1/18/2012

MeHI
Massachusetts
eHealth Institute

A Division of the
Massachusetts
Technology Collaborative

Privacy & Security: Fundamentals of a Security Risk Analysis

Preparing for Meaningful Use Measure 15

Why Are We Here?

Connecting America for Better Health
The Office of the National Coordinator for Health Information Technology ™

- Privacy and Security is a priority for ONC
  - Consistency among Regional Extension Centers

- CMS's HIPAA Compliance Review Analysis
  - Risk Analysis was at top of list, where organizations struggled to comply
    - Did not perform a risk assessment
    - Had outdated risk assessment
    - Did not address all potential areas of risk

- HITECH Act added more stringent breach regulations
  - Increased levels of culpability for some violations
  - Significant increases to the minimum penalty
  - HHS posts a list of breaches affecting 500 or more individuals
  - HIPAA Privacy and Security Audit Program

Breach Notifications

- Breach occurs when unsecured PHI (i.e., not encrypted or destroyed) is impermissibly used or disclosed creating a significant risk of financial, reputational, or other harm

- Large breach – affects 500 or more
  - Report to OCR
  - OCR contacts covered entity to verify report
  - Report will be posted on OCR website
  - OCR will investigate
  - CE reports to individuals and media

- Small breach – affects less than 500
  - May report to OCR at end of year
  - OCR may investigate

Large Breach Statistics

- September 2009 – October 2011
- 364 large breaches
- Almost 18 million individuals affected

Top 3 breaches by type:

1. Theft
2. Unauthorized Access/ Disclosure
3. Loss

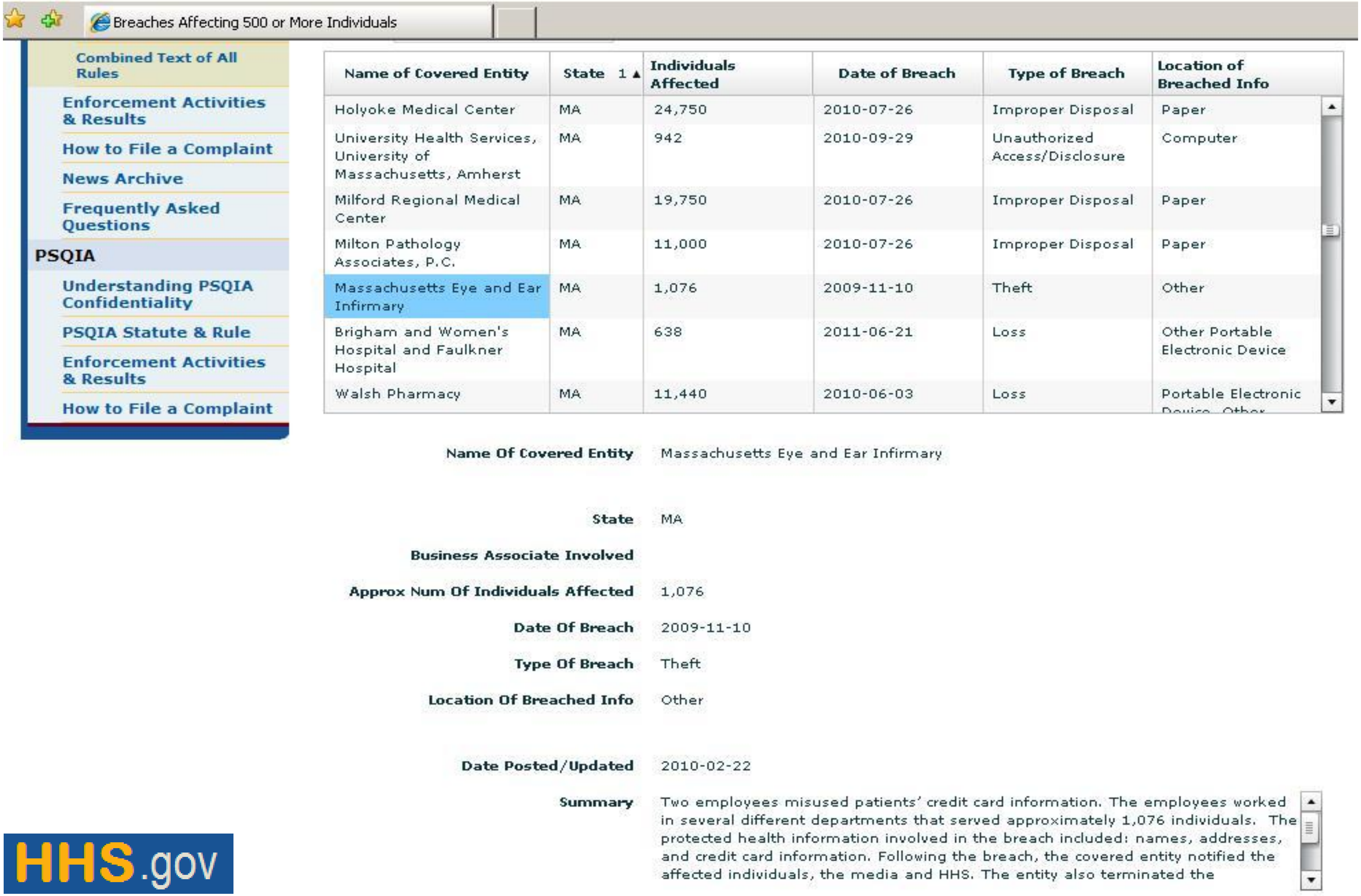
Top 3 breaches by media:

