PHYLLIS PATRICK + Associates

The Risk Analysis/Risk Management Cycle: Foundation for an Effective Security and Privacy Program

HCCA Webinar

September 25, 2014

Phyllis A. Patrick, MBA, FACHE, CHC, CISM

Topics

- Risk Analysis/Risk Management Requirements and Key Concepts
- Establishing an Effective RA/RM Program: Objectives, Approaches, Mitigation and Reporting
- Using the RA/RM Program to Improve Your Information Security and Privacy Program

Security Rule: It's been more than 10 years!

- Have you fully implemented the HIPAA Security Rule?
- Are you complying with the Risk Analysis and Risk Management requirements?
- Have you changed your Risk Analysis and Risk Management process since the Meaningful Use requirements too effect?

Security Management Process

- Administrative Safeguard in the HIPAA Security Rule standard [164.308(a)(i)(i)]
- Two Implementation Specifications:
  - ✓ **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." [164.308(a)1)(ii)(A)]
  - ✓ **Risk Management** (*Required*) – "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.308(a)." [164.308(a)1)(ii)(B)]
- *Note: Applies to Business Associates and Subcontractors as well.*

Meaningful Use Requirements

- Conducting or reviewing a security risk analysis to meet the standards of the HIPAA Security Rule is included in meaningful use requirements of the Medicare and Medicaid EHR Incentive Programs.
- Eligible hospitals and eligible professionals must conduct a security risk analysis in both Stage 1 and Stage 2 of meaningful use to ensure the privacy and security of their patients' protected health information.

CMS, Security Rule Analysis Tipsheet: Protecting Patients' Health Information

Stage 1 and Stage 2 MU Requirement

- Objective: Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.
- Measure:
  - ✓ In Stage 1, eligible hospitals and eligible professionals must conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(1)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.
  - ✓ In Stage 2, eligible hospitals and eligible professionals need to meet the same security risk analysis requirements as Stage 1, but must also address the encryption/security of data at rest.

Additional Considerations for MU

- A security risk analysis needs to be conducted during each reporting period for Stage 1 and Stage 2.
- Meaningful use does not impose new or expanded requirements on the HIPAA Security Rule.
- MU doesn't require specific use of every certification and standard that is included in the certification of EHR technology.
- Myth: The security risk analysis only needs to include the EHR.

General Considerations

- Review your existing security infrastructure, safeguards, policies and practices against legal requirements and industry best practices.
- Identify potential threats to patient privacy and security, and assess the impact on the confidentiality, integrity and availability of your organization's PHI.
- Prioritize risks based on the severity of their impact on your patients and the organization.

Terminology

The Art and Science of "RISK"

- A situation involving exposure to danger
- The potential of losing something of value
  - "Value" – social, physical, financial, reputational, etc.
- The intentional interaction with uncertainty
- Risk perception – subjective judgment people make about the severity and/or probability of a risk
- Risk appetite – varies by individual and by organization

Vulnerability

- "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."
- Vulnerabilities can result in a security incident.
- Vulnerabilities may be **technical** (e.g., lack of appropriate and timely patch management) **or non-technical** (e.g, lack of policies).

Threat

- "The potential for a person or thing to exercise (**accidentally trigger or intentionally exploit**) a specific vulnerability".
- Threats include:
  - ✓ Natural threats (flood, earthquake, tornado)
  - ✓ Human threats (intentional (malicious software, unauthorized access) or unintentional (inaccurate data entry)
  - ✓ Environmental threats (power failure, chemical spill)

Risk

- "The net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a vulnerability and (2) the resulting impact if this occurs.
- Risks arise from
  - ✓ 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 implementation and operation of an IT system

Risk Equation

- A Vulnerability triggered or exploited by a Threat = **Risk**
- Risk is a **combination of factors or events** (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.

Standard Information Security Processes

- Risk analysis and risk management serve as tools to develop and maintain a covered entity's or business associate's strategy to protect the confidentiality, integrity and availability of ePHI.
- "Risk analysis and risk management are important to covered entities and business associates as these processes form the foundation upon which the organization's necessary security activities are built." [68 *Fed. Reg*. 8346, Preamble to Security Rule]

NIST

- National Institute of Standards in Technology – 800 Series of Special Publications (SP).
- See SP 800 – *Risk Management Guide for Information Technology Services*
- "Covered entities may use any of the NIST documents to the extent they provide relevant guidance to that organization's implementation activities. " [CMS FAQs]

Information Security Risk

- Risk is defined as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization."
  ISO/IEC 27005:2008

Why is Risk Analysis so hard?

- Failure to understand what risk really is.
- Failure to set objectives for risk analysis.
- Too much emphasis on quantitative analysis and reliance on statistics.
- Security threats and vulnerabilities are constantly changing.
- Past occurrences are not a good measure of future events.
- Technical threats and vulnerabilities cannot be the only basis for risk analysis.

Risk Analysis/Risk Management Cycle

Identify

Safeguard **Assess**

Manage

Establishing an Effective RA/RM Program

- Objectives
- Approaches
- Mitigation
- Reporting

What is the objective?

- **To protect information assets**
- Emphasis on ePHI that the organization **creates, receives, maintains, transmits**
- Identify the scope of the analysis
- Consider layering the analysis process
  - ✓ Organizational Level
  - ✓ Business Process or Functional Area Level
  - ✓ Information System Level

Issues to Consider

- How to identify all information assets and determine how they are used and handled at each stage of the data life cycle.
- Establish criticality of information assets so risk categories can be derived, risks can be prioritized and resources focused on protecting the most valuable assets and those that represent the greatest potential losses.
- Information can be jeopardized more by bad business practices and lack of awareness by those handling the information than on all technical threats combined.

Approaches

- Quantitative vs. Qualitative
- Integration with other risk management functions → Enterprise-wide Risk Management (EWRM)
- Use of software products
- Talk to people – conduct interviews
- Survey key stakeholders
- Learn from other industries

Sample Risk Analysis Steps

- Identify scope of the analysis – all ePHI that is created, received, maintained or transmitted
- Gather data – where ePHI is created, received, maintained or transmitted
- Tools and methods: surveys, interviews, incident reports, technical reports, role of vendors and business associates.
- Document data.
- Identify and document potential threats and vulnerabilities.

Risk Analysis Steps (Cont'd)

- Assess current security measures and safeguards (technical and non-technical). Document security measures.
- Determine the likelihood of a threat occurring -- High, Medium, Low.
- Determine the potential impact of threat occurrence, e.g.:
  - ✓ Unauthorized access to or disclosure of ePHI
  - ✓ Permanent loss or corruption of ePHI
  - ✓ Loss of financial resources and/or productivity
  - ✓ Loss of physical assets

Risk Analysis Steps (Cont'd)

- Determine the level of risk.
- Create a risk matrix → Likelihood of threat occurrence and resulting impact.
- Develop risk mitigation activities/corrective actions.
- Identify security measures and finalize documentation.

Risk Management Steps

- Develop and implement a risk management plan.
- Implement security measures.
- Evaluate and maintain security measures.

Mitigation

- Taking steps to reduce adverse effects or lessen the risks
- Four types of risk mitigation:
  - ✓ Risk acceptance (other options may outweigh cost of the threat)
  - ✓ Risk avoidance (avoid any exposure)
  - ✓ Risk limitation (take some action)
  - ✓ Risk transference (outsourcing operations)

Reporting

- Risk Profile
  - ✓ Identifies an organization's key risks
  - ✓ Identifies vulnerabilities associated with creating, receiving, maintaining and transmitting ePHI
  - ✓ Describes potential impact of a negative event leading to a significant loss or compromise of ePHI, the likelihood of an event occurring, and a measure of overall risk
  - ✓ Provides management with a "snapshot" of key risks
  - ✓ A learning tool and communication tool
  - ✓ Supports decision-making → allocation of resources
- Risk mitigation plan identifies strategies that can be deployed to mitigate or lessen the risks.

Sample Risk Profile & Risk Mitigation Plan

Vulnerability	Impact	Likelihood	Overall Risk	Safeguards	Mitigation Strategies
Physical Security Outdated key pad/swipe card system for data center	High	Low	High	Security cameras	Upgrade key pad and swipe card system. Maintain log of all visitors.

Sample Risk Profile & Risk Mitigation Plan

Vulnerability	Impact	Likelihood	Overall Risk	Safeguards	Mitigation Strategies
Mobile Device Security • *Mobile devices* • *Removable media (USB)* • *Pictures* • *Texting* • *Email*	Medium	Low	Medium	Policies: - BYOD - Social Media. Security awareness training. Encrypted USB drives. Encrypted laptops. Confidentiality Statement.	• Complete implementation of MDM system. • Continue to encrypt all laptops. • Training program on secure use of smartphones.

Improving Your Information Security & Privacy Program

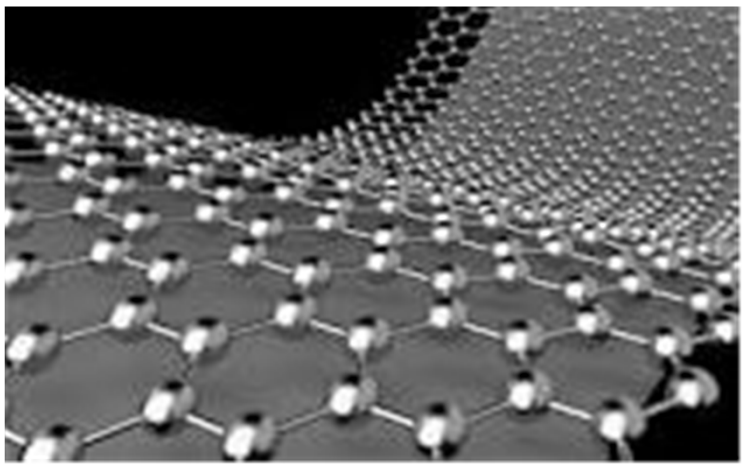
Risk Analysis/Risk Management Cycle

Identify

Safeguard **Assess**

Manage

Security Rule Refresher



Standards

Implementation Specifications

SAFEGUARDS

Documentation Requirements

Required vs. Addressable

Standards	Section	Implementation Specifications	Required vs. Addressable
Security Management Process	§ 164.308(a)(1)	•Risk Analysis • Risk Management • Sanction Policy • IS Activity Review	All Required
Assigned Security Responsibility	§ 164.308(a)(2)		Required
Workforce Security	§ 164.308(a)(3)	•Authorization •Workforce Clearance •Termination	All Addressable
Information Access Management	§ 164.308(a)(4)	•Clearinghouse Functions •Access Authorization •Access Establishment & Modification	Required Addressable Addressable
Security Awareness and Training	§ 164.308(a)(5)	•Security Reminders •Protection from Malicious Software •Log-in Monitoring •Password Management	All Addressable
Security Incident Procedures	§ 164.308(a)(6)		Required
Contingency Plan	§ 164.308(a)(7)	•Data Backup Plan •Disaster Recovery •Emergency Mode Operation •Testing and Revision Procedures •Applications & Data Criticality Analysis	Required Required Required Addressable Addressable
Evaluation	§ 164.308(a)(8)		Required
Business Associate Contracts	§ 164.308(b)(1)		Required

Standards	Sections	Implementation Specifications	Required vs. Addressable
Facility Access Control	164.310(a)(1)	• Contingency Operations • Facility Security Plan • Access Control and Validation Procedures •Maintenance Records	Addressable Addressable Addressable Addressable
Workstation Use	164.310(b)		Required
Workstation Security	164.310(c)		Required
Device and Media Controls	164.310(d)(1)	•Disposal •Media re-use •Accountability •Data back-up and storage	Required Required Addressable Addressable

Standards	Sections	Implementation Specifications	Required vs. Addressable
Access Control	§ 164.312(a)(1)	•Unique User Identification •Emergency Access Procedure •Automatic Logoff •Encryption and decryption	Required Required Addressable Addressable
Audit Controls	§ 164.312(b)	•Integrity •Authentication Method •Person or Entity Authentication •Transmission Security •Integrity Controls •Encryption	Required Addressable Required Addressable Addressable Addressable

Questions to ask your organization

- Do the organization's policies articulate an approach to risk analysis and risk management in protecting confidential information that is created, received, maintained or transmitted?
- Who is responsible for coordinating the risk analysis and risk management program?
- How do senior leaders and board members support the risk analysis and risk management program?
- How is the risk analysis program documented?

Final Thoughts

- The Security Rule does not prescribe a specific risk analysis or risk management methodology.
- The RA/RM program can be tailored to the uniqueness of your organization, taking into account size, resources, culture, and corporate structure.
- Use interdisciplinary team approaches with active clinician participation and engagement. Involve key knowledge leaders.
- Communicate results and update stakeholders on mitigation efforts and achievements.

Are we there yet?

Resources

http://www.healthit.gov/sites/default/files/risk_assessment_user_guide_final_3_26_2014.pdf

http://www.youtube.com/watch?v=mQXzuw4sbIg

http://www.healthit.gov/providers-professionals/video/security-risk-analysis

http://www.youtube.com/watch?v=ilIpd7nFBYU

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

Resources (Cont'd)

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

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

http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

http://scap.nist.gov/hipaa/NIST_HSR_Toolkit_User_Guide.pdf

PHYLLIS PATRICK + Associates

Security | Privacy | Culture

phyllis@phyllispatrick.com
914-696-3622
www.phyllispatrick.com