How to Conduct a Security Risk Analysis that Complies with MU
October 29, 2015
Host: NM Medicaid EHR Incentive Program

Rebecca Wahler, MS, CHPC, CHC
Privacy & Compliance Officer
LCF Research/NMHIC, Albuquerque, NM
Rebecca Wahler is the Privacy and Compliance Officer for LCF Research / NMHIC HIE. She is nationally certified in healthcare privacy and compliance. Previously she was the Privacy and Security lead for the NM HIT Regional Extension Center Grant. As the lead she provided numerous educational trainings, and consultations to medical providers in NM on HIPAA, and HITECH requirements including Risk Assessments.
LCF Research

LCF Research was established in 1990 as a not-for-profit organization to foster health services research among physicians, hospitals, and government agencies and to provide continuing professional education for health professionals.

LCF continues to focus on applied healthcare research and translating research into practice to improve the health of patients and the delivery of quality health care. There are three divisions within LCF: health services research, health information technology, and continuing professional education.
The New Mexico Health Information Collaborative Health Information Exchange (NMHIC HIE) is the statewide health information exchange network. It enables the electronic exchange of patient health information among different and unrelated healthcare organizations, such as doctors’ offices, hospitals, laboratories, pharmacies, and clinics using electronic health record (EHR) systems.
Objectives

- Define the important terms related to a Risk Assessment (RA)
- Define and review the Risk Analysis Steps
- Define and review the Risk Management Steps
- Quick look at potential RA Tools
Background Information

- All electronic protected health information (ePHI) created, received, maintained or transmitted is subject to the Security Rule.
- Covered entities are required to implement reasonable security measures to protect against anticipated threats and/or hazards to the security and/or integrity of the ePHI.
- The Security Rule requires covered entities to evaluate risks and vulnerabilities and to implement Policies and Procedures to address those risks.
Regulatory Requirements

- 45 CFR 164.308(a)(1)(i) – “implement policies and procedures to prevent, detect, contain, and correct security violations”.

- 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 electronic protected health information held by the covered entity”.

- 45 CFR 164.308(a)(1)(ii)(B) – “implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 45 CFR 164.306(a)”.
Objective 1: Protect Patient Health Information

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 by CEHRT 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 the EP, eligible hospital, or CAH's risk management process.
Meaningful Use Objectives

A Risk Assessment is a technique to determine potential vulnerabilities and threats. It will determine the likelihood of those events being exploited and what the impact would be to your business.

A vulnerability can have low, medium, or high impact to your organization and low, medium, or high likelihood, which then determines the overall risk.

e.g., An unencrypted server with your PHI may be stolen from your clinic. Likelihood is medium, impact is high risk (very damaging to your clinic). Overall risk is HIGH.
## Determine the Level of Risk

Risk = likelihood of given threat \times impact

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Low</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>
Key Terms

- **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”.

- **Vulnerabilities** can be grouped into two categories: technical and non-technical
  - **Technical vulnerabilities** may include holes, flaws, or weaknesses in the development of the information systems; or incorrectly implemented and/or configured information systems
  - **Non-technical vulnerabilities** include ineffective or non-existent policies, procedures, or guidelines.
Threat – “the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability”.

There are 3 kinds of threats:

**Natural**
floods, earthquakes, storms, blizzards

**Human**
intentional attacks or unintentional actions

**Environmental**
power failures, pollution, chemicals, sprinkler damage, fire
Key Terms

Risk – “The net mission impact considering (1) the probability that a particular threat will exercise (accidentally or intentionally exploit) a particular vulnerability and (2) the resulting impact if this should occur”.

Risks can arise due to:
1. Unauthorized disclosure, modification, or destruction of information
2. Unintentional errors or omissions
3. IT disruptions due to natural or man-made disasters
4. Failure to exercise due care and diligence in the implementation and maintenance of IT systems
1. Identify the scope of the analysis
2. Gather data, including an asset inventory
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 a threat occurrence
7. Determine the level of risk
8. Identify security measures and finalize documentation
Risk Assessment Team

- A Risk Assessment team should have several members contributing their information.

