The Security Risk Analysis Requirement for MIPS

August 8, 2017, 2:00 p.m. to 3:00 p.m. ET
Peter Mercuri, Practice Transformation Specialist
Today’s Speaker – Peter Mercuri

- Peter Mercuri, MBA, HCISPP, CHSA, CMQP, CEHR, CHTS, CHWP
- Practice Transformation Specialist
- Healthcare Information Security & Privacy Practitioner
- Certified HIPAA Security Administrator
- Responsible for conducting & reviewing Security Risk Analysis
- Member: ISC2, HIMSS, DVHIMSS Board Member, AHIMA
Agenda

1. The HIPAA Security Rule
2. Conducting a Security Risk Analysis
3. Security Areas to Consider
   - Physical Safeguards
   - Administrative Safeguards
   - Technical Safeguards
4. Policies & Procedures
5. The Security Risk Assessment Tool
6. Resources Available
7. Questions
HIPAA Security Rule Requirement for MIPS

• To conduct or review a Security Risk Analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI created or maintained by CERT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3).

• Under the HIPAA Security Rule, you are required to conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the covered entity or business associate. Once you have completed the risk analysis, you must take any additional “reasonable and appropriate” steps to reduce the identified risks to reasonable and appropriate levels. 45 CFR 164.308(a)(1)(ii)
How to Conduct a Bona Fide HIPAA Security Risk Analysis

• There is no single method or “best practice” that guarantees compliance, but most risk analysis and risk management processes have steps in common.

• Common question: Do I have to outsource the security risk analysis?
  – NO. It is possible for small practices to perform a risk analysis themselves using self-help tools; however, the risk analysis must be thorough to pass a CMS audit.
Points to Ponder

• There is a right way, but there are also many wrong ways
• The first security analysis requires a lot of work
• The analysis is not once and done
• It is one of the single biggest audit and investigation findings
• Always requested in OCR Enforcement Action
Performing a Security Risk Analysis
Important First Steps

- Establish a comprehensive information security program
- Designate an accountable Security Officer
- Develop privacy & security policies and procedures
- Distribute and update policies and procedures
- Document authorized access to ePHI
Additional Security Analysis Tasks

- Document process for responding to security incidents
- Implement training and sanctions for non-compliance
- Conduct a risk analysis/establish risk management process
- Implement reasonable safeguards to control risks
- Develop a Disaster Recovery Plan
Additional Security Analysis Tasks (cont.)

- Regularly review records of information system activity
- Implement reasonable steps to select service providers
- Test and monitor security controls following changes
- Obtain assessments from qualified independent third parties
Three Important Terms

1. **Reasonable diligence**: The business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

2. **Reasonable cause**: An act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect. (NEW)
Three Important Terms (cont.)

3. **Willful neglect:** Conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated. *145 CFR 160.401 Definitions* 18
Fines

• 1,000 records, $50,000 per violation = $50,000,000 per violation, capped at $1,500,000 for identical violations during a calendar year.
Security Management Process

What a Risk Analysis IS

• The process of identifying, prioritizing, and estimating risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, and other organizations resulting from the operation of an information system.

• Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.

• NIST SP800-30
What a Risk Analysis IS NOT

• A network vulnerability scan
• A penetration test
• A social engineering test
• A configuration audit
• A network diagram review
• Information system activity review
• SOC 2 or SOC 3 Report
ONC Guide to Privacy and Security of Electronic Health Information

- Risk Analysis is the process of identifying, prioritizing, and estimating risks... considers mitigations provided by security controls planned or in place
- NIST SP800-30
Establishing a Risk Value Think Likelihood
* Impact 52

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>25</td>
</tr>
<tr>
<td>High</td>
<td>15-24</td>
</tr>
<tr>
<td>Medium</td>
<td>8-14</td>
</tr>
<tr>
<td>Low</td>
<td>0-7</td>
</tr>
</tbody>
</table>
Results – If Done Properly

• Avoid security incidents and/or breaches

• Preparation for HITECH mandatory audits

• Preparation for OCR investigation

• Solid educational foundation

• Completion of 45 CFR 164.308(a)(1)(ii)(A) - Risk Analysis
Results – If Done Properly (cont.)

