



HIPAA SECURITY SERIES

Basics of Risk Analysis and Risk Management

The two implementation specifications that anchor every HIPAA security program. We've walked every healthcare client we work with through these steps before they buy a single security tool. This is the same orientation — what risk analysis and risk management actually require, eight steps for each, written so a security officer can execute and a board can read it.

Risk Analysis

Risk Management

§ 164.308(a)(1)

NIST SP 800-30

BASICS OF RISK ANALYSIS AND RISK MANAGEMENT · PAPER 06

The security series of papers will provide guidance from the Centers for Medicare & Medicaid Services (CMS) on the rule titled "Security Standards for the Protection of Electronic Protected Health Information," found at 45 CFR Part 160 and Part 164, Subparts A and C, commonly known as the Security Rule. The Security Rule was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The series will contain seven papers, each focused on a specific topic related to the Security Rule. The papers, which cover the topics listed below, are designed to give HIPAA covered entities insight into the Security Rule and assistance with implementation of the security standards. This series explains specific requirements, the thought process behind those requirements, and possible ways to address the provisions.

CMS recommends that covered entities read the first paper in this series, "Security 101 for Covered Entities" before reading the other papers. The first paper clarifies important Security Rule concepts that will help covered entities as they plan for implementation. This sixth paper in the series is devoted to the required risk analysis and risk management implementation specifications and assumes the reader has a basic understanding of the Security Rule.

SERIES TOPICS

1. Security 101 for Covered Entities
2. Security Standards — Administrative Safeguards
3. Security Standards — Physical Safeguards
4. Security Standards — Technical Safeguards
5. Security Standards — Organizational, Policies & Procedures, and Documentation Requirements
6. Basics of Risk Analysis & Risk Management
7. Implementation for the Small Provider

COMPLIANCE DEADLINES — AS ORIGINALLY ISSUED

No later than April 20, 2005 for all covered entities except small health plans, which have until no later than April 20, 2006.

NOTE

To download the first paper in this series, "Security 101 for Covered Entities," visit the CMS website at: www.cms.hhs.gov/SecurityStandard/ under the "Regulation" page.

Background

All electronic protected health information (EPHI) created, received, maintained or transmitted by a covered entity is subject to the Security Rule. Covered entities are required to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of EPHI. The Security Rule requires covered entities to evaluate risks and vulnerabilities in their environments and to implement policies and procedures to address those risks and vulnerabilities.

The objectives of this paper are to:

- Review the Security Rule required implementation specifications for Risk Analysis and Risk Management.
- Review the basic concepts involved in security risk analysis and risk management.
- Discuss the general steps involved in risk analysis and risk management.

Security Rule Requirements for Risk Analysis and Risk Management

The Security Management Process standard, at § 164.308(a)(1)(ii) in the Administrative Safeguards section of the Security Rule, requires covered entities to “[i]mplement policies and procedures to prevent, detect, contain, and correct security violations.” The Security Management Process standard has four required implementation specifications. Two of the implementation specifications are Risk Analysis and Risk Management.

The required implementation specification at § 164.308(a)(1)(ii)(A), for Risk Analysis, requires a covered entity to, “[c]onduct 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.”

The required implementation specification at § 164.308(a)(1)(ii)(B), for Risk Management, requires a covered entity to “[i]mplement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a) [(the General Requirements of the Security Rule)].”

Both risk analysis and risk management are standard information security processes and are critical to a covered entity's Security Rule compliance efforts. As stated in the responses to public comment in the preamble to the Security Rule, risk analysis and risk management are important to covered entities since these processes will “form the foundation upon which an entity's necessary security activities are built.” (68 Fed. Reg. 8346.)

NOTE

Risk analysis and risk management serve as tools to develop and maintain a covered entity's strategy to protect the confidentiality, integrity, and availability of EPHI.

Much of the content included in this paper is adapted from government resources such as the National Institute of Standards and Technology (NIST) 800 Series of Special Publications (SP), specifically, SP 800-30 - Risk Management Guide for Information Technology Systems. These government resources are freely available in the public domain.

