Appendix E: Risk Assessment Guidelines

This appendix incorporates risk assessment concepts and processes described in NIST SP 800-30 Revision 1, *Effective Use of Risk Assessments in Managing Enterprise Risk*, the NIST Risk Management Framework, and the *HIPAA Security Series: Basics of Risk Analysis and Risk Management*. It is intended to assist covered entities in identifying and mitigating risks to acceptable levels.

The purpose of a risk assessment is to identify conditions where 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 whether the HIPAA-required implementation specifications are sufficient or what additional addressable implementation specifications are needed to reduce risk to an acceptable level.

Key Terms Defined

When talking about risk, it is important that terminology be defined and clearly understood. This section defines important terms associated with risk assessment and management.

- *Risk* is the potential impact that a threat can have on the confidentiality, integrity, and availability on EPHI by exploiting a vulnerability.
- *Threats* are anything that can have a negative impact on EPHI. Threats are:
    - Intentional (e.g., malicious intent); or
    - Unintentional (e.g., misconfigured server, data entry error).
- *Threat sources* are:
    - Natural (e.g., floods, earthquakes, storms, tornados);
    - Human (e.g., intentional such as identity thieves, hackers, spyware authors; unintentional such as data entry error, accidental deletions); or
    - Environmental (e.g., power surges and spikes, hazmat contamination, environmental pollution).
- *Vulnerabilities* are a flaw or weakness in a system security procedure, design, implementation, or control that could be intentionally or unintentionally exercised by a threat.
- *Impact* is a negative quantitative and/or qualitative assessment of a vulnerability being exercised on the confidentiality, integrity, and availability of EPHI.

It can be easy to confuse vulnerabilities and threats. An organization may be vulnerable to damage from power spikes. The threats that could exploit this vulnerability may be overloaded circuits, faulty building wiring, dirty street power, or too much load on the local grid. It is important to separate these two terms in order to assist in proper security control selection. In this example, security controls could range from installing UPS systems, additional fuse boxes, or standby generators, or rewiring the office. These

additional security controls may help to mitigate the vulnerability but not necessarily for each threat.

HIPAA Risk Assessment Requirements

Standard 164.308(a)(1)(i), *Security Management Process*, requires covered entities to:

> *Implement policies and procedures to prevent, detect, contain, and correct security violations.*

The Security Management Process standard includes four required implementation specifications. Two of these specifications deal directly with risk analysis and risk management.

1. **Risk Analysis (R[123])** – 164.308(a)(1)(ii)(A): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
2. **Risk Management (R)** – 163.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).

How to Conduct the Risk Assessment:

Risk assessments can be conducted using many different methodologies. There is no single methodology that will work for all organizations and all situations. The following steps represent key elements in a comprehensive risk assessment program, and provide an example of the risk assessment methodology described in NIST SP 800-30. It is expected that these steps will be customized to most effectively identify risk for an organization based on its own uniqueness. Even though these items are listed as steps, they are not prescriptive in the order that they should be conducted. Some steps can be conducted simultaneously rather than sequentially.

1. **Scope the Assessment.** The first step in assessing risk is to define the scope of the effort, resulting in a general characterization of the information system, its operating environment, and its boundary. To do this, it is necessary to identify where EPHI is created, received, maintained, processed, or transmitted.

   The scope of a risk assessment should include both the physical boundaries of a covered entity's location as well as a logical boundary covering the media containing EPHI, regardless of its location. Ensure that the risk assessment scope takes into consideration the remote work force and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and backup media).

2. **Gather Information.** During this step, the covered entity should identify:

   - The conditions under which EPHI is created, received, maintained, processed, or transmitted by the covered entity; and

[123] "R" indicates a required implementation specification.

- The security controls currently being used to protect the EPHI.

This step is essential to ensure that vulnerabilities and threats are correctly identified. For example, an invalidated belief that a policy is being followed can miss a potential vulnerability, and not knowing about portable media containing EPHI can miss a threat to that environment. The level of effort needed to gather the necessary information depends heavily on the scope of the assessment and the size of the covered entity.

3. **Identify Realistic Threats.** Often performed simultaneously with step 4, *Identify Potential Vulnerabilities*, the goal of this step is to identify the potential threat sources and compile a threat statement listing potential threat-sources that are applicable to the covered entity and its operating environment. The listing of threat sources should include realistic and probable human and natural incidents that can have a negative impact on an organizations ability to protect EPHI. Threats can be easily identified by examining the environments where EPHI is being used.

   Many external sources can be used for threat identification. Internet searches, vendor information, insurance data, and crime statistics are all viable sources of threat data. Examples of some common threat sources are listed in Table 5 below.

Table 5. Common Threat Sources

Type	Examples
Natural	Floods, earthquakes, tornados, landslides, avalanches, electrical storms, and other such events
Human	Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network-based attacks, malicious software upload, and unauthorized access to confidential information)
Environmental	Long-term power failure, pollution, chemicals, liquid leak

4. **Identify Potential Vulnerabilities.** Often performed simultaneously with step 3, *Identify Realistic Threats*, the goal of this step is to develop a list of vulnerabilities (flaws or weaknesses) that could be exploited by potential threat sources. This list should focus on realistic technical and nontechnical areas where EPHI can be disclosed without proper authorization, improperly modified, or made unavailable when needed.

