Overview of HIPAA's Security Risk Analysis Requirement

HIPAA Critical Updates Workshop, September 2016

Jill Moore, UNC School of Government

The HIPAA Security Rule requires covered entities to:

- Ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI) that the covered entity creates, receives, maintains, or transmits.
- Protect against reasonably anticipated threats or hazards to the security or integrity of ePHI.
- Protect against reasonably anticipated uses or disclosures of ePHI that are not allowed by the HIPAA Privacy Rule.
- Ensure that workforce members comply with the HIPAA Security Rule.

To meet these requirements, covered entities must implement administrative, physical, and technical safeguards to protect ePHI. One of the administrative safeguards that the Rule requires is a security management process to prevent, detect, contain, and correct security violations (45 CFR 164.308(a)(1)). The first step in the security management process is a security risk analysis – an "accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability" of the covered entity's ePHI. Covered entities must then implement security measures to reduce the risks and vulnerabilities that are identified through the analysis.

Components of a Security Risk Analysis

The Security Rule does not prescribe a specific process or tool for conducting the security risk analysis, nor does it require covered entities to adopt particular technologies. However, the federal agency responsible for enforcing the Security Rule has published guidance documents that identify several steps as essential (see the Resources section of this handout for links to guidance documents). The following description of the steps is intended to introduce the process and some of the vocabulary associated with it. ***This brief description is not comprehensive and not sufficient to inform an adequate security risk analysis.*** Please make use of the tools and resources later in this document and consult with appropriate professionals in your entity in conducting the analysis.

1. Identify the scope of analysis: Identify all the covered entity's ePHI and take all of it into account in conducting the risk analysis.

2. Gather data: Collect and document relevant data on the entity's ePHI, such as where it is stored, received, maintained, or transmitted.

3. Identify and document potential threats and vulnerabilities to ePHI: This step requires an understanding of what constitutes a "threat" or "vulnerability." Those terms are defined in more detail in the glossary portion of this handout. In general, "vulnerability" means a flaw or

weakness in security systems, policies, or procedures that could result in a breach, while "threat" refers to the potential for a person or thing to either accidentally trigger a vulnerability, or intentionally exploit a vulnerability. A covered entity must identify and document which vulnerabilities would create a risk to ePHI, if the vulnerability was triggered or exploited by a threat. The entity should focus on reasonably anticipated threats and vulnerabilities and should make use of any information it may have to help identify the areas of focus, such as information about past violations or policies or security breaches, input from system administrators, and information from the user community.

4. Assess current security measures: The covered entity must analyze its current technical and non-technical security measures. The outcome of this step should be documentation of current security measures and a determination of whether they are configured and used properly.

5. Determine the likelihood of threat occurrence: The covered entity should use information gathered from the previous steps to assess how likely it is that a threat will trigger or exploit a specific vulnerability. Consider each potential threat and vulnerability combination, and rate its likelihood of occurrence. For example, an entity might choose to rate likelihood of occurrence as high, medium, or low.

6. Determine the potential impact of threat occurrence: The covered entity should consider what outcomes could occur if a threat triggers a vulnerability. For example, will there be unauthorized access to ePHI, or unauthorized disclosure? Will there be permanent loss or corruption of the ePHI? Or temporary loss or unavailability? The impact of these outcomes should be measured to prioritize risk management activities. Different guidance documents and tools provide more detailed information about how to measure impact.

7. Determine the level of risk to ePHI: Risk is determined by considering two things together: (1) the likelihood that a threat will trigger a specific vulnerability; and (2) the impact that will be produced if that happens. The information produced by steps 5 and 6 goes to those points, so it is important to consider that information in this step. Different guidance documents and tools provide more details about how to use the information to determine and assign levels (such as high, medium, or low) to each risk to ePHI that has been identified. Each risk level should be associated with a general action description that identifies the type and timeliness of response that will be needed if the risk occurs. For example, a "high" risk level might have a general action requirement of immediate corrective measures.

8. Identify security measures and finalize documentation: Once risks are identified and risk levels have been assigned, the covered entity will be able to identify actions required to manage the risk.

Risk analysis is an ongoing responsibility. An entity's risk analysis should be revisited at least annually, or more often if necessary to address a new technology or a new procedure involving ePHI.

Tools for Security Risk Analysis

The Office of the National Coordinator for Health Information Technology (ONC) offers a free downloadable Security Risk Assessment Tool at https://www.healthit.gov/providers-professionals/security-risk-assessment. This location on the HealthIT.gov website also contains additional information about the security risk analysis requirement.

Proprietary tools are available from various sources. They may be called "risk assessment" or "risk analysis" tools. Be aware that some tools called "risk assessment" are focused on a *different* risk assessment—the one that is required by the HIPAA Breach Notification Rule to evaluate risks associated with a specific breach incident. For purposes of meeting the requirements described in this handout, be sure the tool you select is a comprehensive *security* risk assessment tool that addresses all of the steps outlined above.

Other Resources

U.S. Department of Health & Human Services (HHS), Guidance on Risk Analysis Requirements under the HIPAA Security Rule, at http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

U.S. Department of Health & Human Services, HIPAA Security Series Paper 6: Basics of Risk Analysis and Risk Management, at http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf.

Glossary of Key Terms and Acronyms

Electronic protected health information (ePHI) – Protected health information (PHI) that is transmitted or maintained in electronic media. Electronic media includes electronic storage media, such as hard drives or USB drives, and transmission media, such as networks or the internet.

HHS – U.S. Department of Health and Human Services.

NIST – National Institute of Standards and Technology. NIST is a federal agency that publishes free materials for the public, including guidelines for managing risk in information technology systems.

OCR – Office for Civil Rights, U.S. Department of Health and Human Services. OCR enforces the HIPAA Privacy and Security rules and has issued guidance documents on many of their provisions.

ONC – Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. ONC is the federal entity responsible for coordinating nationwide efforts to

implement health information technology and electronic health information exchange. It maintains the website HealthIT.gov.

Security management process standard – The portion of the Security Rule that requires covered entities to have a security management process that includes (1) the security risk analysis, (2) risk management—security measures to reduce risks and vulnerabilities, (3) a sanction policy that applies appropriate sanctions against workforce members who fail to comply with security policies and procedures, and (4) information system activity review – procedures to regularly review records of information system activity, such as audit logs or access reports.

Threat – The potential for a person or thing to accidentally trigger or intentionally exploit a vulnerability. Threats include natural threats, such as floods; environmental threats, such as power failures; and human threats, which may be either intentional or unintentional acts that disrupt a system (e.g., with malicious software) or result in unauthorized access to ePHI.

Vulnerability – A flaw or weakness in system security procedures, design, implementation, or internal controls that could result in a security breach or a violation of security policy. A vulnerability may be technical or non-technical. Examples of technical vulnerabilities include flaws in the development of information systems, or incorrectly configured systems. Examples of non-technical vulnerabilities include ineffective or non-existent policies and procedures.