HOW TO COMPLETE THE FORMS

Introduction

Completion of this tool will assist a practice in complying with Meaningful Use and the HIPAA Security Rule, but it is not a guarantee of compliance with either. Practices are still obligated to comply with the specific requirements of each rule. Use of this tool will provide an overall view of the state of security and provide suggestions for remediation of deficiencies. A complete risk assessment must address each asset type separately, which this tool does not do.

This Risk Assessment Tool contains a four-step process designed to enable respondents to identify their level of risk against pre-identified threats and vulnerabilities. The tool is designed for ease of use and user-friendliness. **Cells that populated on one table will be automatically populated on subsequent tabs to ensure accuracy and simplicity.** The US Department of Health and Human Services(HHS), Office for Civil Rights (OCR) references components of the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-66 and 800-30 as guidance for a security risk assessment. NIST SP 800-66 is an introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, and NIST SP 800-30 is a risk management guide for information technology systems.

Background information on the nine primary steps to the risk assessment methodology outlined in NIST SP 800-66 and in NIST SP 800-30 is available on the next tab, labeled **800-66 Risk Guidance**. These steps offer helpful background information on the assessment steps, how they interact with one another and basic descriptions of risk and the components of risk, such as threats and vulnerabilities. Internet links to NIST SP 800-66 and SP 800-30 are also provided for those seeking additional information.

Purpose

The purpose of a risk assessment is to identify conditions where Electronic Protected Health Information (EPHI) could be disclosed without proper authorization, improperly modified, or made unavailable when needed. This information is then used to make risk management decisions on what reasonable and appropriate safeguards are needed to reduce risk to an acceptable level.

This Risk Assessment Tool is intended to be a starting point for identifying cybersecurity risks to your organization.

The Risk Assessment Tool Four-Step Process

The following four-step process is provided for using the Risk Assessment Tool :

Step 1 is the **Screening Questions.** This tab is offered as a means for determining the degree to which threats and associated vulnerabilities apply to their organization's assets. While this tab is an optional feature in the risk analysis, it is strongly recommended that respondents utilize this tab, as these questions will assist in additional responses in Steps 2a and 2b. Users should examine the question and determine the degree to which their current operations address the matching Threat-Vulnerability Statement. The choices from the drop down menu are

Addressed, Partially Addressed or Not Addressed. A column is provided to the far right in the table for respondents to provide expanded responses to the questions in the row.

Steps 2a (People and Processes) and 2b (Technology) utilize the same questions, criteria and risk calculations. It is necessary to separate the two categories of assets for analysis purposes.

The People and Processes and Technology tabs will list assets typically found within a medical practice which are applicable to the Threat-Vulnerability Statement appearing in the next column.

The Recommended Control Measures**,** which is associated with the Threat-Vulnerability, is pre-populated and is provided for respondents to consider in developing their information security posture.

The Existing Control is what the practitioner is doing, if any corrective actions are being taken, to mitigate and reduce the threat or vulnerability. Please populate the cell with all actions and measures being taken to address the threat or vulnerability. If no action is taken, please indicate 'No Action Taken' in this space. There is no correct or incorrect response, this is merely a sampling of what practitioners are doing to mitigate threats or minimize vulnerabilities.

The Existing Control Effectiveness is a Drop-Down list in which the respondent will select the best answer to describe the degree to which their counter-measures address the Threat-Vulnerability statement earlier in the row. When making a selection, respondents should also consider how effective their counter-measures are in relation to the Recommended Control Activity which is suggested in the previous cell. The available response choices are Effective, Partially Effective or Not Effective.

The Exposure Potential is a pre-populated cell from the response in the previous Step 1 tab and represents the risk exposure to the practice for this Threat-Vulnerability statement. The risk exposure is rated on a scale of High, Medium or Low. The purpose is to offer additional guidance and empower the respondent in their selections on the following choices of Impact and the Likelihood of Occurrence, or simply 'Likelihood'. As with the Impact Rating, this is a judgment by the respondent as to how likely an 'Undesirable Event', such as power outage or fire, are to occur to the medical practice. Please select from the appropriate corresponding choice of:

VERY LIKELY is defined as having a probable chance of occurrence.

LIKELY is defined as having a significant chance of occurrence .

NOT LIKELY is defined as a modest or insignificant chance of occurrence .

Impact is the consequences of a security event to the medical practice**.** Please select from the appropriate corresponding choice of High, Medium or Low for each Business Asset.

HIGH is defined as having a catastrophic impact on the medical practice; the medical practice is incapable of offering medical treatments or services and a significant number of medical records have been lost or compromised.

MEDIUM is defined as having a significant impact; the medical practice may offer a reduced array of treatment services to patients. A moderate number of medical records within the practice have been lost or compromised.

LOW is defined as a modest or insignificant impact; the medical practice can continue to offer treatment to patients and some medical records may be lost or compromised.

***NOTE*: Any loss or compromise of 500 medical records or more requires that the practice notify the US Department of Health and Human Services (HHS), Office for Civil Rights (OCR) immediately.**

The Risk Rating requires *no action* by the respondent. The column automatically calculates the risk rating to the medical practice based upon the inputs to the 'Impact' and 'Likelihood' columns.

Step 3, Findings-Remediation, is the final tab requiring completion and is almost entirely auto-populated with data from previous tabs.   The Risks Found column is populated with the data from the People and Process or Technology asset tabs ,which in Steps 2a or 2b was determined to have a Risk Rating of either Medium or High. The Existing Control Measures Applied are the measures, if any, currently being undertaken to address the threat as was indicated in Steps 2a or 2b. Recommended Control Measures are the corresponding recommended corrective measures which were automatically populated in the tabs of Steps 2a and 2b and appear again in this space. The final cell, Additional Steps, offers the respondent an opportunity to consider and state any additional measures they would like to implement.

Step 4 is the **Inventorying of Assets** tab and is completely **optional** to the respondent. In this step, the respondent should list **ALL** devices that are touched by EPHI. Devices may be for example, desktop PCs, fax machines or specialized medical devices with computerized hard drives to record patient data and test results. Any software applications, whether for recording of patient information, billing information or any other purpose which comes into contact with EPHI should also be listed here. The next column will ask whether the device processes, stores or transmits EPHI.   If the devices does not process EPHI, there is no need to proceed further with this device. If the devices DOES process EPHI, then the respondent would select from the next column whether the asset should be categorized as a People and Process asset, or as a Technology asset.

NEXT STEP: Please proceed to the 800-66 Risk Guidance tab which provides guidance on conducting a risk assessment.