Meaningful Use
Objective 1
Security Risk Analysis

Presented by: Alyshia Jones
with Myers and Stauffer LC

December 2018
What is a Security Risk Analysis?

• A security risk analysis (SRA) should be 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.
Why conduct a Security Risk Analysis?

• Prior to the implementation of the program, the provisions of the Proposed Rule were released for public comment. Commenters expressed concern over privacy and security risks imposed by the implementation and use of certified EHR technology.
Why conduct a Security Risk Analysis?

• CMS responded that they intend to mitigate the risks to the security and privacy of patient information by requiring eligible professionals (EPs), eligible hospitals (EHs), and CAHs to 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. CMS believes maintaining privacy and security is crucial for every EP, EH or CAH that uses certified EHR technology. The inclusion of the Protect Patient Health Information objective (security risk analysis) was recommended by the HIT Policy Committee for these reasons.
Protect Patient Health Information

Stage
Applies to Modified Stage 2 and Stage 3 definition.

Objective
Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.
Protect Patient Health Information

Measure
Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of ePHI created or maintained by CEHRT in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process.

Exclusion: None
Requirement Is Not New

- 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.
Suggested Tips

• Review the existing security infrastructure in your practice against legal requirements and industry best practices

• Identify potential threats to patient privacy and security and assesses the impact on the confidentiality, integrity and availability of your e-PHI

• Prioritize risks based on the severity of their impact on your patients and practice

• Determine if you need to perform a full assessment or review of the prior full assessment
Required Elements of a Security Risk Analysis
Required Elements

- A security risk analysis should contain a layered approach and be dated within the appropriate period. Although there is no specified method that guarantees compliance, there are several elements a risk analysis must incorporate, regardless of the method employed.*
  - Contain asset inventory (also referred to as scope of analysis and data collection in OCR guidance)
  - Contain physical, administrative, and technical safeguards to e-PHI
  - Identify threats and vulnerabilities
  - Determine the likelihood of threat occurrence
  - Determine the potential impact of threat occurrence
  - Determine the level of risk
  - Remediation/action plan

*Adapted from The Office of Civil Rights’ Guidance on Risk Analysis Requirements under the HIPAA Security Rule.
Timing of 2017 Security Risk Analysis

• The SRA must be completed on or after the end of the EHR reporting period & no later than December 31st and must show date completed.

• Example 1
  o A provider cannot use an SRA completed in May 2017 if the EHR reporting period is May 1, 2017 – July 30, 2017. The scope of the SRA must include the full EHR reporting period, which means it must be completed between July 30, 2017 but on or before December 31, 2017.

• Example 2
  o A provider whose EHR reporting period is October 2, 2017 – December 30, 2017 must complete the SRA on December 30, 2017 or December 31, 2017.

*45 CFR 164.306, 45 CFR 164.316(b)(2)(iii), CMS Program Year 2017 Objective 1 Tip Sheet
Periodic Reviews to SRA

- The risk analysis is an ongoing process after your full SRA is completed
- Meaningful use requires an SRA each calendar year for each EHR reporting period
- Providers must determine if a FULL assessment or REVIEW of the prior full assessment is needed

<table>
<thead>
<tr>
<th>Assessment</th>
<th>Report Results*</th>
<th>Monitor &amp; Review</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Perform Full Assessment</td>
<td>- Vulnerabilities</td>
<td>- Security incidents</td>
</tr>
<tr>
<td>or</td>
<td>- Threats</td>
<td>- Ownership change</td>
</tr>
<tr>
<td>- Review of Prior Full Assessment</td>
<td>- Risks</td>
<td>- Key staff turn over</td>
</tr>
<tr>
<td></td>
<td>*Document the results of your assessment.</td>
<td>- New technology</td>
</tr>
<tr>
<td></td>
<td>*Date when your assessment was completed MM/DD/YYYY.</td>
<td>- System upgrade</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Action plans</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Corrective actions</td>
</tr>
</tbody>
</table>

*45 CFR 164.306, 45 CFR 164.316(b)(2)(iii), CMS Program Year 2017 Objective 1 Tip Sheet

Reaching across Arizona to provide comprehensive quality health care for those in need
**Full vs Review Assessments**

**Perform Full Assessment**
- New technology
- System upgrade
- Any events under Review column *(to the right)*
- Anytime as determined by the practice

**Perform Review**
- Security incidents
- Ownership change
- Key staff turn over

*Prerequisites:* prior completion of full assessment
SRA Report Documentation

Full Assessment

- Practice Security Risk Report
- Vendor Security Risk Report
- SRA Tool Report from NIST [National Institute of Standards and Technology]

Review of Prior Full Assessment

- Emails documenting the security team’s review of the prior year’s SRA.
- Signed and dated memo documenting the date of review and review procedures.
- Meeting minutes showing the annual SRA review.
Asset Inventory

• A SRA should identify where all e-PHI is created, stored, received, maintained or transmitted. The asset inventory is used to determine the scope of the security risk analysis.

