Tips for Eligible Professionals Completing a Security Risk Analysis (SRA)

What is a security risk analysis (SRA)?

The security risk analysis (SRA) relates to objective 1 – Protect Patient Health Information. The objective of the measure is to ensure providers and practices are protecting electronic patient health information (ePHI) created or maintained by the CEHRT through the implementation of appropriate technical capabilities.

How to conduct a SRA?

The SRA should be conducted or reviewed 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 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 EP's risk management process.

What components should the SRA include?

The SRA should be conducted, reviewed, or updated between January 1 of the program year and the date of attestation. The SRA should include the following components at a minimum:

- Physical, administrative and technical safeguards tailored to the size and complexity of the practice.
- An asset inventory that identifies where **all ePHI is stored, received, maintained or transmitted. (not limited to CEHRT)**
- Identification of all potential threats and vulnerabilities to ePHI.
- Assessment of all current security measures.
- Assessment of the likelihood of all threat occurrences identified by the practice.
- Assessment of the potential impact of all treat occurrences identified by the practice.
- Assessment of the level of risk determined by analyzing the likelihood and impact of threat occurrence.
- Documented as being completed, reviewed or updated by the practice during the appropriate time frame
- An action plan (also referred to as mitigation and remediation plan) for addressing the identified threats to ePHI.

What are the best practices for SRA?

- Ensure the completed SRA is retained for a minimum of six years from the date of attestation.
- Ensure the SRA is for the correct period. If it was reviewed and no updates were made, retain documentation to show the date it was reviewed.
- If a third party completes the SRA, ensure it is tailored specifically to your practice.
- Ensure the SRA encompasses all aspects of the practice. Anything that handles ePHI should be included in the scope of the SRA.
- The SRA can be completed using several different methods. Ensure the format used includes all of the components listed above.

What are the most common mistakes found in the SRA?

- Not completing an SRA.
- Not retaining the SRA for the correct time period.
- SRA does not assess the risk level of the threats and vulnerabilities identified.
- SRA does not include an action plan addressing how the identified threats and vulnerabilities will be mitigated.
- SRA does not include an asset inventory.
- SRA only was completed based on the capabilities of the CEHRT and does not incorporate assets outside of the CEHRT which handle ePHI.

For more guidance on the security risk analysis, please refer to CMS or the Office of Civil Rights (OCR). CMS has published tip sheets, FAQs and a common myths and facts reference for providers and practices. OCR is responsible for issuing annual guidance on the provisions in the HIPAA Security Rule.

See the tip sheet provided by CMS located at: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/2016_SecurityRiskAnalysis.pdf

See SRA guidance provided by OCR located at:
http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf