“RISK ASSESSMENTS 101 FOR MEANINGFUL USE AND HIPAA/HITECH”

MAY 13, 2016

Presented by:
Claire Cieri, MS,CHC,CHCO,CPMA,CHCA,CPC,CEMC

Disclaimer

- This material is designed to provide information about medical compliance in an educational format.
- No legal advice is being offered.
- Every reasonable effort has been taken to insure that the information provided is accurate. However, interpretations can sometimes be varied on certain meanings and situations. Solutions and results will vary at each facility.
Agenda:
- Risk Analysis for:
  - HIPAA/HITECH
  - Meaningful Use
- What is a Risk Analysis?
- One size does not fit all
- Consequences of Neglect
- OCR Audits
The very first requirement of the HIPAA Security Rule: Conduct a Risk Analysis:

Definition for Covered Entities:

- “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the covered entity or business associate. “

- First time Risk Assessment is used and is specific to assessing the risks in response to a suspected breach. Interesting?
■ HIPAA Security rule required compliance by 2005
■ Created Meaningful Use incentive program at that time

Unsecured PHI is:

■ Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402 (h) (2) of Pub. L. 111-5
■ Statistical
■ Unrecognizable
HIPAA privacy safeguards:

“Safeguards: a covered entity must have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information”. 45 CFR 164.530(c)(1)

- Requires a written risk analysis to be periodically updated
- Foundation for the three types of safeguards-Administrative, physical and Technical- policies and procedures related to them, and safeguard training.

Security Risk Analysis:

- Protecting Patients’ Health Information
- Required by:
  - HIPAA Security Rule
  - Meaningful Use Stages 1-3
HIPAA Security Rule

- Covered entities required to conduct:
  - Accurate and thorough analysis
  - Potential risks, vulnerabilities
  - Confidentiality, integrity, availability
  - Of ALL ephi

Risk Analysis: HIPAA Security Rule

- CEs must conduct a RA to identify risks and vulnerabilities (see MU) to e-PHI
- First step in organization’s Security Rule compliance efforts
- Implement changes to make PHI more secure, then monitor the results (risk management)
Implementation Specification: Risk Management (Required)

- “Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with:
  - Security Standards: General Requirements”

Risk Analysis Mandates 2

**Meaningful Use Stage 2 Security Measure**

- Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data stored in Certified EHR technology in accordance with requirements under 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 its risk management process
Meaningful Use

- Attest/Certify
- Documentation
- Audit/Repayment
- Risk Assessment

What is RISK? one answer is:

- A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:
  1. The adverse impacts that would arise if the circumstance or event occurs, and
  2. The likelihood of occurrence
Risk Analysis: Risks

- Security vulnerabilities such as user access controls not properly configured, allow staff to inappropriately view patient health information
- Threats to PHI such as theft of portable device that is not encrypted

Information Risk Management Definition

- Risk management is a comprehensive process that requires organizations to: frame risk (establish the context for risk-based decisions), assess risk, respond to risk once determined and monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision making is integrated into every aspect of the organization-NIST.
Key Points as you start your Risk Assessment/Analysis

- Must be possible to have loss or harm in order to have risk
- Must have asset-threat-vulnerability “triple” to have risk
- Risk is a likelihood issue
- Risk is an impact issue
- Risk is a derived value (like speed is a derived value – distance/time)

Three (3) Questions to Consider:

- 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 the human, natural, and environmental threats to information systems that contain e-PHI?
Security Rule (and Meaningful use) does not prescribe a specific risk analysis

Methods will vary dependent on the size, complexity and capabilities of the organization

Rule identifies risk analysis/assessment as the chief element in achieving compliance

Rule also established several objectives any methodology adopted must achieve

What is a Risk Analysis?

Here is the definition of Risk Assessment:

“The process of identifying risks to organizational operations (including mission, function, image, reputation, assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security measures”

“Synonymous” (NIST)
What is **Information System-Related Security Risk?**

- Risk that arises through the loss of confidentiality, integrity, or availability of information or information systems considering impacts to organizational operations and assets, individuals, other organizations, and the Nation. A subset of **Information Security Risk.** - NIST

What is **Information Security Risk?**

- The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. - NIST
In consideration of the HIPAA/HITECH Act:

- **RISK** is the potential occurrence of an event that has an adverse financial impact.
- If a healthcare organization has a breach, the average cost could be as high as $363 per affected individual.
- Costs include remediating the harm, notification to affected individuals and to the OCR, and lost business.

**Risk Analysis Process**

- Review existing security of PHI
- Monitor results
- ID threats and vulnerabilities
- Mitigate security risks
- Assess risks for likelihood and impact
- Monitor results
✓ Numerous methods of performing a risk assessment/analysis
✓ No single method or best practice that guarantees compliance with the Security Rule
✓ One example is outlined in NIST SP 800-30
✓ But- several elements a risk assessment MUST incorporate

Scope of the Analysis

- Include all sensitive information
- Think Information asset inventory
- Risks to all the ePHI that an organization creates, receives, transmits, maintains
- Includes hard drives, smart cards, portable electronic media (think telecommuting) backup media, servers, databases
- Take into account all of your ePHI, regardless of the particular electronic medium in which it is created, received, maintained, transmitted.
Steps for the Scope

- Identify location, contact information, number of workforce members, and responsible person (usually Security Official) for each physical facility that has IT systems that contain ePHI.
- Write a brief statement of the scope of the risk analysis, indicating number of physical facilities, workforce members in each, and prevalence of IT systems that contain ePHI.
- The risk assessment will address threats and vulnerabilities related to each of the IT systems that contain ePHI.