Although only federal agencies are required to follow federal guidelines like the NIST 800 series, non-federal covered entities may find their content valuable when performing compliance activities. As stated in the CMS frequently asked questions (FAQs) on the HIPAA Security Rule, *"Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization's implementation activities. While NIST documents were referenced in the preamble to the Security Rule, this does not make them required. In fact, some of the documents may not be relevant to small organizations, as they were intended more for large, governmental organizations."*

The Security Rule does not prescribe a specific risk analysis or risk management methodology. This paper is not intended to be the definitive guidance on risk analysis and risk management. Rather, the goal of this paper is to present the main concepts of the risk analysis and risk management processes in an easy-to-understand manner. Performing risk analysis and risk management can be difficult due to the levels of detail and variations that are possible within different covered entities. Covered entities should focus on the overall concepts and steps presented in this paper to tailor an approach to the specific circumstances of their organization.

Important Definitions to Understand

To better understand risk analysis and risk management processes, covered entities should be familiar with several important terms, including "vulnerability," "threat," and "risk," and the relationship between the three terms. These terms are not specifically defined in the Security Rule. The definitions in this paper are provided to put the Risk Analysis and Risk Management discussion in context. These definitions do not modify or update the Security Rule and are not inconsistent with the terms used in the Security Rule. Rather, the following definitions are consistent with common industry definitions and are from documented sources, such as NIST SP 800-30. Explanations of the terms are adapted from NIST SP 800-30 and are presented in the context of the Security Rule.

NOTE

A risk analysis will identify potential threats to and vulnerabilities of information systems and the associated risk.

Vulnerability

Vulnerability is defined in NIST SP 800-30 as *"[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, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as an inappropriate use or disclosure of EPHI. Vulnerabilities may be grouped into two general categories, technical and non-technical. Non-technical vulnerabilities may include ineffective or non-existent policies, procedures, standards or guidelines. Technical vulnerabilities may include: holes, flaws or weaknesses in the development of information systems; or incorrectly implemented and/or configured information systems.

Threat

An adapted definition of threat, from NIST SP 800-30, is *"[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability."*

There are several types of threats that may occur within an information system or operating environment. Threats may be grouped into general categories such as natural, human, and environmental. Examples of common threats in each of these general categories include:

- **Natural threats** may include floods, earthquakes, tornadoes, and landslides.
- **Human threats** are enabled or caused by humans and may include intentional (e.g., network and computer based attacks, malicious software upload, and unauthorized access to EPHI) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.
- **Environmental threats** may include power failures, pollution, chemicals, and liquid leakage.

Risk

The definition of risk is clearer once threat and vulnerability are defined. An adapted definition of risk, from NIST SP 800-30, is:

NOTE

A Vulnerability triggered or exploited by a Threat equals a 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 if this should occur. ...[R]isks arise from legal liability or mission loss due to —

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."

Risk is a function of 1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and 2) the resulting impact on the organization. This means that risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.

NOTE

A threat must have the capability to trigger or exploit a vulnerability to create risk.

Example Risk Analysis and Risk Management Steps

There are numerous methods of performing risk analysis and risk management. There is no single method or "best practice" that guarantees compliance with the Security Rule. However, most risk analysis and risk management pro-

cesses have common steps. The following steps are provided as examples of steps covered entities could apply to their environment. The steps are adapted from the approach outlined in NIST SP 800-30.

EXAMPLE RISK ANALYSIS STEPS

1. Identify the scope of the analysis.
2. Gather data.
3. Identify and document potential threats and vulnerabilities.
4. Assess current security measures.
5. Determine the likelihood of threat occurrence.
6. Determine the potential impact of threat occurrence.
7. Determine the level of risk.
8. Identify security measures and finalize documentation.

NOTE

CMS is not recommending that all covered entities follow this approach, but rather is providing it as a frame of reference.

EXAMPLE RISK MANAGEMENT STEPS

1. Develop and implement a risk management plan.
2. Implement security measures.
3. Evaluate and maintain security measures.

When the following example risk analysis and risk management approaches contain actions that are required for compliance with the Security Rule, such as documentation, appropriate language and citations are used to highlight the Security Rule requirement. For example, the statement within these example approaches that a covered entity "must document" a certain action is a reference to the requirements of § 164.316(b)(1)(ii), the Documentation standard. These example approaches identify that a covered entity must or should perform certain actions, as required by the Security Rule, but does not require a covered entity to meet the requirements only by using the methods, steps, or actions identified in the example approach.

Example Risk Analysis Steps

As previously stated, the Security Rule requires covered entities to conduct an accurate and thorough risk analysis. This section of the paper provides an example approach to risk analysis which may be used by covered entities.

