



Risk Assessment Matrix Instructions

This document will walk you through each column of the Risk Assessment Matrix. Please print the Risk Assessment Matrix document before beginning to review these instructions. You will notice that the Risk Assessment Matrix already contains some data. The LTC Consortium Security Subcommittee has identified potential risks for each Standard and Implementation Specification with the hope that this information will assist you in your risk identification. The information contained in the tool is just a sampling of the types of risk you might identify for your company.

If you prefer not to use the risks identified by the subcommittee – you will notice there is a second Risk Assessment Matrix that is blank. Both documents are created in Microsoft Excel and are meant for you to update as you work through your Risk Analysis.

This is a companion document to several other LTC Consortium tools; the Overview of the HIPAA Security Rule and Risk Analysis; the Risk Assessment Matrix Overview and the Risk Assessment Matrix Definition document.

Column 1: Implementation Specification

This column contains both Security Rule Standards and Implementation Specifications. The gray box identifies the Security Rule Standard and the corresponding regulation number. Each “row” beneath the Standard is a specific Implementation Specification. Implementation Specifications are instructions for implementing the Security Standards as stated in the Security Rule.

Column 2: Required vs. Addressable

Each Security Standard is required. However, the Implementation Specifications may be required OR addressable. This column simply identifies whether or not the Implementation Specification is Required or Addressable. (Please refer to page 8336 of the Federal Register Vol. 68, No. 34 for specific instructions on how to handle the Addressable Implementation Specifications.)

Column 3: Risk

This column will be used to identify a risk for the delineated Standard or Implementation Specification. The Risk is “what” can happen. (Refer to the LTC Consortium Assessment Matrix Definition document)

Column 4: Vulnerability

This column will be used to identify a vulnerability specific to the Risk identified. The Vulnerability is “how” a risk can happen. (Refer to the LTC Consortium Assessment Matrix Definition document)

Columns 5 through 8 all relate to the Threat

Column 5: Threat

This column will be used to document a threat specific to the risk identified. The Threat is “who” can cause the risk to happen. (Refer to the LTC Consortium Assessment Matrix Definition document)

Column 6: Actor

This column will be used to document whether or not the actor (who) is internal or external. In other words, is the threat carried out by someone internal to your organization or external?

Column 7: Motive

This column will be used to document whether or not the act being carried out is a deliberate or accidental event.

Column 8: Access

This column will be used to document whether or not the risk is via the network or an actual physical threat.

Columns 9 and 10 relate to the Outcome

Column 9: Security Requirement

This column will be used to document one of three fundamental Security Requirements – those are Confidentiality, Integrity and Availability. For each risk identified you will determine how the e-PHI is at risk – is it the Confidentiality, Integrity and/or Availability of the e-PHI. (Refer to the LTC Consortium Assessment Matrix Definition document)

Column 10: Outcome

This column will be used to document the outcome if the risk is carried out. The possible outcomes are; disclosure, modification, loss/destruction and/or interruption. Typically there is a correlation between the Security Requirement and the Outcome. (Refer to the LTC Consortium Assessment Matrix Definition document)

Columns 11 through 13 relate to the Total Risk Score

Column 11: Probability

This column will be used to document the probability of the identified risk being carried out. You will score each risk with a 1, 2 or 3. A score of 3 indicates the highest probability.

Column 12: Impact

This column will be used to document the impact if the identified risk is carried out. You will score each risk with a 1, 2, or 3. A score of 3 indicates the highest impact.

Column 13: Risk Score

This column will be used to document the calculated Risk Score. This score is calculated by multiplying the Probability Score and the Impact Score. Your results will be between 1 and 9 with 9 being the most significant risk.

Column 14: Comments

This column of course is just to be used for any anecdotal thoughts that should be documented along the way.