1. Paper
2. Laptop
3. Desktop

MeHI Massachusetts eHealth Institute

A Division of the Massachusetts Technology Collaborative

OCR Reported Breaches Page (aka Wall of Shame!)



Combined Text of All Rules

Enforcement Activities & Results

How to File a Complaint

News Archive

Frequently Asked Questions

PSQIA

Understanding PSQIA Confidentiality

PSQIA Statute & Rule

Enforcement Activities & Results

How to File a Complaint

Name of Covered Entity	State 1 ▲	Individuals Affected	Date of Breach	Type of Breach	Location of Breached Info
Holyoke Medical Center	MA	24,750	2010-07-26	Improper Disposal	Paper
University Health Services, University of Massachusetts, Amherst	MA	942	2010-09-29	Unauthorized Access/Disclosure	Computer
Milford Regional Medical Center	MA	19,750	2010-07-26	Improper Disposal	Paper
Milton Pathology Associates, P.C.	MA	11,000	2010-07-26	Improper Disposal	Paper
Massachusetts Eye and Ear Infirmary	MA	1,076	2009-11-10	Theft	Other
Brigham and Women's Hospital and Faulkner Hospital	MA	638	2011-06-21	Loss	Other Portable Electronic Device
Walsh Pharmacy	MA	11,440	2010-06-03	Loss	Portable Electronic Device, Other

Name Of Covered Entity	Massachusetts Eye and Ear Infirmary
State	MA
Business Associate Involved	
Approx Num Of Individuals Affected	1,076
Date Of Breach	2009-11-10
Type Of Breach	Theft
Location Of Breached Info	Other
Date Posted/Updated	2010-02-22
Summary	Two employees misused patients' credit card information. The employees worked in several different departments that served approximately 1,076 individuals. The protected health information involved in the breach included: names, addresses, and credit card information. Following the breach, the covered entity notified the affected individuals, the media and HHS. The entity also terminated the

HHS.gov

Top 5 Security Rule Issues Investigated by OCR

- HHS Office for Civil Rights Administers HIPAA compliance
- HIPAA Security Rule responsibility changed from CMS to OCR (July 2009)