1. Identify the Scope of the Analysis

Risk analysis is not a concept exclusive to the healthcare industry or the Security Rule. Risk analysis is performed using different methods and scopes. The risk analysis scope that the Security Rule requires is the potential risks and vulnerabilities to the confidentiality, availability and integrity of all EPHI that a covered entity creates, receives, maintains, or transmits. This includes EPHI in all forms of electronic media. Electronic media is defined in § 160.103, as:

"(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as

EXAMPLES OF ELECTRONIC MEDIA WITH EPHI

magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission."

Hard drives, Floppy Disks, CDs, DVDs, Smart Cards, Personal Digital Assistants (PDA), Transmission Media, or Portable Electronic Storage Media.

Electronic media could range from a single workstation to complex communications networks connected between multiple locations. Thus, a covered entity's risk analysis should take into account all of its EPHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its EPHI.

2. Gather Data

Once the scope of the risk analysis is identified, the covered entity should gather relevant data on EPHI. For example, a covered entity must identify where the EPHI is stored, received, maintained or transmitted. A covered entity could gather relevant data by: reviewing past and/or existing projects; performing interviews; reviewing documentation; or using other data gathering techniques. The data on EPHI gathered using these methods must be documented. (See §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

Many covered entities inventoried and performed an analysis of the use and disclosure of all protected health information (PHI) (which includes EPHI) as part of HIPAA Privacy Rule compliance, even though it was not a direct requirement. This type of inventory and analysis is a valuable input for the risk analysis.

The level of effort and resource commitment needed to complete the data gathering step depends on the covered entity's environment and amount of EPHI held. For example, a small provider that keeps its medical records on paper may be able to identify all EPHI within the organization by analyzing a single department which uses an information system to perform billing functions. In another covered entity with large amounts of EPHI, such as a health system, identification of all EPHI may require reviews of multiple physical locations, most (if not all) departments, multiple information systems, portable electronic media, and exchanges between business associates and vendors.

3. Identify and Document Potential Threats and Vulnerabilities

Once the covered entity has gathered and documented relevant data on EPHI, the next step is to identify potential threats and vulnerabilities to the confidentiality, availability and integrity of the EPHI. As discussed earlier, the potential for a threat to trigger or exploit a specific vulnerability creates risk. Therefore, identification of threats and vulnerabilities are central to determining the level of risk.

The identification of threats and vulnerabilities could be separated into two distinct steps but are so closely related in the risk analysis process that they should be identified at the same time. Independent identification may result in large lists

of threats and vulnerabilities that, when analyzed (in subsequent steps to identify risk), do not provide valuable information.

Identify and Document Threats

Covered entities must identify and document reasonably anticipated threats to EPHI. (See §§ 164.306(a)(2) and 164.316(b)(1)(ii).) To start, covered entities may compile a categorized list (such as natural, human, and environmental) of threats. Covered entities may identify different threats unique to the circumstances of their environment.

After the complete list is compiled, the covered entity should reduce the list to only those reasonably anticipated threats. This can be done by focusing on specific characteristics of the entity in relation to each of the threat categories. For example, the geographic location of the entity will determine the natural threats that may create a risk. A hurricane is a threat, but a covered entity in Kansas probably would not consider it a reasonably anticipated threat due to its location. However, a covered entity in Kansas should consider the likelihood of a tornado a reasonably anticipated threat.

NOTE

A covered entity should focus its list of threats to those that are reasonably anticipated.

For most covered entities, human threats will be of greatest concern, because human threats have the potential to be triggered or exploited more frequently than natural or environmental threats. Potential human sources that could target a covered entity and trigger or exploit vulnerabilities are employees (the most common source), ex-employees, hackers, commercial rivals, terrorists, criminals, general public, vendors, customers and visitors. Anyone that has the access, knowledge and/or motivation to cause an adverse impact on the covered entity can act as a threat.

Covered entities should analyze several information sources to help identify potential human threats to their systems. Information sources such as any history of system break-ins, security violation reports, and ongoing input from systems administrators, help desk personnel and the user community should be reviewed.

Identify and Document Vulnerabilities

While identifying potential threats, covered entities must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk to EPHI. (See §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).) The process of identifying vulnerabilities is similar to the process used for identifying threats. The entity should create a list of vulnerabilities, both technical and non-technical, associated with existing information systems and operations that involve EPHI.

