Risk Analysis and Management Tool

Risk analysis process is a requirement of HIPAA and creates a result that is UNIQUE TO EACH FACILITY. There are numerous methods of performing risk analysis and risk management. There is no single method or best practice that guarantees compliance with the Security Rule. However, most risk analysis and risk management processes have common steps.

When would I need to perform this risk analysis?

- Natural threats may include floods, earthquakes, tornadoes and landslides
- Human threats are enabled or caused by humans and may include:
  - **Intentional** — network and computer-based attacks, malicious software upload, and unauthorized access to electronic information
  - **Unintentional** — inadvertent data entry or deletion and inaccurate data entry actions
- Environmental threats may include power failures, pollution, chemicals and liquid leakage
- Hardware security
- Physical or building security
- Software implementations
- Staffing changes
- Building access

**EXAMPLE: Performing a Risk Analysis**

1. Identify
   - Patient information contained in laptop
2. What risk(s) exist
   - Loss/theft of the laptop data
3. Identify vulnerabilities
   - Loss of data, breach, required reporting to patient, DHS and media, public image
4. Current security measures
   - Laptops not left unattended during working hours, automatic logout after 10 minutes of inactivity, require password to access patient information on laptop, laptops locked in file cabinet after hours, key limited to RN and office manager
5. Likelihood
   - Not likely
6. Impact Severity
   - High
7. Determine the level of risk
   - Moderate
8. Selecting security measures
   - Encrypt laptops, locking laptop cables, refresher training, reduce auto logout settings
   - Cost of each
     - Encrypt software $110 × 5 laptops; cables $10.99 × 5 laptops
9. Select security measure to implement
   - Cables are cumbersome. Software is expensive. No data stored on laptop; requires password.
10. Implement security measures
    - Retrain staff. Reduced auto logout to three minutes.
11. Evaluate security measures
    - Six months later reassess. Now providers take laptops home for on-call access. Purchase encryption software and install. Redo risk analysis with encryption software included.
Performing a Risk Analysis

1. Identify assets that need protection and vulnerabilities

_________________________________________________________________________________________________
_________________________________________________________________________________________________

2. What risk(s) exist

_________________________________________________________________________________________________
_________________________________________________________________________________________________

3. Identify threats and potential vulnerabilities

☐ _______________________________________________________________________________________________
☐ _______________________________________________________________________________________________
☐ _______________________________________________________________________________________________
☐ _______________________________________________________________________________________________
☐ _______________________________________________________________________________________________

4. Assess current security measures in place

_________________________________________________________________________________________________
_________________________________________________________________________________________________

5. Determine the likelihood of the risks occurring:

☐ Low: Minimal, little or no impact
☐ Medium: Small but tangible harm, noticeable to limited number, some effort to repair
☐ High: Considerable or extended system outage, compromise of large amount of information

6. Determine the potential impact of threat occurrence and impact of severity

☐ Not likely: Unlikely to ever occur or two/three times every five years
☐ Likely: Likely to occur once every year or once per month
☐ Very likely: Likely to occur multiple times per month or multiple times per day
7. **Determine the level of risk:** Take answers from steps 5 and 6 and determine the overall risk level below

<table>
<thead>
<tr>
<th>Likelihood of occurrence</th>
<th>IMPACT SEVERITY</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LOW</td>
</tr>
<tr>
<td>Not likely</td>
<td>Low</td>
</tr>
<tr>
<td>Likely</td>
<td>Low</td>
</tr>
<tr>
<td>Very likely</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

8. **Selecting security measures to guard against those risks**

   - 
   - 

   What will each security measure cost — out of pocket costs and personnel time/ease of use
   
   - 
   - 

9. **Document risk assessment findings.** Maintain copy of this completed form.

**RISK MANAGEMENT STEPS:**

1. **Develop and select which security measure to implement:**

   - 
   - 
   - 
   - 

2. **Implement security measures.** Date of implementation: 

3. **Evaluate and maintain security measures.**

   Date implemented measures re-evaluated: 
   Changes made: 
   Staff involved in risk analysis process: 

AFMC HealthIT, a division of AFMC
1020 W. 4th St., Suite 300 • Little Rock, AR 72201

501-212-8616 • healthit@afmc.org • afmc.org/healthit