Data Collection

- Collect and Document Data About All Information Assets
- Identify and compile relevant information pertaining to creation, receipt, maintenance, processing, and transmission of ePHI for each IT system unit by type.
- The method used to gather data (perform interviews, review documentation, review past/existing projects) must be documented and the data gathered must be documented.
- This is the most time consuming activity for an organization that have not created an inventory of its electronic IT systems. If updated on a regular basis, your organization will facilitate the HIPAA Security Rule required risk analysis reviews and updates going forward.
Identify and Document Potential Threats and Vulnerabilities

- Organizations must identify and document reasonably anticipated threats to ePHI
- Organizations may identify different threats that are unique to the circumstances of their environment
- Organizations must also identify and document vulnerabilities, which, if triggered or exploited by a threat, would create risk of inappropriate access to or disclosure of ePHI

Steps for Identifying Threats/Vulnerabilities to ePHI

- Identify threat sources in four categories:
  - Malicious intent
  - Accidental
  - Structural
  - Natural disaster
- Rate the likelihood potential from least likely to most likely
- Identify the top 5 threat sources to your organization
- Identify what security measure, if any is in effect
Several types of threats that may occur within an information system:

- Natural threats, such as floods, earthquakes
- Human threats are enabled or caused by humans and may include intentional or unintentional actions
- Environmental threats such as power failures, chemicals, liquid leakage

Assess Current Security Measures

- Identify and assess the current security controls in your organization that your organization has documented and implemented to safeguard ePHI
- Identify whether security measures required by the Security Rule are in place and, most importantly, if current security measures are configured and used properly
A thorough understanding of the actual security controls in place for a covered entity (and business associate) will reduce the list of vulnerabilities, as well as the realistic probability, of a threat attacking (intentional or unintentionally) ePHI.

Security measures implemented will vary among organizations.

Small organizations tend to have more control within their environment, therefore their security controls will be different from a large organization’s.

Determine the likelihood of threat occurrence

Security Rule requires organizations to take into account the probability of potential risks to ePHI.

The results of this assessment, combined with the initial list of threats, will influence the determination of which threats the Rule requires protection against because they are “reasonably anticipated.”
Determine the potential Impact of Threat Occurrence

- Organizations must consider the impact, or criticality, of potential risks to the confidentiality, integrity and availability of ePHI.
- The covered entity must assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability.
- An entity may use either a qualitative or quantitative method or a combination of the two methods to measure the impact on the organization.

System and data sensitivity can be determined based on the level of protection required to maintain the ePHI’s confidentiality, integrity, and availability. The adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security objectives:
  - Integrity
  - Availability
  - Confidentiality

Document all threat and vulnerability combinations along with associated likelihood estimates.
### Determine the level of Risk: Threat likelihood to impact on vulnerability

<table>
<thead>
<tr>
<th>Threat Likelihood</th>
<th>Low Impact</th>
<th>Moderate Impact</th>
<th>High Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Moderate</td>
<td>Low</td>
<td>Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

### Determine the Level of Risk

- **Organizations should assign risk levels for all threat and vulnerability combinations**
- **The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence.**
- **Risk level determination could be performed by assigning a risk level based on the average of the assigned likelihood and impact levels**
Determine the Level of Risk

- The output after doing the level of risk activity should be documentation of the assigned risks levels and a list of corrective actions to be performed to mitigate each risk level.
- Implement security controls at an acceptable level through safeguard policies and procedures to mitigate the risk.

The HIPAA security rule permits covered entities and business associates to take into consideration the following in selecting security controls and measures:
- Size, complexity, and capabilities
- Technical infrastructure, hardware, and software security capabilities
- Costs of security measures
- Probability and criticality of potential risks to ePHI.
Risk assessment issues...

- 68% of 2012 OCR Phase/Audits of HIPAA/HITECH Failed Risk Analysis (80% of providers)
- 73% of 26 OCR Resolution Agreements/CAPs (corrective action plans) Cite Failed Risk Analyses/Assessments
- Failure to understand that Risk Assessments are a basic foundational step AND required by regulation

Healthcare is the next Cyber Security Battleground

- “Because the health care industry is not as “resilient to cyber intrusions (as) the financial and retail sectors, therefore the possibility of increased cyber intrusions is likely” – FBI Alert
- “...observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personal Identifiable Information (PII)” – FBI Alert
Risk management is NOT a “HIPAA Compliance” issue
- It is a patient safety/quality of care/information risk issue
- The first medical oath is “First, do no harm”
- That includes identifying RISK!- to your patients, to your organization and to other stakeholders

The “Eighth Element”