There are numerous sources of information to review when identifying and documenting both technical and non-technical vulnerabilities. Sources of information to identify non-technical vulnerabilities may include previous risk analysis documentation, audit reports or security review reports. Sources of information to identify technical vulnerabilities may include assessments of information systems, information system security testing, or publicly available vulnerability lists and advisories.

The Internet is a valuable resource for sharing technical vulnerability lists and advisories. It contains sites that provide information on specific technical vulnerabilities and the mechanisms for sign-up and distribution of technical vulnerability advisories. These lists will be especially useful to large covered entities. In contrast, small covered entities will likely rely

on their business associates for identification of system vulnerabilities, especially if their applications and information systems are maintained by outside vendors or contractors.

Another important way to identify technical vulnerabilities in information systems is through information systems security testing. The purpose of security testing is to assess the effectiveness of the security safeguards implemented to protect data, such as EPHI. There are many approaches to security testing. A common approach may involve developing a security testing and evaluation plan and to use security testing tools to scan workstations or the entire network (workstations and servers) for known technical vulnerabilities. The output of the security testing may be a report identifying technical vulnerabilities that exist within the organization.

4. Assess Current Security Measures

The next step is to assess the current security measures. The goal of this step is to analyze current security measures implemented to minimize or eliminate risks to EPHI. For example, a vulnerability is not likely to be triggered or exploited by a threat if effective security measures are implemented.

Security measures can be both technical and non-technical. Technical measures are part of information systems hardware and software. Examples of technical measures include access controls, identification, authentication, encryption methods, automatic logoff and audit controls. Non-technical measures are management and operational controls, such as policies, procedures, standards, guidelines, accountability and responsibility, and physical and environmental security measures.

NOTE

Security measures can be both technical and non-technical.

Security measures implemented to reduce risk will vary among covered entities. For example, small covered entities tend to have more control within their environment. Small covered entities tend to have fewer variables (i.e. fewer workforce members and information systems) to consider when making decisions regarding how to safeguard EPHI. As a result, the appropriate security measures that reduce the likelihood of risk to the confidentiality, availability and integrity of EPHI in a small covered entity may differ from those that are appropriate in large covered entities.

The output of this step should be documentation of the security measures a covered entity uses to safeguard EPHI. The output should identify whether security measures required by the Security Rule are already in place. The documentation should also identify if current security measures are configured and used properly. (See §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

5. Determine the Likelihood of Threat Occurrence

Once the first four steps in the risk analysis process are complete, the covered entity has the information needed to determine 1) the likelihood that a threat will trigger or exploit a specific vulnerability and 2) the resulting impact on the covered entity. The next two steps (steps 5 and 6) use information gathered from the previous steps to help the covered entity make likelihood and impact determinations. The purpose of these steps is to assist the covered entity in determining the level of risk and prioritizing risk mitigation efforts.

"Likelihood of occurrence" is the probability that a threat will trigger or exploit a specific vulnerability. Covered entities should consider each potential threat and vulnerability combination and rate them by likelihood (or probability) that the combination would occur. Ratings such as high, medium and low or numeric representations of probability may be used

to express the likelihood of occurrence. The ratings used will depend on the covered entity's approach. For example, a covered entity may choose to rate risks as high, medium and low, which could be defined as:

- **High Likelihood** — a high probability exists that a threat will trigger or exploit one or more vulnerabilities. This might be due to the existence of multiple organizational deficiencies, such as the absence, inadequacy or improper configuration of security controls, or due to geographic location (such as, within a flood zone).
- **Medium Likelihood** — a moderate probability exists that a threat will trigger or exploit one or more vulnerabilities due to the existence of a single organizational deficiency, such as the lack of security measures.
- **Low Likelihood** — a low probability exists that a threat will trigger or exploit a single vulnerability due to the existence of a single organizational deficiency, such as improper configuration of security controls.

The output of this step should be documentation of all threat and vulnerability combinations with associated likelihood ratings that may impact the confidentiality, availability and integrity of EPHI of a covered entity. (See §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

6. Determine the Potential Impact of Threat Occurrence

If a threat triggers or exploits a specific vulnerability, there are many potential outcomes. For covered entities, the most common outcomes include, but are not limited to:

- Unauthorized access to or disclosure of EPHI.
- Permanent loss or corruption of EPHI.
- Temporary loss or unavailability of EPHI.
- Loss of financial cash flow.
- Loss of physical assets.

