

Guidance on Risk Analysis Requirements under the HIPAA Security Rule

Introduction

The Office for Civil Rights (OCR) is responsible for issuing annual guidance on the provisions in the HIPAA Security Rule.¹ (45 C.F.R. §§ 164.302 – 318.) This series of guidances will assist organizations² in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to secure electronic protected health information (e-PHI). The guidance materials will be developed with input from stakeholders and the public, and will be updated as appropriate. We begin the series with the risk analysis requirement in § 164.308(a)(1)(ii)(A). Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. Therefore, a risk analysis is foundational, and must be understood in detail before OCR can issue meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information. The guidance is not intended to provide a one-size-fits-all blueprint for compliance with the risk analysis requirement. Rather, it clarifies the expectations of the Department for organizations working to meet these requirements.³ An organization should determine the most appropriate way to achieve compliance, taking into account the characteristics of the organization and its environment. We note that some of the content contained in this guidance is based on recommendations of the National Institute of Standards and Technology (NIST). NIST, a federal agency, publishes freely available material in the public domain, including guidelines.⁴ Although only federal agencies are required to follow guidelines set by NIST, the guidelines represent the industry standard for good business practices with respect to standards for securing e-PHI. Therefore, non-federal organizations may find their content valuable when developing and performing compliance activities. All e-PHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of e-PHI. Risk analysis is the first step in that process. We understand that the Security Rule does not prescribe a specific risk analysis methodology, recognizing that methods will vary dependent on the size, complexity, and capabilities of the organization. Instead, the Rule identifies risk analysis as the foundational element in the process of achieving compliance, and it establishes several objectives that any methodology adopted must achieve.

¹ Section 13401(c) of the Health Information Technology for Economic and Clinical (HITECH) Act.

² As used in this guidance the term “organizations” refers to covered entities and business associates. The guidance will be updated following implementation of the final HITECH regulations.

³ The HIPAA Security Rule: Health Insurance Reform: Security Standards, February 20, 2003, 68 FR 8334.

⁴ The 800 Series of Special Publications (SP) are available on the Office for Civil Rights’ website – specifically, *SP 800-30 - Risk Management Guide for Information Technology Systems*. (<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html>.)

Risk Analysis Requirements under the Security Rule

The Security Management Process standard in the Security Rule requires organizations to “[i]mplement policies and procedures to prevent, detect, contain, and correct security violations.” (45 C.F.R. § 164.308(a)(1).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Section 164.308(a)(1)(ii)(A) states:

RISK ANALYSIS (Required). 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 [organization].

The following questions adapted from NIST Special Publication (SP) 800-66⁵ are examples organizations could consider as part of a risk analysis. These sample questions are not prescriptive and merely identify issues an organization may wish to consider in implementing the Security Rule:

- Have you identified the e-PHI within your organization? This includes e-PHI that you create, receive, maintain or transmit.
- What are the external sources of e-PHI? For example, do vendors or consultants create, receive, maintain or transmit e-PHI?
- What are the human, natural, and environmental threats to information systems that contain e-PHI?

In addition to an express requirement to conduct a risk analysis, the Rule indicates that risk analysis is a necessary tool in reaching substantial compliance with many other standards and implementation specifications. For example, the Rule contains several implementation specifications that are labeled “addressable” rather than “required.” (68 FR 8334, 8336 (Feb. 20, 2003).) An addressable implementation specification is not optional; rather, if an organization determines that the implementation specification is not reasonable and appropriate, the organization must document why it is not reasonable and appropriate and adopt an equivalent measure if it is reasonable and appropriate to do so. (See 68 FR 8334, 8336 (Feb. 20, 2003); 45 C.F.R. § 164.306(d)(3).) The outcome of the risk analysis process is a critical factor in assessing whether an implementation specification or an equivalent measure is reasonable and appropriate. Organizations should use the information gleaned from their risk analysis as they, for example:

- Design appropriate personnel screening processes. (45 C.F.R. § 164.308(a)(3)(ii)(B).)
- Identify what data to backup and how. (45 C.F.R. § 164.308(a)(7)(ii)(A).)
- Decide whether and how to use encryption. (45 C.F.R. §§ 164.312(a)(2)(iv) and (e)(2)(ii).)
- Address what data must be authenticated in particular situations to protect data integrity. (45 C.F.R. § 164.312(c)(2).)
- Determine the appropriate manner of protecting health information transmissions. (45 C.F.R. § 164.312(e)(1).)