♦ Annual risk assessments that cover all areas of the organization!
♦ Health care organizations need to utilize technology that provides both control over and visibility into the organization’s regulatory risk in order to move toward improved quality of care, or risk the organization’s financial health by managing against unseen risk and chasing after compliance.
First Risk Analysis

1. Review existing security infrastructure against legal requirements and industry best practices
2. Identify potential threats to patient privacy and security vulnerabilities and assess the potential impact if that what-if occurred
3. Prioritize risks for action based on the likelihood of specific risks and their potential impact on patients, the practice and others
4. No simple checklist. Federal, state and privacy security requirements will continue to evolve
5. Will return annually to reassess

Security Risk Analysis is:
(using a medical definition)

♦ Assess clinical risk and diagnose a condition
♦ Use RA to create an action plan to make your practice “better” at protecting patient information
♦ Privacy and Security are like chronic diseases that require treatment, ongoing monitoring and evaluation
Actions!

1. Think *ongoing* program, NOT project
2. Select the methodology you will follow and make sure it meets requirements
3. Become familiar with your exact requirements for your Risk Assessment (HIPAA/HITECH physical, administrative and technical requirements; Meaningful Use Requirements)
4. Complete your Risk Assessment/Analysis
5. Build and execute your risk response plan
6. Update your risk analysis at least once a year

♦ With the information compiled from the previous activities, your organization has assembled all of the necessary information to not only complete your risk assessment/analysis, but also to modify safeguard policies and procedures to fit your organization’s particular operation environment at the level of risk that it finds acceptable.

♦ The Risk Assessment must be ongoing. Organizations must identify when updates are needed. The frequency will depend on the organization but at least once a year. New technologies, a security incident or key staff turnover will require an update.
Increased Enforcement

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Valuation</th>
<th>All identical violations for calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know</td>
<td>$100-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1000-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful neglect- Corrected in 30 days</td>
<td>$10,000-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful neglect-not corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

Scary Stories

The numbers are scary... Since the 2009 HITECH Breach Notification Rule more than 38.7 million have had their PHI compromised in HIPAA privacy and security breaches...
What’s the Big Deal?

- Street cost for a stolen Record
  - Medical $50 vs SSN: $1

- Payout for Identity theft
  - Medical: $20,000 vs Regular: $2000

- Medical records can be exploited 4X longer
  - Credit cards can be cancelled; not MR

Scary Story Number 1:
March 2016

North Memorial Health Care required to pay $1.55 HIPAA settlement for lack of BAA and Risk Analysis Failures stemming from a 2011 data breach. North Memorial had not performed a comprehensive risk analysis for the entire organization. North Memorial is now required to conduct risk analyses that include all electronic equipment capable of touching ePHI, as well as data systems and applications run by or on behalf of NM.
Scary Story Number 2: April-June 2014

Community Health Systems notified 4.5 million of its patients that their personal information was stolen by cybercriminals. The Chinese hackers exploited the Heartbleed vulnerability. Only on Aug. 19 did the FBI issue an alert to healthcare organizations that may be susceptible to an attack. Alert was not specific to Chinese hacking group. Largest hacking-related breach ever reported.

Scary Story Number 3: May 2013

Idaho State University notified HHS of the breach in which ePHI of 17,500 patients was unsecured for 10 months, due to the disabling of firewall protections at servers maintained by ISU. OCR’s investigation indicated that ISU’s risk analyses and assessments of its clinics were incomplete and inadequately identified potential risks or vulnerabilities. ISU settled for $400,000 and agreed to a corrective action plan.
Scary Story number 4: June 2010

Hospice of North Idaho paid $50,000 to HHS after an unencrypted laptop containing the information of 441 patients had been stolen. HONI had not conducted adequate risk analysis to safeguard patient ePHI. First HIPAA Breach settlement involving fewer than 500 patients......!

Good patient care means safe record-keeping practices. Do not forget that an EHR represents a unique and valuable human being: it is not just a collection of data you are guarding—it’s a life.
Healthcare is compliant when it:

- is documented, charged and billed correctly
  - is provided in an approved facility
  - promotes patient rights
- is reimbursed correctly
  - is provided by qualified physicians/staff
  - is medically necessary
- meets quality standards
  - is provided without financial incentives

_It takes less time to DO A THING RIGHT, then it does to EXPLAIN WHY you did it wrong._

- Henry Wadsworth Longfellow
Resources:

- Guidance on Risk Analysis Requirements under the HIPAA Security Rule:
  Published by the Office of Civil Rights (OCR)
- HIMSS Fact Sheets
- HIMSS Risk Assessment (RA) Toolkit
- American Medical Association: HIPAA Violations and Enforcement
- United States Department of Justice: Scope of Criminal Enforcement under 42 U.S.C. 1320d-6
- The 800 Series of Special Publications (SP) are available on the Office for Civil Rights’ website specifically, SP 800-30- Risk Management Guide for Information Technology Systems.
- NIST SP 800-66, Section #4 “Considerations When Applying the HIPAA Security Rule.”
- The Security Series papers: Available at: http://www.hhs.gov/ocr/hipaa

Thank You!!

Please email me questions at: claire@mardac.com or ph. 541-520-2052