All of these outcomes have the potential to affect the confidentiality, availability and integrity of EPHI created, received, maintained, or transmitted by covered entities. The impact of potential outcomes, such as those listed above, should be measured to assist the covered entity in prioritizing risk mitigation activities.

Measuring the impact of a threat occurring in a covered entity can be performed using different methods. The most common methods are qualitative and quantitative. Both of these methods allow a covered entity to measure risk.

Qualitative Method

The qualitative method rates the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability on a scale such as high, medium and low. The qualitative method is the most common measure used to measure the impact of risk. This method allows the covered entity to measure all potential impacts, whether tangible or intangible. For example, an intangible loss, such as a loss of public confidence or loss of credibility, can be measured using a high, medium or low scale.

NOTE

Covered entities should consider the advantages and disadvantages of both qualitative and quantitative methods for determining the potential impact.

Quantitative Method

In contrast, the quantitative method measures the tangible potential impact of a threat triggering or exploiting a specific vulnerability, using a numeric value associated with resource cost. This might include resource costs, such as repair costs to information systems or the replacement cost for an asset that is lost or stolen. The quantitative method provides valuable information for cost-benefit analysis associated with risks. However, it is generally difficult to assign numeric values to intangible losses. Therefore, all potential impacts generally cannot be determined using this method.

A covered entity may use either method or a combination of the two methods to measure impact on the organization. Since there is no single correct method for measuring the impact during the risk analysis, a covered entity should consider the advantages and disadvantages of the two approaches.

The output of this step should be documentation of all potential impacts and ratings associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of EPHI within a covered entity. (See §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

7. Determine the Level of Risk

Next, covered entities should determine the level of risk to EPHI. As discussed earlier, risk is a function determined by the likelihood of a given threat triggering or exploiting a specific vulnerability and the resulting impact. The covered entity will use the output of the previous two steps (steps 5 and 6) as inputs to this step. The output of those steps, likelihood and potential impact of threat occurrence data, will focus the covered entity's risk level determination to reasonably anticipated risks to EPHI.

NOTE

Risk ranking will assist covered entities in prioritizing activities that must be performed.

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 can be used to assist in determining risk levels. A risk level matrix is created using the values for likelihood of threat occurrence and resulting impact of threat occurrence. The matrix may be populated using a high, medium, and low rating system, or some other rating system. For example, a threat likelihood value of "high" combined with an impact value of "low" may equal a risk level of "low." Or a threat likelihood value of "medium" combined with an impact value of "medium" may equal a risk level of "medium."

Next, each risk level is labeled with a general action description to guide senior management decision making. The action description identifies the general timeline and type of response needed to reasonably and appropriately reduce the risk to acceptable levels. For example, a risk level of "high" could have an action description requiring immediate implementation of corrective measures to reduce the risk to a reasonable and appropriate level. Assigning action descriptions provides the covered entity additional information to prioritize risk management efforts.

One output of this step should be documented risk levels for all threat and vulnerability combinations identified during the risk analysis. Another output should be a list of corrective actions to be performed to mitigate each risk level. (See §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

8. Identify Security Measures and Finalize Documentation

Once risk is identified and assigned a risk level, the covered entity should begin to identify the actions required to manage the risk. The purpose of this step is to begin identifying security measures that can be used to reduce risk to a reasonable and appropriate level. When identifying security measures that can be used, it is important to consider factors such as: the effectiveness of the security measure; legislative or regulatory requirements that require certain security measures to be implemented; and requirements of the organization's policies and procedures. Any potential security measures that can be used to reduce risks to EPHI should be included in documentation.

This step only includes identification of security measures. The evaluation, prioritization, modification, and implementation of security measures identified in this step is part of the risk management process, addressed in the next section "Example Risk Management Steps."

NOTE

During the risk management process, recommended security measures will be evaluated, prioritized, modified, and implemented.

The final step in the risk analysis process is documentation. The Security Rule requires the risk analysis to be documented but does not require a specific format. (See § 164.316(b)(1)(ii).) A risk analysis report could be created to document the risk analysis process, output of each step and initial identification of security measures. The risk analysis documentation is a direct input to the risk management process.

Example Risk Management Steps

Once the covered entity has completed the risk analysis process, the next step is risk management. Risk management, required by the Security Rule, includes the implementation of security measures to reduce risk to reasonable and appropriate levels to, among other things, ensure the confidentiality, availability and integrity of EPHI, protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI, and protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted or required under the HIPAA Privacy Rule.