• Asset inventory can be in multiple formats. Examples include, but are not limited to:

Separate Listing

15 laptops
25 desk tops
5 smart phones
55 employees
Athena EHR

*Guidance issued by the Office of Civil Rights, 45 CFR 164.306(a), 45 CFR 164.308(a)(1)(ii)(A), and 45 CFR 164.316(b)(1)

ABC Practice employees 25 medical providers and two office personnel. These employees have access to ePHI via 5 desk top computers. Employees are not permitted to remove PHI from the practice. Mobile devices are not authorized to receive or transmit ePHI. All ePHI is stored, received, maintained or transmitted through our certified EHR technology, Athena.
Safeguarding ePHI

• According to the Centers for Medicare & Medicaid Services (CMS), the SRA should not review only the EHR system (technical aspect). The SRA should contain physical, administrative, and technical safeguards to e-PHI.

• **New Requirement as of Stage 2 in 2014**: The SRA is required to address the security and encryption of their ePHI in accordance with 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3).

• Examples include, but are not limited to:

<table>
<thead>
<tr>
<th>Physical Safeguards</th>
<th>Administrative Safeguards</th>
<th>Technical Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Building alarm systems</td>
<td>• Staff training</td>
<td>• Secure passwords</td>
</tr>
<tr>
<td>• Locked offices</td>
<td>• Monthly review of user activities</td>
<td>• Backing-up data</td>
</tr>
<tr>
<td>• Screens shielded from secondary viewers</td>
<td>• Policy enforcement</td>
<td>• Virus checks</td>
</tr>
</tbody>
</table>

*45 CFR 164.308, 45 CFR 164.310, 45 CFR 164.312, 45 CFR 164.312 (a)(2)(iv), and 45 CFR 164.306(d)(3).*
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.

**Sample Threat**

<table>
<thead>
<tr>
<th>Physical</th>
<th>Natural Disaster</th>
<th>What security measures are in place in the event of a natural disaster?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative</td>
<td>Disgruntled Former Employee poses a threat to e-PHI</td>
<td>Is there a protocol in place to report a breach of e-PHI?</td>
</tr>
<tr>
<td>Technical</td>
<td>Security Breach to EHR System</td>
<td>Is there a protocol in place to prevent a breach of e-PHI?</td>
</tr>
</tbody>
</table>

- Data is backed up to an offsite server daily in the event of a natural disaster that destroys the main server room.
- Breaches of e-PHI will be reported in accordance with the practice’s security management policy.
- Firewalls are in place to protect against breaches of security.

* Guidance issued by the Office of Civil Rights, 45 CFR 164.308, 45 CFR 164.310, and 45 CFR 164.312
Threats and Vulnerabilities

- Organizations must:
  - Identify and document reasonably anticipated threats to e-PHI.
  - Identify different threats that are unique to the circumstances of their environment.
  - 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.
- Examples of threats and vulnerabilities include, but are not limited to the following:
  - Natural Disaster (tornado does damage to server room)
  - Security Breach to EHR system (theft of a laptop containing e-PHI)
  - Disgruntled former employee (leaks patient files)
- The threats and vulnerabilities identified may vary significantly based on the size, type, and complexity of the practice.

*Guidance issued by the Office of Civil Rights, 45 CFR 164.308(a)(1)(ii)(A), and 45 CFR 164.316(b)(1)(ii)*
Risks

- The Security Rule requires organizations to take into account the probability of potential risks to e-PHI. 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.”

- Practices could assign a likelihood to each of the identified threats/vulnerabilities. For this example we will use a number scale 1-5, 5 being very likely.

<table>
<thead>
<tr>
<th>Threat Category</th>
<th>Threat Event</th>
<th>Likelihood Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural Disaster</td>
<td>Tornado does damage to server room</td>
<td>1</td>
</tr>
<tr>
<td>Security Breach to EHR</td>
<td>Theft of a laptop containing e-PHI</td>
<td>3</td>
</tr>
<tr>
<td>Disgruntled Employee(s)</td>
<td>Employee leaks patient files</td>
<td>3</td>
</tr>
</tbody>
</table>

* Guidance issued by the Office of Civil Rights and 45 CFR 164.306
Impact of Risks

- The Rule also requires consideration of the “criticality,” or impact, of potential risks to confidentiality, integrity, and availability of e-PHI.
- 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.
- For this example we will use a quantitative method. Impact has been assessed with a number scale 1-5, 5 being critical.

<table>
<thead>
<tr>
<th>Threat Category</th>
<th>Threat Event</th>
<th>Impact Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural Disaster</td>
<td>Tornado does damage to server room</td>
<td>5</td>
</tr>
<tr>
<td>Security Breach to EHR</td>
<td>Theft of a laptop containing e-PHI</td>
<td>3</td>
</tr>
<tr>
<td>Disgruntled Employee(s)</td>
<td>Employee leaks patient files</td>
<td>4</td>
</tr>
</tbody>
</table>

* Guidance issued by the Office of Civil Rights and 45 CFR 164.306
**Level of Risks**

- 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.
- For example, the risk level determination might be performed by calculating the average of the assigned likelihood and impact levels.

<table>
<thead>
<tr>
<th>Threat Category</th>
<th>Threat Event</th>
<th>Likelihood Score</th>
<th>Impact Score</th>
<th>Risk Level (Average of Likelihood and Impact)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural Disaster</td>
<td>Tornado does damage to server room</td>
<td>1</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Security Breach to EHR</td>
<td>Theft of a laptop containing ePHI</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Disgruntled Employee(s)</td>
<td>Employee leaks patient files</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

* Guidance issued by the Office of Civil Rights and 45 CFR 164.306(a)(2), 164.308(a)(1)(ii)(A), 164.316(b)(1)
Final Risk Report

• The Security Rule requires the risk analysis to be **documented** but does not require a specific format. Regardless of the format chosen, the previously discussed elements should be well documented in the final report regardless of the type of assessment performed.

• Identify the **look back period the SRA covers**

• Make sure **completion date** of the review **has a specific date (MM/DD/YYYY)**.

* Guidance issued by the Office of Civil Rights and 45 CFR 164.316(b)*
## Action Plan

- The SRA should include a list of corrective actions to be performed to mitigate each risk level.
- All deficiencies do not have to be mitigated prior to attestation. The EHR incentive program requires correcting any deficiencies according to the timeline established in the provider’s risk management process.

<table>
<thead>
<tr>
<th>Threat Category</th>
<th>Threat Event</th>
<th>Likelihood Score</th>
<th>Impact Score</th>
<th>Risk Level</th>
<th>Action Plan/Remediation Steps</th>
<th>Estimated Completion Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural Disaster</td>
<td>Tornado does damage to server room</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>Implement disaster recovery plan</td>
<td>December 2017</td>
</tr>
<tr>
<td>Security Breach to EHR</td>
<td>Theft of a laptop containing ePHI</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>Encrypt all laptops</td>
<td>Action in place</td>
</tr>
<tr>
<td>Disgruntled Employee(s)</td>
<td>Employee leaks patient files</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>Revoke access to systems for terminated employees</td>
<td>Action ongoing</td>
</tr>
</tbody>
</table>

* Guidance issued by the Office of Civil Rights, 45 CFR 164.316(b), and FAQ7705
Audit Findings

24 Reaching across Arizona to provide comprehensive quality health care for those in need
What Happens During an Audit?

• All providers that receive a Medicaid EHR incentive payment could potentially be selected by AHCCCS for post payment audit.

• If selected, AHCCCS post payment analysts will conduct a thorough review of the documentation attached to your attestation in ePIP to determine if it meets the MU requirements.

• AHCCCS may have follow-up questions or make additional documentation requests.
Common SRA Audit Findings

- Failure to complete and/or update the SRA within the appropriate time period for the program year.
- Failure to maintain documentation.
- Failure to sufficiently document all required elements of the SRA.
Resources

Reaching across Arizona to provide comprehensive quality health care for those in need
Resources

• HIPAA Security Rule
• Guidance from Office for Civil Rights (OCR)
• CMS SRA Tip Sheet
• CMS Objective 1 Tip Sheet
• National Institute of Standards and Technology (NIST) SRA Template
• The Office of the National Coordinator (ONC) (Pages 41-53)
• Federal Final Rule

Please note that the information in the presentation should be used solely as a tool to gain a better understanding of the security risk analysis requirements. It is the provider’s responsibility to complete, review, or update a compliant security risk analysis for each program year’s attestation.
Questions?

Reaching across Arizona to provide comprehensive quality health care for those in need
Thank You

Reaching across Arizona to provide comprehensive quality health care for those in need