



## Conducting your Security Risk Assessment

The purpose of this document is to assist you in conducting a security risk assessment in a streamlined yet effective manner. This document walks through the steps the LTC Consortium believes are necessary for a successful security risk assessment. Additional Long Term Care Consortium tools will be referenced throughout this document. All of these tools can be found on the AHCA website. ([www.ahca.org/hipaa/index.htm](http://www.ahca.org/hipaa/index.htm))

### Step 1:

Identify all sources of Electronic Protected Health Information (e-PHI) within your organization. Some areas to consider:

1. Which computer applications use e-PHI?
2. How is this e-PHI transmitted or transferred between systems?
3. Which servers store the e-PHI?
4. Is e-PHI being stored on local drives or mobile computing devices?
5. Where are the server back-up tapes stored?

### Step 2:

Identify “experts” for each of the e-PHI sources. Experts would typically include:

1. Information Owner (A business manager or department head that is overall responsible for the specific e-PHI)
2. End User Experts
  - a. User knowledgeable of how the application uses PHI
  - b. User knowledgeable of the access levels of the application
3. Security Expert
4. Network Expert
5. Developer (The person who wrote the program – this might be your vendor)
6. Business Analyst (If you have a larger organization – you might have someone in the Information Technology Group who oversees the application)

**Step 3:**

Once you have completed the identification of team members you are ready to begin the security risk assessment process. You will begin by assembling a team of the experts identified above for each e-PHI source. This team will work to identify security risks, threats, vulnerabilities, sources of risk and other items for each e-PHI source. Make sure you have someone that can represent each area of expertise for each identified e-PHI application.

The tool you can use to document this security risk assessment is the Risk Assessment Matrix. The Risk Assessment Matrix is a spreadsheet that lists all of the Standards and Implementation Specifications of the Security Rule. This tool will allow you to document, risks, threats, vulnerabilities, potential outcomes, as well as generate a risk score. The following steps will walk you through using Risk Assessment Matrix tool.

**Step 4:**

Review the Risk Assessment Matrix Instructions. (Found on the AHCA website)

**Step 5:**

Review the Risk Assessment Training Program (found on the AHCA website). Schedule risk assessment training with your e-PHI expert team.

**Step 6:**

Conduct risk assessment training using the Risk Assessment Training Program. At the completion of the risk assessment training, your team will be prepared to start identifying risks related to their area of expertise.

**Step 7:**

Use the Risk Assessment Matrix located on the AHCA website to document the identified risks.

**Step 8:**

Meet with your teams to begin identifying threats and vulnerabilities for each risk identified. Document these findings on the Risk Assessment Matrix. If possible, Actor, Motive, Access, Security Requirements and Outcome should be identified and documented as well.

*Steps 7 and 8 will be repeated for each e-PHI source identified in Step 1.*

**Step 9:**

After Steps 7 and 8 have been completed for all e-PHI sources, the team should review and approve the risks and related information collected.

**Step 10:**

Each risk will now be “scored”. This process is completed by identifying a probability score and an impact score. The probability and impact scores are then multiplied together to identify the risk score. This risk score is important because it will help determine the sequence of mitigating your risks. A higher risk score would likely receive more attention as compared to a lower scored risk.

**Step 11:**

Identify mitigation alternatives (solutions) for the risks identified. This will probably require your team to be pulled together again so they can identify possible solutions. Remember, a solution may eliminate the risk or reduce it to a reasonable level. These alternatives will vary based upon time and dollars available. The risk score should also be a factor in the alternatives identified.

**Step 12:**

Select the mitigation alternative. Again, the risk score in conjunction with the dollars and resources required will help you select the mitigation alternative. Keep in mind that a risk may be too expensive to mitigate and your business may be willing to accept the “residual risk” and may choose no mitigation or very limited mitigation based on the situation.

**Step 13:**

Develop a plan to implement the mitigation alternative. This plan will include the timeline and resources – both financial and personnel needed to complete the implementation.

**Step 14:**

Initiate and complete the implementation plan. You will use the implementation plan to monitor your progress towards compliance with the Security Rule.

**Step 15:**

Develop a process to monitor for ongoing compliance. The Security Rule requires periodic review in response to environmental or operational changes affecting the security of the e-PHI.

Throughout this process you will need to build in an approval process. The approval process may vary depending on the size of your organization. For example, your senior management team may be the group who will ultimately select the mitigation alternatives to be implemented or make the decision to accept the residual risk.

**Additional resources created by the LTC Consortium:**

1. Overview of the HIPAA Security Rule and Risk Analysis
2. Risk Assessment Matrix Definitions
3. Risk Assessment Matrix
4. Policy and Procedure Overview
5. Security Standards: Matrix
6. Risk Assessment Matrix Instructions
7. Risk Assessment Training Program