1. Develop and Implement a Risk Management Plan

The first step in the risk management process should be to develop and implement a risk management plan. The purpose of a risk management plan is to provide structure for the covered entity's evaluation, prioritization, and implementation of risk-reducing security measures.

For the risk management plan to be successful, key members of the covered entity's workforce, including senior management and other key decision makers, must be involved. The outputs of the risk analysis process will provide these key workforce members with the information needed to make risk prioritization and mitigation decisions.

The risk prioritization and mitigation decisions will be determined by answering questions such as:

- Should certain risks be addressed immediately or in the future?
- Which security measures should be implemented?

Many of the answers to these questions will be determined using data gathered during the risk analysis. The entity has already identified, through that process, what vulnerabilities exist, when and how a vulnerability can be exploited by a threat, and what the impact of the risk could be to the organization. This data will allow the covered entity to make informed decisions on how to reduce risks to reasonable and appropriate levels.

An important component of the risk management plan is the plan for implementation of the selected security measures. The implementation component of the plan should address:

- Risks (threat and vulnerability combinations) being addressed;
- Security measures selected to reduce the risks;
- Implementation project priorities, such as: required resources; assigned responsibilities; start and completion dates; and maintenance requirements.

The implementation component of the risk management plan may vary based on the circumstances of the covered entity. Compliance with the Security Rule requires financial resources, management commitment, and the workforce involvement. Cost is one of the factors a covered entity must consider when determining security measures to implement. However, cost alone is not a valid reason for choosing not to implement security measures that are reasonable and appropriate.

The output of this step is a risk management plan that contains prioritized risks to the covered entity, options for mitigation of those risks, and a plan for implementation. The plan will guide the covered entity's actual implementation of security measures to reduce risks to EPHI to reasonable and appropriate levels.

2. Implement Security Measures

Once the risk management plan is developed, the covered entity must begin implementation. This step will focus on the actual implementation of security measures (both technical and non-technical) within the covered entity. The projects or activities to implement security measures should be performed in a manner similar to other projects, i.e., these projects or activities should each have an identified scope, timeline and budget. Covered entities may also want to consider the benefits, if any, of implementing security measures as part of another existing project, such as implementation of a new information system.

A covered entity may choose to use internal or external resources to perform these projects. The Security Rule does not require or prohibit either method. It is important to note that, even if it uses outside vendors to implement the security measures selected, the covered entity is responsible for its compliance with the Security Rule.

3. Evaluate and Maintain Security Measures

The final step in the risk management process is to continue evaluating and monitoring the risk mitigation measures implemented. Risk analysis and risk management are not one-time activities. Risk analysis and risk management are ongoing, dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management processes to reduce newly identified or updated risk levels to reasonable and appropriate levels.

The Security Rule requires covered entities to maintain compliance with the standards and implementation specifications. 45 CFR § 164.306(e), states:

"Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 [(the Organizational Requirements)] and this subpart [(the Security Rule)] must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of [EPHI] as described at § 164.316."

The Security Rule does not specify how frequently to perform risk analysis and risk management. The frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed (e.g., bi-annual or every 3 years) depending on circumstances of their environment.

A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation. The Evaluation standard (§ 164.308(a)(8)) requires covered entities to:

"Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of [EPHI], that establishes the extent to which an entity's security policies and procedures meet the requirements of [the Security Rule]."

For example, if the covered entity is planning to incorporate new technology to make operations more efficient, such as using notebook computers or handheld devices that contain EPHI, the potential risk to these devices must be analyzed to ensure the 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 new technology, then the entity must determine if additional security measures are needed. Performing the risk analysis and risk management processes before implementing the new technology will allow the covered entity to reduce the associated risks to reasonable and appropriate levels.

In Summary

Risk analysis and risk management are the foundation of a covered entity's Security Rule compliance efforts. Risk analysis and risk management are on going processes that will provide the covered entity with a detailed understanding of the risks to EPHI and the security measures needed to effectively manage those risks. Performing these processes appropriately will ensure the confidentiality, availability and integrity of EPHI, protect against any reasonably anticipated threats or hazards to the security or integrity of EPHI, and protect against any reasonably anticipated uses or disclosures of EPHI that are not permitted or required under the HIPAA Privacy Rule.

Resources

The previous papers in this series address specific requirements of the Security Rule. The final paper in this series will address implementation of Security Rule standards and implementation specifications in the small provider environment.

