Security Risk Analysis for Meaningful Use

Presented by: Priscilla Clark with Myers and Stauffer LC

July 2020

AHCCCS
Arizona Health Care Cost Containment System

Security Risk Analysis Objective

- Learn the required elements of a security risk analysis (SRA).
- Learn when to complete your annual security risk analysis to qualify for the PI program.
- Learn what resources are available to help you complete your SRA.

What is a Security Risk Analysis?

- A 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 (CEHRT).

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 Critical Access Hospitals (CAHs) to conduct or review a SRA 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 a CEHRT.
- The inclusion of the Protect Patient Health Information objective (security risk analysis) was recommended by the HIT Policy Committee for these reasons.

Requirement Is Not New

- Requirement originated in Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule, §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.
- Since the inception of the Medicaid Promoting Interoperability (PI) program, meaningful use providers have been required to conduct or review their risk analysis each program year to receive an incentive payment.

Security Risk Analysis

- **Objective**: Protect electronic protected health information (e-PHI) created or maintained by the CEHRT through the implementation of appropriate technical, administrative, and physical safeguards.
- **Measure**: Conduct or review a SRA in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the security (including encryption) of data created or maintained by CEHRT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), implement security updates as necessary, and correct identified security deficiencies as part of the provider's risk management process.
- **Exclusion**: None

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 SRA should contain a layered approach and be completed 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 Office of Civil Rights (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 2020 Security Risk Analysis

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

Program Year	PI Reporting Period	When do I complete the Annual SRA?^
2020	01.01.2020 – 03.31.2020	03.31.2020 – 12.31.2020
2020	10.01.2020 – 12.29.2020	12.29.2020 – 12.31.2020
2020	06.01.2020 – 08.29.2020	08.29.2020 – 12.31.2020
2020	10.03.2020 – 12.31.2020	12.31.2020

^The SRA report must include the completion date.

*45 CFR 164.306, 45 CFR 164.316(b)(2)(iii), CMS Program Year 2020 Objective 1 Tip Sheet

Periodic Reviews to Security Risk Analysis

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

Assessment

- Perform Full Assessment

or

- Review of Prior Full Assessment

Report Results*

- Vulnerabilities
- Threats
- Risks

Document the results of your assessment.

Date when your assessment was completed *MM/DD/YYYY*.

Monitor & Review

- Security incidents
- Ownership change
- Key staff turn over
- New technology
- System upgrade
- Action plans
- Corrective actions

*45 CFR 164.306, 45 CFR 164.316(b)(2)(iii), CMS Program Year 2020 Objective 1 Tip Sheet

Full Versus Review Assessments

Perform Full Assessment

- New technology
- System upgrade (i.e. upgrading to 2015 CEHRT)
- 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 is required

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. The email must demonstrate that no updates were necessary. If updates were necessary, the updated SRA should be submitted.
- 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 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

Paragraph format within Final Report

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

*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)

Safeguarding e-PHI

- 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 e-PHI in accordance with 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3).
- Examples include, but are not limited to:

Physical Safeguards

- Building alarm systems
- Locked offices
- Screens shielded from secondary viewers

Administrative Safeguards

- Staff training
- Monthly review of user activities
- Policy enforcement

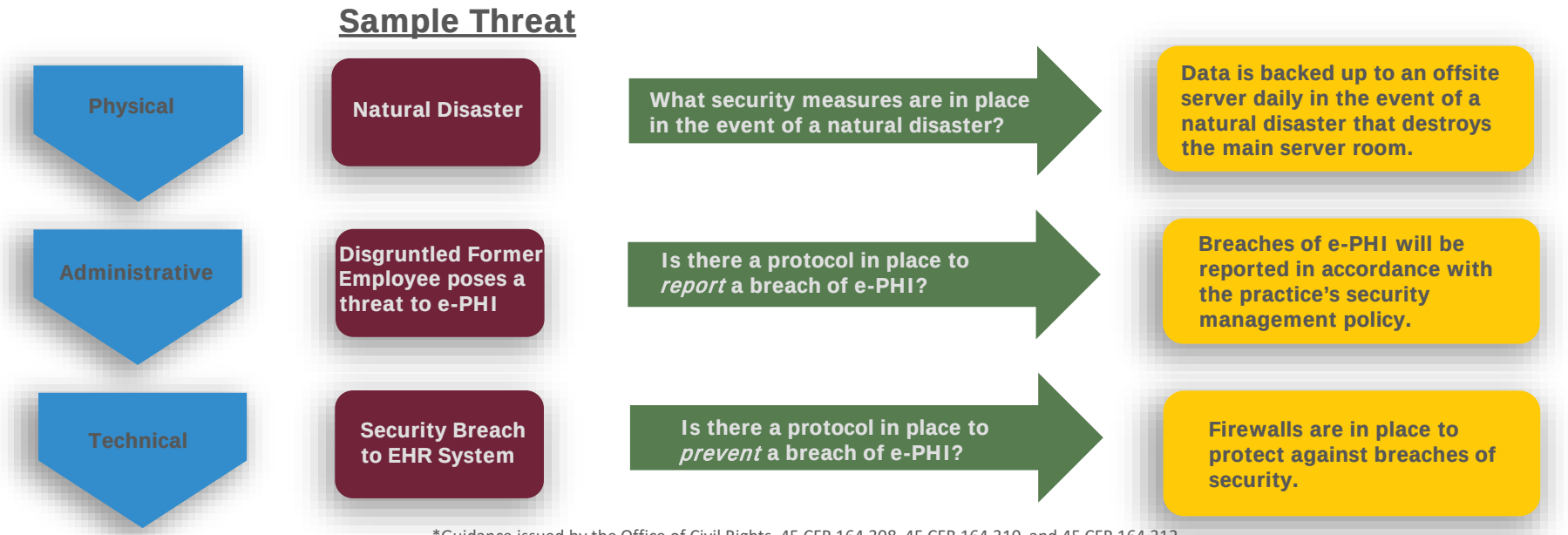
Technical Safeguards

- Secure passwords
- Backing-up data
- Virus checks
- Data encryption

*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.



*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).

Likelihood of 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.

Threat Category	Threat Event	Likelihood Score
Natural Disaster	Tornado does damage to server room	1
Security Breach to EHR	Theft of a laptop containing e-PHI	3
Disgruntled Employee(s)	Employee leaks patient files	3

* 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.

Threat Category	Threat Event	Impact Score
Natural Disaster	Tornado does damage to server room	5
Security Breach to EHR	Theft of a laptop containing e-PHI	3
Disgruntled Employee(s)	Employee leaks patient files	4

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

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

*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).

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 PI incentive program requires correcting any deficiencies according to the timeline established in the provider's risk management process.

Threat Category	Threat Event	Likelihood Score	Impact Score	Risk Level	Action Plan/ Remediation Steps	Estimated Completion Date
Natural Disaster	Tornado does damage to server room	1	5	3	Implement disaster recovery plan	December 2020
Security Breach to EHR	Theft of a laptop containing ePHI	3	3	3	Encrypt all laptops	Action in place
Disgruntled Employee(s)	Employee leaks patient files	3	4	4	Revoke access to systems for terminated employees	Action ongoing

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

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).



Audit Findings

What Happens During an Audit?

- All providers that receive a Medicaid PI 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 the EP's attestation in ePIP to determine if it meets the program requirements.
- AHCCCS may have follow-up questions or make additional documentation requests.

Common 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*

- CMS Objective 1 Tip Sheet
- HIPAA Security Rule
- Guidance from Office for Civil Rights (OCR)
- CMS SRA Tip Sheet
- National Institute of Standards and Technology (NIST) SRA Instructions and Template
- The Office of the National Coordinator (ONC) SRA Template Instructions
- The Office of the National Coordinator (ONC) SRA Template
- The Office of the National Coordinator (ONC) (Pages 41-53)
- Federal Final Rule - Modified Stage 2 and Stage 3
- Security Risk Analysis Frequently Asked Questions**
- Tips for Creating a Security Risk Analysis**

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

**To access the AHCCCS Security Risk Analysis Frequently Asked Questions and Tips for Creating a Security Risk Analysis click on the links above, then click the drop down arrow labeled "Educational Resources". The FAQ and Tips link is included under the "Tip Sheets" header.

Questions?

Thank You.