.readytalk.com/r/xmcj9kl1jzo6&eom

- Quality Improvement - Root cause analysis: Digging deep to improve
  Wednesday, November 29th, 12 noon CST
  Registration link: https://cc.readytalk.com/r/aobwvje4lb2v&eom

Your MISSION is Our MISSION

AMA
AMERICAN MEDICAL ASSOCIATION