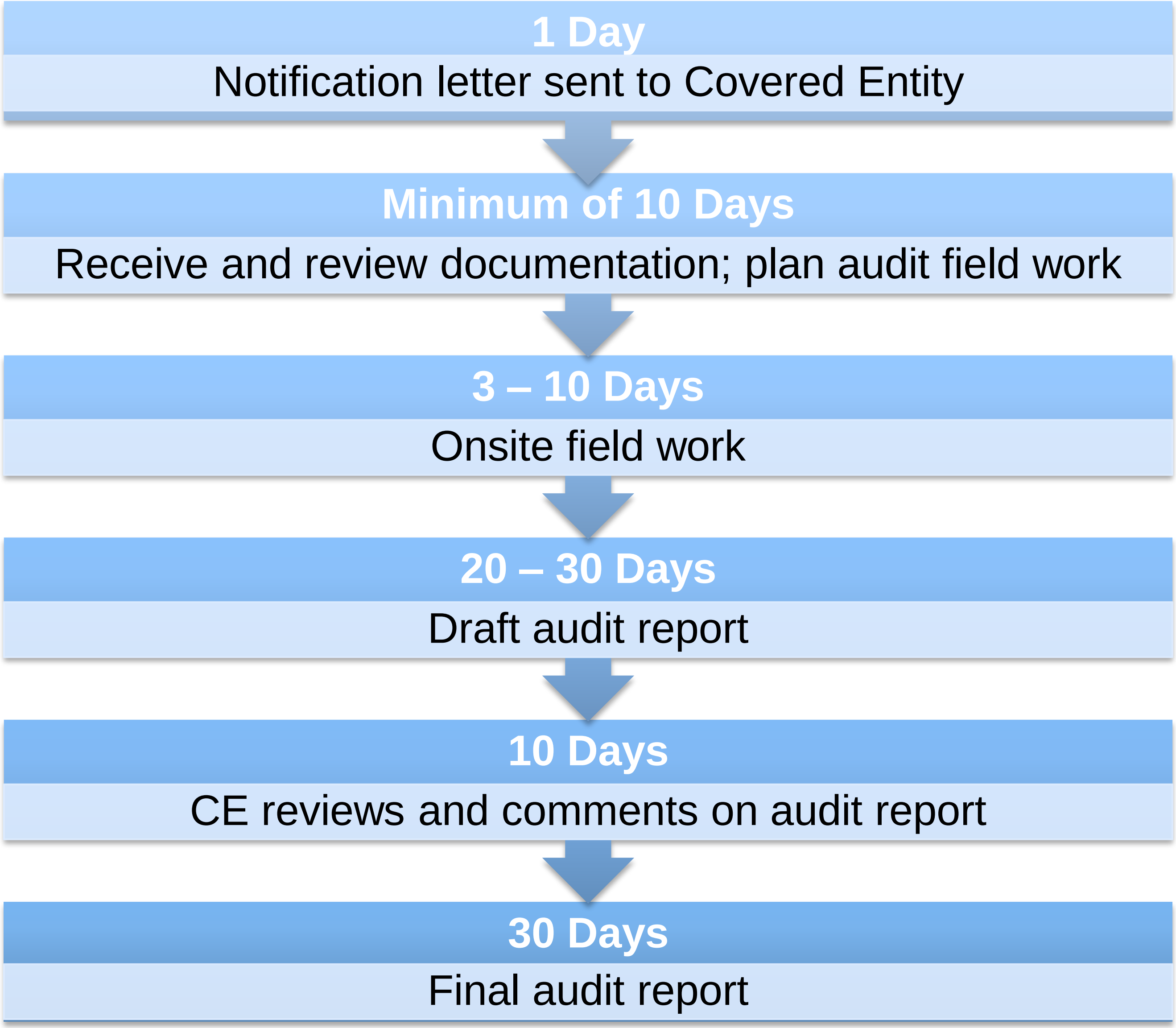
1. Response and Reporting
2. Awareness and Training
3. Access Control
4. Information Access Management
5. Workstation Security

OCR HIPAA Privacy & Security Audit Program

- HITECH Act requires HHS to perform periodic audits
- Pilot Program to assess privacy and security compliance
- Up to 150 Covered Entities to be audited
- November 2011 through December 2012
- All covered entities are eligible for audits
  - Individual providers
  - Organizational providers
  - Health plans
  - Health care clearinghouses

- Business Associates will be included in future audits

Audit Process (Elapsed Time)



1 Day

Notification letter sent to Covered Entity

Minimum of 10 Days

Receive and review documentation; plan audit field work

3 – 10 Days

Onsite field work

20 – 30 Days

Draft audit report

10 Days

CE reviews and comments on audit report

30 Days

Final audit report

What is a Security Risk Analysis?

- First step in identifying and implementing security safeguards
- Foundation upon which security activities are built
- Tool to develop and maintain strategy for protecting ePHI:
  - ***Confidentiality***
  - ***Integrity***
  - ***Availability***
  - ***(CIA?!)***
- Identifies potential:
  - ***Vulnerabilities***
  - ***Threats***
  - ***Risks***

CIA??