- Usually includes Office Manager, I.T. person(s), EHR technical person, clinical person, billing/coding person, medical records, clinical person
Identify the Scope of the Analysis

- The risk analysis scope required by the Security Rule pertains to all electronic media.
- Any media that stores, transmits, receives, or maintains ePHI.
- Electronic media includes hard drives, CDs, thumbnail drives, PDAs, transmission media, storage media, and portable media.
- Asset inventory (stuff and software)
Gather Data

- Determine where your data is stored, received, maintained, or transmitted.
- This can be accomplished through review of existing or past projects, interviews with personnel, and documentation review.
- During the data gathering process don’t forget all systems that use ePHI (EHR, billing systems, scheduling systems, Practice Management, encrypted email systems, etc.).
Identify and Document Potential Threats and Vulnerabilities

- Document threats and vulnerabilities to confidentiality, availability, and integrity of the ePHI.
- Identify and document threats (reasonable anticipated threats from natural, human, and environmental sources).
  
  e.g., fire, water damage, disgruntled employee, web access goes down, power outages, etc.
- Identify and document vulnerabilities (technical and non-technical should be listed).
Assess Current Security Measures

- Security measures can be both technical and non-technical

- Technical measures are often part of the information systems hardware and software programs
  
  *e.g.*, risk of patient reading EHR record on unprotected computer. Technical measure might be an automatic log off and lock out program with the EHR

- Non-technical measures are often operational controls, policies and procedures
  
  *e.g.*, same example as above, policy written that all staff must lock all computers when unattended
What is the probability that a threat will trigger or exploit a specific vulnerability?

**High likelihood**
existence of multiple organizational deficiencies

**Medium likelihood**
existence of a threat may trigger or exploit one or more vulnerabilities due to one organizational deficiency

**Low likelihood**
a single vulnerability due to a single organizational deficiency
Determine the Potential Impact of a Threat Occurrence

What is likely to happen if a threat is triggered or exploited?

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
- Loss of patient confidence/public relations problems
Identify Security Measures and Finalize Documentation

- Once risk is identified and assigned a risk level then the actions to lessen that risk can be taken
- Always document efforts to lessen risks
- Always consider the effectiveness of the security measure, legislative or regulatory requirements, policies and procedures
Risk Management Steps

1. Develop and implement a risk management plan
2. Implement security measures
3. Evaluate and maintain security measures
Develop

- Develop and implement a risk management plan. This helps to provide structure for the evaluation, prioritization, and implementation of the measures.
- Key members should be included (office manager, IT staff, senior medical person).
- Determine the timeline for security measures.
- Determine the person(s) responsible for implementing those measures.
Implement

• When implementing security measures consider the scope of the project, timeline, and budget.
• Internal or external resources can be used to perform these security measures.
The final step is to continually evaluate and monitor your risk mitigation measures to determine if they are effective.

Risk analysis and management is an on-going process.

Annual review is recommended, but more frequently may be appropriate for your situation.
Potential Risk Assessment Tools available:

- **Government Website Version**
  Great tool if you would like more explanation available to you, including regulations and examples.

- **Excel spreadsheet version.** Cleaner version, and you can save a version to your own company computers.
§164.308(a)(1) - Standard
Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its ePHI?
- Yes
- No
- Flag

Current Activities | Notes | Remediation

With respect to a threat/vulnerability affecting your ePHI:

- Likelihood:
  - Low
  - Medium
  - High

- Impact:
  - Low
  - Medium
  - High

An information system is an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and users.

A portable electronic device is any electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.

Electronic storage media includes...
### Risk Assessment

#### Screening Questions

<table>
<thead>
<tr>
<th>Security Program</th>
<th>Policy</th>
<th>Risk Management</th>
<th>Training</th>
<th>Personnel</th>
<th>Physical</th>
<th>Network</th>
<th>Logical</th>
<th>Operations</th>
<th>Incident</th>
<th>Disaster</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Central Point of Contact</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has your organization formally appointed a central point of contact for security coordination? If so, whom, and what is their position within the organization? Are the responsibilities clearly documented in any job description or policy?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>External Parties</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you work with any third parties such as IT service providers, that have access to your patient’s information? If so, list these third parties and indicate if your organization has a Business Associate Agreement in place with these third parties.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Risk Assessment Tool, Cont.

<table>
<thead>
<tr>
<th>Asset Management Category</th>
<th>Threat-Vulnerability Statement</th>
<th>Recommended Control Measures</th>
<th>Perform Control Analysis</th>
<th>Exposure</th>
<th>Assess Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Program</td>
<td>Management has not defined responsibilities for the information security program. [TVS001]</td>
<td>All information security responsibilities are clearly documented. This is to ensure timely, safe and effective handling of all situations, administration user accounts-including additions, deletions, and modifications. [RCM001] - Ensure responsibilities are formalized within the employee(s) job descriptions as well as within relevant IS policies. - The Information Security Policy Template provided by the REC could help formalize this role.</td>
<td>0 Partially Effective</td>
<td>Likely</td>
<td>High</td>
</tr>
</tbody>
</table>
Additional Resources

1. [www.cms.hhs.gov](http://www.cms.hhs.gov) under “Regulations and Guidance” for the latest security papers, checklists and announcements


Questions

General Questions: contact 505-938-9900

For help completing a Risk Assessment or other Privacy and Security related matters contact Michelle Bowdich at 505-938-9909 or michelle.bowdich@lcfresearch.org