   Covered entities should use internal and external sources to identify potential vulnerabilities. Internal sources may include previous risk assessments, vulnerability scan and system security test results, and audit reports. External sources may include Internet searches, vendor information, insurance data, and vulnerability databases such as the National Vulnerability Database (http://nvd.nist.gov). At the end of this appendix, a suggested (but not all-inclusive) source list is provided that organizations may wish to use to help in vulnerability identification.

5. **Assess Current Security Controls.** Often performed simultaneously with step 2, *Gather Information*, the purpose of this step is to determine if the implemented or planned security controls will minimize or eliminate risks to EPHI. A thorough understanding of the actual security controls in place for a covered entity will reduce the list of vulnerabilities, as well as the realistic probability, of a threat attacking (intentionally or unintentionally) EPHI.

   Covered entities should evaluate technical and nontechnical security controls at all places where EPHI is created, received, maintained, processed, or transmitted. This evaluation should determine whether the security measures implemented or planned are adequate to protect EPHI, and whether those measures required by the Security Rule are in place, configured, and used properly. The appropriateness and adequacy of security measures may vary depending on the structure, size, and geographical dispersion of the covered entity.

6. **Determine the Likelihood and the Impact of a Threat Exercising a Vulnerability.** The next major step in measuring the level of risk is to determine the likelihood and the adverse impact resulting from a threat successfully exploiting a vulnerability. This information can be obtained from existing organizational documentation, such as business impact and asset criticality assessments. A business impact assessment prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions.

   If these organizational documents do not exist, the system and data sensitivity can be determined based on the level of protection required to maintain the EPHI's confidentiality, integrity, and availability. The adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security objectives: integrity, availability, and confidentiality. Table 6 provides a brief description of each security objective and the consequence (or impact) of its not being met.

Table 6. Security Objectives and Impacts

Security Objective	Impacts
Loss of Confidentiality	System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Security Objective	Impacts
Loss of Integrity	System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.
Loss of Availability	If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

Some tangible impacts can be measured quantitatively in terms of lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts, such as the loss of public confidence, the loss of credibility, or damage to an organization's interest, cannot be measured in specific units but can be qualified or described in terms of high, medium, and low impacts. Qualitative and quantitative methods can be used to measure the impact of a threat occurring

7. **Determine the Level of Risk.** The purpose of this step is to assess the level of risk to the IT system. The determination of risk takes into account the information gathered and determinations made during the previous steps. The level of risk is determined by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk-level determination may be performed by assigning a risk level based on the average of the assigned likelihood and impact levels. A risk-level matrix, such as the sample depicted in Table 7, can be used to assist in determining risk levels.

Table 7. Sample Risk-Level Matrix

Threat Likelihood	Impact		
	Low	Moderate	High
High	Low	Moderate	High
Moderate	Low	Moderate	Moderate
Low	Low	Low	Low

8. **Recommend Security Controls.** During this step, security controls that could mitigate the identified risks, as appropriate to the organization's operations, are recommended. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. Security control recommendations provide input to the risk mitigation process, during which the recommended security controls are evaluated, prioritized, and implemented.

   It should be noted that not all possible recommended security controls can be implemented to reduce loss. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition to cost, organizations should consider the operational impact and feasibility of introducing the recommended security controls into the operating environment.

9. **Document the Risk Assessment Results.**

   Once the risk assessment has been completed (threat sources and vulnerabilities identified, risks assessed, and security controls recommended), the results of each step in the risk assessment should be documented. NIST SP 800-30 provides a sample risk assessment report outline that may prove useful to covered entities.

Risk Assessment Results Affect Risk Management

The results of a risk assessment play a significant role in executing an organization's risk management strategy. In the context of the HIPAA Security Rule, the security control baseline, which consists of the standards and required implementation specifications, should be viewed as the foundation or starting point in the selection of adequate security controls necessary to protect EPHI. In many cases, additional security controls or control enhancements will be needed to protect EPHI or to satisfy the requirements of applicable laws, policies, standards, or regulations.

The risk assessment provides important inputs to determine the sufficiency of the security control baseline. The risk assessment results, coupled with the security control baseline, should be used to identify which addressable implementation specifications should be implemented to adequately mitigate identified risks.

Risk Assessment Resources

The following resources may provide useful information to assist covered entities in performing risk assessment, analysis, and management activities, and demonstrate compliance with the Security Management Process standard and related implementation specifications:

- HIPAA Security Series, Basics of Risk Analysis and Risk Management, 6/2005: rev. 3/2007; http://www.cms.hhs.gov/EducationMaterials/Downloads/BasicsofRiskAnalysisandRiskManagement.pdf

- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*; http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- Department of Homeland Security (DHS) National Infrastructure Protection Plan; http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm
- NIST National Vulnerability Database (NVD); http://nvd.nist.gov/
- US-CERT; http://www.us-cert.gov/index.html
- Carnegie Mellon CERT Coordination Center; http://www.cert.org/insider_threat/