Not the Central Intelligence Agency or the Culinary Institute of America!

- Confidentiality
  - The nondisclosure of information except to another authorized person.
  - The ethical principle or legal right that a health professional will hold secret all information relating to a patient.
- Integrity
  - The state of being whole, entire, or undiminished.
  - The accuracy and consistency of data.
  - Protection of data from accidental or unauthorized intentional change.
- Availability
  - Present and ready for use.
  - Accessibility of information in a usable format.
  - Available for authorized users when the data is needed.

Key Terms Defined

Adapted from NIST SP 800-30

- Vulnerability

  "Flaw or weakness in system security procedures, design, implementation, or internal control that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy."

  - Non-technical (e.g., ineffective or non-existent policies, procedures, standards or guidelines)
  - Technical (e.g., flaws, weaknesses in IT systems; incorrectly implemented or configured systems)

- Threat

  "The potential for a person or thing to exercise a specific vulnerability."

  - Natural (e.g., floods, earthquakes, tornadoes, etc.)
  - Human
    - Intentional (e.g., network attacks, malicious software upload, unauthorized access to ePHI)
    - Unintentional (e.g., inadvertent data entry or deletion, inaccurate data entry)

- Risk

  "The net mission impact considering 1) the probability that a particular threat will exercise a particular vulnerability, and 2) the resulting impact if this should occur. Risks arise from:

  - Unauthorized 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"

Why do a Security Risk Analysis?

In no particular order of importance!

- Meaningful Use
  - Core Measure 15
- HIPAA
  - Security Rule
- It’s the right thing to do to help protect patients’ health information

Core Measure 15: Protect Electronic Health Information

Objective:

Protect electronic health information created or maintained by the 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 its risk management process.

Attestation:

Yes/No

Requirements for a "Yes" Attestation

- Conducted or reviewed a Security Risk Analysis of certified EHR
  - Per HIPAA Security Rule, 45 CFR 164.308(a)(1)
- Implemented security updates as necessary
  - Updated software for certified EHR
  - Changes in workflow processes
  - Changes in storage methods
  - Any other corrective action to eliminate identified security deficiencies
- Corrected identified security deficiencies
  - Prior to reporting period *OR*
  - During the reporting period
- New review for each subsequent reporting period

MeHI Massachusetts eHealth Institute | A Division of the Massachusetts Technology Collaborative