- Completion of foundational security program step
- Creation of sound basis for risk management decisions
- Development of remediation plan
- Risk analysis/remediation report
- Basis for ongoing risk management
Performing a Security Risk Analysis

• Define the scope of the risk analysis and collect data regarding the ePHI
• Identify potential threats and vulnerabilities to patient privacy and to the security of your practice’s ePHI
• Assess the effectiveness of implemented security measures in protecting against the identified threats and vulnerabilities
• Determine the likelihood that a particular threat will occur and the impact it would have to the ePHI
Performing a Security Risk Analysis, cont’d

• Determine and assign risk levels based on the likelihood and impact of a threat occurrence
• Prioritize the remediation or mitigation of identified risks based on the severity of their impact on your patients and practice
• Document your risk analysis including information from the steps you have taken as well as the risk analysis results
• Review and update your risk analysis on a periodic basis
Protecting Patients’ Electronic Health Information

• The SECURITY RULE requires that you put into place REASONABLE and APPROPRIATE:
  – Physical safeguards
  – Administrative safeguards
  – Technical safeguards
Physical Safeguards

- Your practice and other places where patient data is accessed
- Computer equipment
- Portable devices

Examples:
- Building alarm systems
- Locked offices
- Screens shielded from secondary viewers
Administrative Safeguards

• Designated security officer
• Workforce training and oversight
• Controlling information access
• Periodic security reassessment
• Examples:
  – Staff training
  – Monthly review of user activities
  – Policy enforcement
Technical Safeguards

• Controls access to EHR
• Use of audit logs to monitor users and other EHR activities
• Measures that keep electronic patient data from improper changes
• Secure authorized electronic exchanges of patient information
• Examples:
  – Secure passwords
  – Back up data
  – Virus checks
  – Data encryption
Policies and Procedures

• Written policies and procedures to ensure HIPAA security compliance
• Documentation of security measures
• Examples:
  – Written protocols on authorizing users
  – Record retention
Organizational Requirements

• Business Associate Agreements

• Examples:
  – Plan for identifying and managing vendors who access, create or store PHI
  – Documented agreements
  – Review and update
Demonstrate Good Faith Effort – Exercise Reasonable Diligence
The Security Management Process Standard

• Is one of the requirements in the HIPAA Security Rule
• Conducting a risk analysis is one of the requirements that provides instructions to implement the security management process
• ONC worked with OCR to create a tool to help guide health care providers from small practices through the risk assessment process
The Security Management Process Standard

• Use of this tool is not required by the HIPAA Security Rule but is meant to provide helpful assistance

• Security Risk Assessment (SRA) Tool:
The Security Risk Assessment Tool

**Security Risk Assessment Tool**

**What is the Security Risk Assessment Tool (SRA Tool)?**

The Office of the National Coordinator for Health Information Technology (ONC) recognizes that conducting a risk assessment can be a challenging task. That's why ONC, in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), developed a downloadable SRA Tool [exe - 91.3 MB] to help guide you through the process. This tool is not required by the HIPAA Security Rule, but is meant to assist providers and professionals as they perform a risk assessment.

The SRA Tool is a self-contained, operating system (OS) independent application that can be run on various environments including Windows OS's for desktop and laptop computers and Apple's iOS for iPad only. The iOS SRA Tool application for iPad, available at no cost, can be downloaded from Apple’s App Store.

The SRA Tool takes you through each HIPAA requirement by presenting a question about your organization's activities. Your “yes” or “no” answer will show you if you need to take corrective action for that particular item. There are a total of 156 questions.

**SRA Tutorial Video**

**Top 10 Myths of Security Risk Analysis**

As with any new program or regulation, there may be misinformation making the rounds.

Read the top 10 list distinguishing fact from fiction.

**SRA Tool (Windows version)**
Download the Security Risk Assessment Tool

The SRA Tool takes you through each HIPAA requirement by presenting a question about your organization’s activities. Your “yes” or “no” answer will show you if you need to take corrective action for that particular item. There are a total of 156 questions.

Resources are included with each question to help you:

- Understand the context of the question
- Consider the potential impacts to your PHI if the requirement is not met
- See the actual safeguard language of the HIPAA Security Rule

You can document your answers, comments, and risk remediation plans directly into the SRA Tool: The tool serves as your local repository for the information and does not send your data anywhere else.

Completing a risk assessment requires a time investment. At any time during the risk assessment process, you can pause to view your current results. The results are available in a color-coded graphic view (Windows version only) or in printable PDF and Excel formats.

For details on how to use the tool, download the SRA Tool User Guide [PDF - 4.5 MB].

A paper-based version of the tool is also available:

- Administrative Safeguards [DOCX - 397 KB]*
- Technical Safeguards [DOCX - 312 KB]*
- Physical Safeguards [DOCX - 263 KB]*

*Persons using assistive technology may not be able to fully access information in this file. For assistance, contact ONC at PrivacyAndSecurity@hhs.gov.
Download the SRA Tool User Guide
Security Risk Assessment Tutorial

Security Risk Assessment Tool

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC) recognizes that conducting a risk assessment can be a challenging task. That’s why ONC, in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), developed a downloadable SRA Tool [.exe - 91.3 MB] to help guide you through the process. This tool is not required by the HIPAA Security Rule, but is meant to assist providers and professionals as they perform a risk assessment.

