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 organizations[2] 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

---

[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.)

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.

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) 800-66[5] 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

[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