HIPAA Security Rule

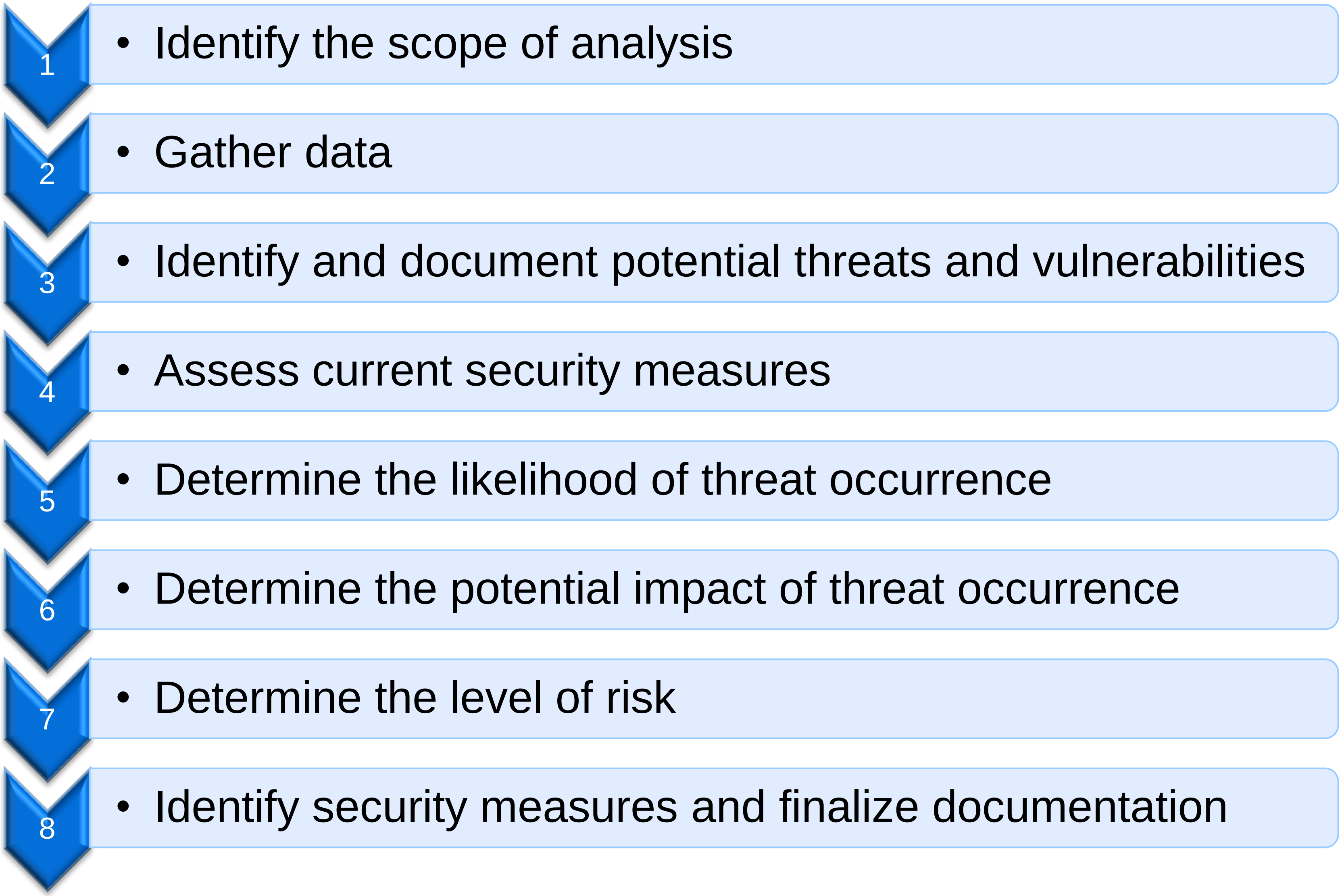
- Risk Analysis
  - §164.308(a)(1)(ii)(A)
  - "…conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information…"

- Risk Management
  - §164.308(a)(1)(ii)(B)
  - "…implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level…"

Many Methods Available!

- No specific methodology or tool prescribed in Security Rule
- No single method that guarantees compliance
- Methodologies will vary based on organization’s:
  - Size
  - Complexity
  - Capabilities

Key Elements of a Security Risk Analysis



1. Identify the scope of analysis
2. Gather data
3. Identify and document potential threats and vulnerabilities
4. Assess current security measures
5. Determine the likelihood of threat occurrence
6. Determine the potential impact of threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation

1. Identify the Scope of the Analysis

- Potential risks and vulnerabilities to:
  - Confidentiality
  - Integrity
  - Availability

- Of ePHI that a covered entity:
  - Creates
  - Maintains
  - Transmits

- Includes ePHI in all forms of electronic media, including:
  - Hard drives
  - CDs
  - DVDs
  - Smart cards
  - PDAs
  - USB drives
  - Etc., etc.

2. Gather Data

- Identify where the ePHI is:
  - Stored
  - Received
  - Maintained
  - Transmitted

- Gather relevant data by:
  - Reviewing past and/or existing projects
  - Performing interviews
  - Reviewing documentation
- Data on ePHI gathered must be documented

3. Identify & Document Potential Threats & Vulnerabilities

1. Identify and document threats – “reasonably anticipated”
   - Natural
   - Human
   - Environmental

   - Human threats are greatest concern
     - Employees – most common source
     - Ex-employees
     - Hackers; criminals
     - General public
     - Vendors
     - Customers; visitors

2. Identify and document vulnerabilities
   - Technical
     - IS assessments
     - IS security testing
     - Public vulnerability lists and advisories (Via internet and Business Associates)
   - Non-technical
     - Previous Risk Analysis documentation
     - Audit/security review reports

4. Assess Current Security Measures

Goal = To analyze current security measures implemented to minimize or eliminate risks to ePHI