The SRA Tool is a self-contained, operating system (OS) independent application that can be run on various environments including Windows OS’s for desktop and laptop computers and Apple’s iOS for iPad only. The iOS SRA Tool application for iPad, available at no cost, can be downloaded from Apple’s App Store.

The SRA Tool takes you through each HIPAA requirement by presenting a question about your organization’s activities. Your “yes” or “no” answer will show you if you need to take corrective action for that particular item. There are a total of 156 questions.

Top 10 Myths of Security Risk Analysis

As with any new program or regulation, there may be misinformation making the rounds.

Read the top 10 list distinguishing fact from fiction.
Select Security Risk Assessment

What Assessment would you like to work on?

- Import Assessment
- Create New
- Continue Current
Security Risk Assessment Tool Home Page

§164.308(a)(1)(i) - Standard

Does your practice develop, document, and implement policies and procedures for assessing and managing risk to its ePHI?

- Yes
- No
- Flag

An information system is an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and users.

A portable electronic device is any electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.
Your practice may not have adequate controls to safeguard ePHI if it does not develop and implement policies and procedures for assessing and managing risk to its ePHI.

Some potential impacts include:

- Unauthorized or inappropriate access to ePHI can compromise the confidentiality, integrity, and availability of your practice’s ePHI.
- Unauthorized disclosure, loss, or theft of ePHI can lead to medical identity theft.
- Accurate ePHI may not be available when needed, which can adversely impact your healthcare professionals’ ability to diagnose and treat their patients.
Examples of Safeguards

Implement policies and procedures to prevent, detect, contain, and correct security violations.
[45 CFR §164.308(a)(1)(i)]

Develop, document, and disseminate to workforce members a risk assessment policy that addresses its purpose, scope, roles, responsibilities, management commitment, the expected coordination among organizational entities, and compliance requirements. The policy should also outline procedures to facilitate its implementation and associated risk assessment controls.
[NIST SP 800–53 RA–1]
Security Risk Assessment Options

- Next Question
- Report
- Glossary
- Navigator
- Related Info
- Export
## Security Risk Assessment Summary

<table>
<thead>
<tr>
<th>ID</th>
<th>Citation</th>
<th>Answer</th>
<th>Flagged</th>
<th>Risk Level</th>
<th>Current Activities</th>
<th>Notes</th>
<th>Remediation</th>
<th>Reason</th>
<th>Last Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>A01</td>
<td>§164.308(a) (1)(i)</td>
<td>Yes</td>
<td></td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td></td>
<td>[A.]9/6/2016 3:21:02 pm</td>
</tr>
<tr>
<td>A02</td>
<td>§164.308(a) (1)(i)</td>
<td>Yes</td>
<td></td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td></td>
<td>[A.]1/13/2017 3:40:09 pm</td>
</tr>
<tr>
<td>A03</td>
<td>§164.308(a) (1)(ii)(A)</td>
<td>Yes</td>
<td></td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td></td>
<td>[A.]1/13/2017 3:43:19 pm</td>
</tr>
<tr>
<td>A04</td>
<td>§164.308(a) (1)(ii)(A)</td>
<td>Yes</td>
<td></td>
<td>Low</td>
<td>Once a year</td>
<td>N/A</td>
<td></td>
<td></td>
<td>[A.]9/6/2016 3:22:18 pm</td>
</tr>
<tr>
<td>A05</td>
<td>§164.308(a) (1)(ii)(B)</td>
<td>Yes</td>
<td></td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td></td>
<td>[A.]9/6/2016 3:22:30 pm</td>
</tr>
<tr>
<td>A07</td>
<td>§164.308(a) (1)(ii)(B)</td>
<td>Yes</td>
<td></td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td></td>
<td>[A.]9/6/2016 3:22:44 pm</td>
</tr>
<tr>
<td>A08</td>
<td>§164.308(a) (1)(ii)(B)</td>
<td>Yes</td>
<td></td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td></td>
<td>[A.]9/6/2016 3:23:06 pm</td>
</tr>
<tr>
<td>A14</td>
<td>§164.308(a) (2)</td>
<td>Yes</td>
<td></td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td></td>
<td>[A.]1/13/2017 3:40:44 pm</td>
</tr>
<tr>
<td>A22</td>
<td>§164.308(a)</td>
<td>Yes</td>
<td></td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td></td>
<td>[A.]1/13/2017</td>
</tr>
</tbody>
</table>
Security Risk Assessment Table View

![Security Risk Assessment Tool](image)

- Administrative: 0 (Low), 0 (Medium), 19 (High)
- Physical: 0 (Low), 0 (Medium), 16 (High)
- Technical: 0 (Low), 0 (Medium), 3 (High)
- Combined: 0 (Low), 0 (Medium), 38 (High)
## Security Risk Analysis Report

![Security Risk Analysis Report](image)

