Tips for completing your own Security Risk Assessment (SRA)

Note: the information below is taken from an article written by the U.S. Department of Health and Human Services: Guidance on Risk Analysis Requirements under the HIPAA Security Rule.

In Accordance with 45 C.F.R §164.306, Eligible Professionals (EPs) must implement policies and procedures to prevent, detect, contain, and correct security violations.

The four implementation specifications are:

1. **Risk Analysis:** Conduct an accurate and through assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health (ePHI) information that is created, received, maintained or transmitted by the organization.
2. **Risk Management:** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
3. **Sanction Policy:** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.
4. **Information Systems Activity Review:** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

When beginning your security risk assessment, you must first identify all ePHI within your organization, including external sources (such as vendors, consultants, referring providers) for whom you exchange ePHI with. Next, consider all human, natural, or environmental threats to that ePHI.

This initial review will give you the foundation for your risk assessment. From there, you should begin by designing appropriate personnel screening processes, identify what data to backup, identify how to back up the data, decide how to use encryption, address what data must be authenticated in particular situations to protect data integrity, and determine the appropriate manner of protecting health information transmission.

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 technical or non-technical. Technical vulnerabilities include holes, flaws, or weaknesses in the development of information systems or incorrectly implemented or configured information systems. Non-technical vulnerabilities include ineffective or non-existent policies, procedures, standards or guidelines.

Threat: the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Threats can be natural, human, or environmental. Natural threats include floods, earthquakes, tornadoes, etc. Human threats include network attacks, malicious software uploads, unauthorized access, inadvertent data entry, deletion of patient data, or inaccurate data entry. Environmental threats include power failures, chemical leakage, pollution, etc.

Risk: the net mission impact considering (1) the probability that a particular threat will exercise (accidentally trigger or intentionally exploit) a particular vulnerability and (2) the resulting impact is this should occur.

Risks arise from legal liability or mission loss due to the following:

1. Unauthorized (malicious or accidental) disclosure, modification, or destruction of information.
2. Unintentional errors and omissions
3. IT disruptions due to natural or man-made disasters
4. Failure to exercise due care and diligence in the implementation and operation of the IT system.

Risks should be evaluated as a combination of 1) The likelihood of a given threat triggering or exploiting a particular vulnerability, and 2) the resulting impact on the organization. Therefore, a risk should not be viewed as a single event, but rather a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.

Elements of a Risk Analysis (required):

Scope of the analysis: includes the potential risks and vulnerabilities to the confidentiality, availability, and integrity of all ePHI that an organization creates, receives, maintains, or transmits. This includes ePHI in all forms of electronic media, such as hard drives, USBs or CDs, smart cards, transmission media, portable electronic media, etc.

Data Collection: identify and document where all of the ePHI is stored, received, maintained, or transmitted.

Identify and Document Potential Threats and Vulnerabilities: identify and document reasonably anticipated threats to ePHI. Identify different threats that are unique to your environment. Identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk of inappropriate access or disclosure of ePHI.

Assess Current Security Measures: assess and document the security measures used to safeguard ePHI and whether current security measures are configured and used properly.

Determine the Likelihood of Threat Occurrence: take into account the probability of potential risks to ePHI. The result of this assessment, combined with the initial list of threats, will influence the determination of which threats require protection against because they are “reasonably anticipated.” The output of this part should be documentation of all threat and vulnerability combinations with associated likelihood estimates.

Determine the Potential Impact of Threat Occurrence: consider the “criticality,” or impact, of potential risks to confidentiality, integrity, and availability or ePHI. Assess the magnitude of the potential impact

resulting from a threat triggering or exploiting a specific vulnerability. Your results may be qualitative, quantitative, or a combination of the two. The output of this process should be documentation of all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability, and integrity or ePHI within an organization.

Determine the Level of Risk: assign risk levels for all threat and vulnerability combinations. The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence.

Finalize Documentation and perform Periodic Review and Updates to the Risk Assessment: A truly integrated risk analysis and management process is performed as new technologies and business operations are planned. Events that would suggest a risk assessment update are: experiencing a security incident, changing ownership, loosing or gaining staff members, adopting new technology, etc. During these types of events, it is imperative to ensure that ePHI is reasonably and appropriately protected. If it is determined that existing security measures are not sufficient to protect against the risks associated with the evolving threats or vulnerabilities, a changing business environment, or the introduction of new technology, then the organization must determine if additional security measures are needed.

For information regarding audit requirements for PHI security, privacy, and breaches, click here http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html