# Security Risk Analysis Tip Sheet

OCTOBER 2014

MINNESOTA MDH DEPARTMENT OF HEALTH

Minnesota Department of Health, Office of Health Information Technology | www.health.state.mn.us/e-health | MN.eHealth@state.mn.us

# Table of Contents



## Acknowledgements

**The Minnesota Department of Health thanks the many members of the Minnesota e-Health Initiative and the Minnesota e-Health Privacy and Security workgroup for their time, leadership and expertise in developing and endorsing this piece.**

**Minnesota e-Health Privacy and Security Workgroup Co-Chairs**

Laurie Beyer-Kropuenske, JD
Director, Information Policy Analysis Division
Minnesota Department of Administration

LaVonne Wieland, RHIA, CHP
System Director Compliance & Privacy Compliance
HealthEast Care System

**Special Advisors**

Sarah Radermacher, HIPAA & HITECH Compliance Consulting, LLC
Jane McGrath, Stratis Health
Bill Sonterre, Stratis Health

**Other Advisors and Project Support**

Lisa Moon, Office of Health Information Technology, Minnesota Department of Health
Bob Johnson, Office of Health Information Technology, Minnesota Department of Health

## Background

All electronic protected health information (ePHI) created, received, maintained or transmitted by an organization is subject to the HIPAA Security Rule.

## Are all healthcare providers, organizations required to complete a HIPAA Privacy & Security Risk Analysis?

Strong compliance programs are built on privacy, security and compliance functions. Conducting a security risk analysis is a key requirement of the HIPAA Security Rule. **HIPAA** requires all individuals, organizations, and agencies who meet the definition of a "covered entity (CE)" have an ongoing process to assess their HIPAA privacy and security activities and processes and implement a risk management process to correct identified deficiencies. The Security Risk Analysis is also a core requirement for providers seeking payment through the Medicare and Medicaid EHR Incentive Program, commonly known as the Meaningful Use Program. **Meaningful Use** (MU) requires eligible providers (EPs), eligible hospitals (EHs), and critical access hospitals (CAHs), conduct a security risk analysis and correct any identified deficiencies each time they attest to meaningful use. Table 1 shows the requirements for Meaningful use Stage 1 and Stage 2 related to the HIPAA Security Rule.

### Table 1: Meaningful Use Stage 1 and Stage 2- Security Risk Analysis

| Protect Electronic Health Information: Stage 1 and Stage 2 Meaningful Use Requirement | | |
|---|---|---|
| **OBJECTIVE** | **MEANINGFUL USE MEASURE** | **HIPAA REQUIREMENT** |
| **Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities** | **Stage 1 MU:**<br>Eligible Professionals (EP) must conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process. | The HIPAA Security Rule requires that an accurate and thorough analysis of potential risks and vulnerabilities is conducted to protect the confidentiality, integrity and availability of electronic protected health information. When the Security Risk Analysis is completed, you must take any additional "reasonable and appropriate" steps to reduce identified risks (45 CFR 164.308(a)(1)(ii)). |
| | **Stage 2 MU:**<br>Eligible Professionals need to meet the same security risk analysis requirements as Stage 1, but must also address encryption/security of data at rest. | |
| *Note: A Security Risk Analysis must be completed during each reporting period for Stage 1 and Stage 2 and yearly thereafter.* | | |

## What is a Risk Analysis?

The HIPAA Security Rule requires organizations that handle protected health information to regularly review the administrative, physical and technical safeguards they have in place to protect information. By conducting risk analysis, health care providers can uncover potential weaknesses in their security policies, processes and systems. Risk analysis also helps providers address vulnerabilities; potentially preventing health data breaches or other adverse security events while supporting improved security of patient health data.

A risk analysis is foundational to any compliance program and is built on guidance from NIST SP 800-30 Standards[1]. How it is completed will depend on the size, complexity and capabilities of the organization. Core Elements of a Risk Analysis are listed in Table 2.