### Table: Security Risk Analysis

<table>
<thead>
<tr>
<th>ID</th>
<th>Citation</th>
<th>Answer</th>
<th>Risk Level</th>
<th>Current Activities</th>
<th>Notes</th>
<th>Remediation</th>
<th>Reason</th>
<th>Last Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>P001</td>
<td>§164.318(a)</td>
<td>Yes</td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td></td>
<td>3:41:21 pm</td>
</tr>
<tr>
<td>P002</td>
<td>§164.318(b)</td>
<td>Yes</td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td>[A]:1/13/2017</td>
<td>3:41:32 pm</td>
</tr>
<tr>
<td></td>
<td>(1)(i)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P003</td>
<td>§164.318(b)</td>
<td>Yes</td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td>[A]:1/13/2017</td>
<td>3:41:42 pm</td>
</tr>
<tr>
<td></td>
<td>(1)(ii)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P004</td>
<td>§164.318(b)</td>
<td>Yes</td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td>[A]:1/13/2017</td>
<td>3:41:53 pm</td>
</tr>
<tr>
<td></td>
<td>(2)(i)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P005</td>
<td>§164.318(b)</td>
<td>Yes</td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td>[A]:1/13/2017</td>
<td>3:42:06 pm</td>
</tr>
<tr>
<td></td>
<td>(2)(ii)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P006</td>
<td>§164.318(b)</td>
<td>Yes</td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td>[A]:1/13/2017</td>
<td>3:42:17 pm</td>
</tr>
<tr>
<td></td>
<td>(2)(iii)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T01</td>
<td>§164.312(a)</td>
<td>Yes</td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td>[A]:1/13/2017</td>
<td>3:55:27 pm</td>
</tr>
<tr>
<td></td>
<td>(1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T25</td>
<td>§164.312(b)</td>
<td>Yes</td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td>[A]:1/13/2017</td>
<td>3:42:59 pm</td>
</tr>
<tr>
<td>T37</td>
<td>§164.312(d)</td>
<td>Yes</td>
<td>Low</td>
<td></td>
<td>N/A</td>
<td></td>
<td>[A]:1/13/2017</td>
<td>3:43:08 pm</td>
</tr>
</tbody>
</table>

Showing 1 to 20 of 42 entries
START NOW! Don’t Wait

DO IT NOW!
Don’t Forget About the SRA
What Happens After Its Finished?
Asset Inventory List

• Remember:
  – Demonstrate good faith effort
  – Exercise reasonable diligence
Privacy and Security Tab in Header

Privacy and Security

Health Information Privacy, Security, and Your EHR
Health IT Privacy and Security Resources

The Office of the National Coordinator for Health Information Technology (ONC), U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), and other HHS agencies have developed a number of resources for you. These tools, guidance documents, and educational materials are intended to help you better integrate HIPAA and other federal health information privacy and security into your practice.

- **Tools and Templates**
  - **Guide to Privacy and Security of Electronic Health Information** [PDF - 1.3 MB]. ONC tool to help small health care practices in particular succeed in their privacy and security responsibilities. The Guide includes a sample seven-step approach for implementing a security management process.
  - **Security Risk Assessment (SRA) Tool**. HHS downloadable tool to help providers from small practices navigate the security risk analysis process.
  - **Security Risk Analysis Guidance** [PDF - 41 KB]. OCR’s expectations for how providers can meet the risk analysis requirements of the HIPAA Security Rule.
  - **HIPAA Security Toolkit Application**. National Institute of Standards and Technology (NIST) toolkit to help organizations better understand the requirements of the HIPAA Security Rule.
HealthIT.gov Links

• Health Information Privacy, Security, and Your EHR
  – https://www.healthit.gov/providers-professionals/ehr-privacy-security

• Information Security Policy Template
  – https://www.healthit.gov/providers-professionals/implementation-resources/information-security-policy-template

• Security Risk Assessment Tool
HealthIT.gov Links (cont.)

• Guide to Privacy and Security of Electronic Health Information

• Health Information Privacy, Security, and Your EHR
More Online Resources

- **Security Risk Analysis Tip Sheet**

- **Summary of the HIPAA Security Rule**

- **Healthcare Information and Management Systems Society**
  - [www.HIMSS.org](http://www.HIMSS.org)

- **National Cyber Security Alliance**
  - [www.staysafeonline.org](http://www.staysafeonline.org)
Quality Insights Can Help

- **Quality Insights QPP Support Center**
  - For practices with **15 or fewer** eligible providers
  - Email: qpp-support@qualityinsights.org
  - Phone: 877.497.5065
  - Website: www.qppsupport.org

- **Quality Insights Quality Innovation Network (QIN)**
  - For practices with **16 or more** eligible providers
  - Email: kwild@qualityinsights.org
  - Phone: 877.987.4687, Ext. 108
  - Website: www.qualityinsights-qin.org
Questions