Covered entities should periodically check the CMS website at www.cms.hhs.gov under "Regulations and Guidance" for additional information and resources as they work through the security implementation process. There are many other sources of information available on the Internet. While CMS does not endorse guidance provided by other organizations, covered entities may also want to check with other local and national professional health care organizations, such as national provider and health plan associations for additional information.

NEED MORE INFORMATION?

Visit the CMS website often at www.cms.hhs.gov under "Regulations and Guidance" for the latest security papers, checklists, and announcements of upcoming events.

Visit the Office for Civil Rights website, <http://www.hhs.gov/ocr/hipaa>, for the latest guidance, FAQs and other information on the Privacy Rule.

Security Standards Matrix

Appendix A of the Security Rule. Tags:

R REQUIRED

A ADDRESSABLE

Administrative Safeguards		
Standard	Section	Implementation Specifications
Security Management Process	164.308 (a) (1)	Risk Analysis R
		Risk Management R
		Sanction Policy R
		Information System Activity Review R
Assigned Security Responsibility	164.308 (a) (2)	— R
Workforce Security	164.308 (a) (3)	Authorization and/or Supervision A
		Workforce Clearance Procedures A
		Termination Procedures A
Information Access Management	164.308 (a) (4)	Isolating Health Care Clearinghouse Functions R
		Access Authorization A
		Access Establishment and Modification A
Security Awareness and Training	164.308 (a) (5)	Security Reminders A
		Protection from Malicious Software A
		Log-in Monitoring A
		Password Management A
Security Incident Procedures	164.308 (a) (6)	Response and Reporting R
Contingency Plan	164.308 (a) (7)	Data Backup Plan R

Standard	Section	Implementation Specifications
		Disaster Recovery Plan R
		Emergency Mode Operation Plan R
		Testing and Revision Procedure A
		Applications and Data Criticality Analysis A
Evaluation	164.308 (a) (8)	— R
Business Associate Contracts and Other Arrangements	164.308 (b) (1)	Written Contract or Other Arrangement R

Physical Safeguards

Standard	Section	Implementation Specifications
Facility Access Controls	164.310 (a) (1)	Contingency Operations A
		Facility Security Plan A
		Access Control and Validation Procedures A
		Maintenance Records A
Workstation Use	164.310 (b)	— R
Workstation Security	164.310 (c)	— R
Device and Media Controls	164.310 (d) (1)	Disposal R
		Media Re-use R
		Accountability A
		Data Backup and Storage A

Technical Safeguards

Standard	Section	Implementation Specifications
Access Control	164.312 (a) (1)	Unique User Identification R
		Emergency Access Procedure R
		Automatic Logoff A
		Encryption and Decryption A
Audit Controls	164.312 (b)	— R
Integrity	164.312 (c) (1)	Mechanism to Authenticate Electronic Protected Health Information A
Person or Entity Authentication	164.312 (d)	— R
Transmission Security	164.312 (e) (1)	Integrity Controls A
		Encryption A

Organizational Requirements

Standard	Section	Implementation Specifications
Business associate contracts or other arrangements	164.314 (a) (1)	Business Associate Contracts R
		Other Arrangements R
Requirements for Group Health Plans	164.314 (b) (1)	Implementation Specifications R

Policies and Procedures and Documentation Requirements

Standard	Section	Implementation Specifications
Policies and Procedures	164.316 (a)	—
Documentation	164.316 (b) (1)	Time Limit R
		Availability R

Standard	Section	Implementation Specifications
		Updates R



CYBER SECURITY RESOURCE

PROTECTING DATA · SECURING TRUST

About Cyber Security Resource

Protecting Data — Securing Trust

We're a healthcare-focused cybersecurity firm. We help medical technology, SaaS, and regulated organizations build security programs that hold up — under audit, under attack, and under board scrutiny.

Our approach is structured and cost-effective. We focus on practical risk management, compliance alignment, and real-world security testing. The goal is simple: **meet HIPAA, HITRUST, and enterprise customer requirements with confidence** — without spending a year and six figures to get there.

This library is the same orientation we hand a new client on day one. Use it as a working reference; the requirements are unchanged from the original CMS guidance, and the design is built to be readable in a boardroom or on a security analyst's second monitor.

CONTACT

support@cybersecurityresource.com
+1 (442) 222-1338

HEADQUARTERS

Carlsbad, California
United States

WEB · EDITION

cybersecurityresource.com
Cyber Security Resource Edition ·
2026