### Table 2: Core Elements of Risk Analysis[2]

| CORE ELEMENTS OF RISK ANALYSIS | REQUIREMENTS | RESULTS AND OUTCOMES |
|---|---|---|
| **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 |
| **Data Collection** | An organization must identify where the e-PHI is stored, received, maintained or transmitted. The data on e-PHI collection methods must be documented. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)). | An organization must identify where the e-PHI is stored, received, maintained or transmitted |
| **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).)<br>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).) | Organizations identify threats that are unique to the circumstances of their environment (e.g., virus, spam; theft; fire)<br>Organizations identify vulnerabilities (e.g., anti-virus software not updated; laptops not encrypted; lack of policies and procedures) |

[1] Available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf.

[2] Adapted from Guidance on Risk Analysis Requirements under the HIPAA Security Rule 2010 Office of Civil Rights http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

| CORE ELEMENTS OF RISK ANALYSIS | REQUIREMENTS | RESULTS AND OUTCOMES |
|---|---|---|
| **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 45C.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. |
| **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).)<br>The results of this Analysis, 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).)<br>An organization must assess the magnitude of the potential impact resulting from a threat | 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.<br>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 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)). |

| CORE ELEMENTS OF RISK ANALYSIS | REQUIREMENTS | RESULTS AND OUTCOMES |
|---|---|---|
| **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 Analysis** | 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).) | A truly integrated risk analysis and risk management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation. |

## How frequently does a Security Risk Analysis need to be completed?

**HIPAA** does not mandate a time frame for conducting a risk analysis and mitigation plan. However, **MU** requirements specify the risk analysis is to be conducted prior to or during the MU reporting period. The recommended best practice is to conduct or review a risk analysis on an annual basis with ongoing documentation detailing plans and activities to correct identified deficiencies. The exception would be for covered entities that have undergone significant physical, environment, or system updates. In this situation the covered entity should conduct or review the risk analysis following these changes to ensure privacy and security of e-PHI has not been compromised. HIPAA also requires that policies and procedures that support strong security measures be clearly documented, maintained for six (6) years, accessible to all staff, and staff are trained on the policies and procedures. However, this activity is not the same as completing a security risk analysis.

## Correcting Identified Deficiencies

Items identified during the security risk analysis that do not meet HIPAA requirements are often referred to as "Identified deficiencies." Examples of identified deficiencies may include gaps or deficiencies in written policies and procedures, missing or incomplete documentation of security processes and omission of safeguard measures. Covered entities are required to document a plan to correct deficiencies identified during the risk analysis process, this is often referred to as a **Mitigation or Remediation Plan.**

## What should be included in the Mitigation Plan?

A **Mitigation Plan** should at a minimum, include a list of interventions and/or acceptance to address each deficiency identified during the security risk analysis. This includes the documentation of risk status (e.g., high, medium, low), the owner of the risk/mitigation strategy, a planned completion date for each risk mitigation, the actual completion date of such intervention and actions, as well as notes that track progress for correcting the deficiency. Unlike the security risk analysis which is normally a onetime/annual evaluation, the Mitigation Plan is an active-working document that details the steps the organization has undertaken to correct the deficiencies. The recommended best practice for the mitigation plan is to review and update activities to correct deficiencies on a quarterly basis. However, if a covered entity has a number of deficiencies to correct the **Mitigation Plan** may need to be reviewed and updated more frequently.

## Starting Point: Security Risk Analysis Tools and Resources

A new tool from The Office of the National Coordinator for Health IT (ONC) can help make the Health Insurance Portability and Accountability Act (HIPAA) Security Rule more understandable and security risk Analysis easier. The tool was designed to help guide health care providers in small to medium sized offices conduct risk assessments of their organizations. The Security Risk Analysis (SRA) Tool application lets users take a self-directed tour of HIPAA standards and conduct a self-paced risk Analysis. Download the Windows version of the tool at http://www.HealthIT.gov/security-risk-Analysis. For iPad users download the iOS iPad version from the Apple App Store (search under "HHS SRA Tool").

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/riskAnalysis.pdf

The Office of the National Coordinator for Health Information Technology (ONC) has produced a risk Analysis 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/SmallPracticeSecurityGuide-1.pdf

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 provides information that is relevant to information technology security.