⁵ See NIST SP 800-66, Section #4 "Considerations When Applying the HIPAA Security Rule." Available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf>

Important Definitions

Unlike “availability”, “confidentiality” and “integrity”, the following terms are not expressly defined in the Security Rule. The definitions provided in this guidance, which are consistent with common industry definitions, are provided to put the risk analysis discussion in context. These terms do not modify or update the Security Rule and should not be interpreted inconsistently with the terms used in the Security Rule.

Vulnerability

Vulnerability is defined in NIST Special Publication (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 inappropriate access to or disclosure of e-PHI. 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 such as 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 e-PHI) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.
- Environmental threats such as power failures, pollution, chemicals, and liquid leakage.

Risk

An adapted definition of risk, from NIST SP 800-30, is:

“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 can be understood as 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.

Elements of a Risk Analysis

There are numerous methods of performing risk analysis and there is no single method or “best practice” that guarantees compliance with the Security Rule. Some examples of steps that might be applied in a risk analysis process are outlined in NIST SP 800-30.⁶

The remainder of this guidance document explains several elements a risk analysis must incorporate, regardless of the method employed.

Scope of the Analysis

The scope of risk analysis that the Security Rule encompasses includes the potential risks and vulnerabilities to the confidentiality, availability and integrity of all e-PHI that an organization creates, receives, maintains, or transmits. (45 C.F.R. § 164.306(a).) This includes e-PHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media. Electronic media includes a single workstation as well as complex networks connected between multiple locations. Thus, an organization’s risk analysis should take into account all of its e-PHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its e-PHI.

Data Collection

An organization must identify where the e-PHI is stored, received, maintained or transmitted. An organization could gather relevant data by: reviewing past and/or existing projects; performing interviews; reviewing documentation; or using other data gathering techniques. The data on e-PHI gathered using these methods must be documented. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1).)

Identify and Document Potential Threats and Vulnerabilities

Organizations must identify and document reasonably anticipated threats to e-PHI. (See 45 C.F.R. §§ 164.306(a)(2) and 164.316(b)(1)(ii).) Organizations may identify different threats that are unique to the circumstances of their environment. Organizations must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

Assess Current Security Measures

Organizations should assess and document the security measures an entity uses to safeguard e-PHI, whether security measures required by the Security Rule are already in place, and if current security measures are configured and used properly. (See 45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1).) The security measures implemented to reduce risk will vary among organizations. For example, small organizations tend to have more control within their environment

⁶ Available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf>.

Small organizations tend to have fewer variables (i.e. fewer workforce members and information systems) to consider when making decisions regarding how to safeguard e-PHI.

As a result, the appropriate security measures that reduce the likelihood of risk to the confidentiality, availability and integrity of e-PHI in a small organization may differ from those that are appropriate in large organizations.⁷

Determine the Likelihood of Threat Occurrence

The Security Rule requires organizations to take into account the probability of potential risks to e-PHI. (See 45 C.F.R. § 164.306(b)(2)(iv).) The results of this assessment, combined with the initial list of threats, will influence the determination of which threats the Rule requires 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 that may impact the confidentiality, availability and integrity of e-PHI of an organization. (See 45 C.F.R. §§ 164.306(b)(2)(iv), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

Determine the Potential Impact of Threat Occurrence

The Rule also requires consideration of the “criticality,” or impact, of potential risks to confidentiality, integrity, and availability of e-PHI. (See 45 C.F.R. § 164.306(b)(2)(iv).) An organization must assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. An entity may use either a qualitative or quantitative method or a combination of the two methods to measure the impact on the organization.

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 of e-PHI within an organization. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

Determine the Level of Risk

Organizations should assign risk levels for all threat and vulnerability combinations identified during the risk analysis. 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. The risk level determination might be performed by assigning a risk level based on the average of the assigned likelihood and impact levels.