- Security measures
  - Technical
    - Access controls
    - Identification
    - Authentication
    - Encryption methods
    - Automatic logoff
    - Audit controls
  - Non-technical
    - Policies and procedures
    - Standards
    - Guidelines
    - Accountability and responsibility
    - Physical and environmental

Output = Documentation of security measures used to safeguard ePHI

5. Determine the Likelihood of Threat Occurrence

Goal = Determine the level of risk and prioritize risk mitigation efforts

- Consider each potential threat and vulnerability combination
- Rate them by likelihood/probability that combination would occur
- Express likelihood ratings (e.g., high, medium, low *or* 1, 2, 3)
- Probability exists that a threat will trigger or exploit one or more vulnerabilities
  - *High* – e.g., absence or inadequate security controls *and* located in a flood zone
  - *Medium* – e.g., lack of security controls
  - *Low* – e.g., improper configuration of security controls

Output = Documentation of all threat and vulnerability combinations with associated likelihood ratings

6. Determine the Potential Impact of Threat Occurrence

Goal = Measure impact of potential outcomes; prioritize risk mitigation plans

- Most common outcomes
  - Unauthorized access to or disclosure of ePHI
  - Permanent loss or corruption of ePHI
  - Temporary loss or unavailability of ePHI
  - Loss of financial cash flow
  - Loss of physical assets

- Qualitative Method
  - Rates magnitude of potential impact
  - High, medium, low
  - Most common method to measure impact of risk
  - Measures tangible and intangible impacts (e.g., loss of public confidence, loss or credibility)

- Quantitative Method
  - Measures tangible potential impact
  - Numeric value associated with cost (e.g., repair or replacement costs for lost or stolen assets)
  - Good for cost-benefit analysis; difficult for intangibles

Output = Documentation of all impacts and ratings associated with occurrence of threats

7. Determine the Level of Risk

- Risk level determined by:
  - Analyzing values assigned in steps 5 and 6
  - Assigning a risk level based on assigned likelihood and impact level
  - Using a risk level matrix

Likelihood	Impact		
	High	Medium	Low
High			
Medium			
Low			

- Label each risk level with action description for decision making
  - General timeline
  - Type of response needed
  - Assists in prioritizing risk management efforts

Output = 1) Documented risk levels for all threat and vulnerability combinations identified during Risk Analysis

2) List of corrective actions to mitigate each risk level

8. Identify Security Measures & Finalize Documentation

- Identify actions to manage risk
- Identify security measures to be used to reduce risk to *reasonable and appropriate levels*
- Final step is to document Risk Analysis
  - Security Rule requires documentation
  - No specific format in Security Rule
  - Risk Analysis report should document:
    - Risk Analysis process
    - Output of each step
    - Initial identification of security measures

- Risk Analysis documentation is a direct input to the Risk Management process

……to be continued!

Sample Topics of Interest for Audits

- Establishing and terminating users' access to systems with ePHI.
- Emergency access to electronic information systems.
- Inactive computer sessions (periods of inactivity).
- Recording and examining activity in information systems that contain/use ePHI.
- Risk Analyses of information systems that house or process ePHI.
- Employee violations (sanctions).
- Electronically transmitting ePHI.
- Preventing, detecting, containing and correcting violations (incident reports).
- Regularly reviewing records of IS activity (audit logs, access reports, security incident tracking reports).
- Creating, documenting and reviewing exception reports or logs.
- Monitoring systems and the network, including all network perimeter devices (firewalls, routers).

More Topics of Interest for Audits

- Physical access to information systems and the facility in which they reside.
- Establishing security access controls.
- Remote access activity (network infrastructure, platform, access servers, authentication, and encryption software).
- Internet usage.
- Wireless security (transmission and usage).
- Maintenance/repairs of hardware, walls, doors, and locks in sensitive areas.
- Terminating an electronic session and encrypting and decrypting ePHI.
- Password and server configurations.
- Anti-virus software.
- Network remote access.
- Computer patch management.

Useful Resources

HIPAA Security Rule Educational Paper Series:

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

CMS Meaningful Use Specifications:

https://www.cms.gov/EHRIncentivePrograms/Downloads/EP-MU-TOC.pdf

NIST Risk Management Guide for IT Systems:

http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

ONC Health IT:

http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__home/1204

Office for Civil Rights – Health Information Privacy:

http://www.hhs.gov/ocr/privacy/index.html