The output should be documentation of the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

⁷ For more information on methods smaller entities might employ to achieve compliance with the Security Rule, see #7 in the Center for Medicare and Medicaid Services’ (CMS) Security Series papers, titled “Implementation for the Small Provider.” Available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf>.

Finalize Documentation

The Security Rule requires the risk analysis to be documented but does not require a specific format. (See 45 C.F.R. § 164.316(b)(1).) The risk analysis documentation is a direct input to the risk management process.

Periodic Review and Updates to the Risk Assessment

The risk analysis process should be ongoing. In order for an entity to update and document its security measures “as needed,” which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed. (45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii).) The Security Rule does not specify how frequently to perform risk analysis as part of a comprehensive risk management process. 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. For example, if the covered entity has experienced a security incident, has had change in ownership, turnover in key staff or management, is planning to incorporate new technology to make operations more efficient, the potential risk should be analyzed to ensure the e-PHI 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 entity must determine if additional security measures are needed. Performing the risk analysis and adjusting risk management processes to address risks in a timely manner will allow the covered entity to reduce the associated risks to reasonable and appropriate levels.⁸

In Summary

Risk analysis is the first step in an organization’s Security Rule compliance efforts. Risk analysis is an ongoing process that should provide the organization with a detailed understanding of the risks to the confidentiality, integrity, and availability of e-PHI.

Resources

The Security Series papers available on the Office for Civil Rights (OCR) website, <http://www.hhs.gov/ocr/hipaa>, contain a more detailed discussion of tools and methods available for risk analysis and risk management, as well as other Security Rule compliance requirements. Visit <http://www.hhs.gov/ocr/hipaa> for the latest guidance, FAQs and other information on the Security Rule.

⁸ For more information on methods smaller entities might employ to achieve compliance with the Security Rule, see #6 in the Center for Medicare and Medicaid Services’ (CMS) Security Series papers, titled “Basics of Risk Analysis and Risk Management.” Available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf>.

Several other federal and non-federal organizations have developed materials that might be helpful to covered entities seeking to develop and implement risk analysis and risk management strategies. The Department of Health and Human Services does not endorse or recommend any particular risk analysis or risk management model. The documents referenced below do not constitute legally binding guidance for covered entities, nor does adherence to any or all of the standards contained in these materials prove substantial compliance with the risk analysis requirements of the Security Rule. Rather, the materials are presented as examples of frameworks and methodologies that some organizations use to guide their risk analysis efforts.

The National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce, is responsible for developing information security standards for federal agencies. NIST has produced a series of Special Publications, available at <http://csrc.nist.gov/publications/PubsSPs.html>, which provide information that is relevant to information technology security. These papers include:

- Guide to Technical Aspects of Performing Information Security Assessments (SP800-115)
- Information Security Handbook: A Guide for Managers (SP800-100; Chapter 10 provides a Risk Management Framework and details steps in the risk management process)
- An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (SP800-66; Part 3 links the NIST Risk Management Framework to components of the Security Rule)
- A draft publication, Managing Risk from Information Systems (SP800-39)

The Office of the National Coordinator for Health Information Technology (ONC) has produced a risk assessment guide for small health care practices, called Reassessing Your Security Practices in a Health IT Environment, which is available at http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10741_848086_0_0_18/SmaIIPracticeSecurityGuide-1.pdf.

The Healthcare Information and Management Systems Society (HIMSS), a private consortium of health care information technology stakeholders, created an information technology security practices questionnaire, available at <http://www.himss.org/content/files/ApplicationSecurityv2.3.pdf>. The questionnaire was developed to collect information about the state of IT security in the health care sector, but could also be a helpful self-assessment tool during the risk analysis process.

The Health Information Trust Alliance (HITRUST) worked with industry to create the Common Security Framework (CSF), a proprietary resource available at <http://hitrustcentral.net/files>. The risk management section of the document, Control Name: 03.0, explains the role of risk assessment and management in overall security program development and implementation. The paper describes methods for implementing a risk analysis program, including knowledge and process requirements, and it links various existing frameworks and standards to applicable points in an information security life cycle.