Protect Patient Health Information:
Security Risk Analysis Requirements Tip Sheet
Program Year 2018

The following information has been compiled from the Centers for Medicare & Medicaid Services (CMS) and the Office for Civil Rights (OCR) to provide guidance to eligible professionals (EPs) and eligible hospitals (EHs) regarding the meaningful use (MU) objective **Protect Patient Health Information**.

In order to be deemed a meaningful user of certified EHR technology (CEHRT) and receive an EHR incentive payment, providers must attest to having met the objective Protect Patient Health Information. To meet this objective, EPs and EHs must conduct or review a **security risk analysis** (SRA) 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 the 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.

There are numerous methods of performing risk analysis and there is no single method or "best practice" that guarantees compliance. Although there is no specified method that guarantees compliance, there are several elements a risk analysis must incorporate, regardless of the method employed.

Requirement	Explanation	Regulation Reference 45 C.F.R §§	Source
Time Period	The SRA must be completed **on or after the end of the EHR reporting period** so the analysis covers the full reporting period and must be conducted within the 2017 calendar year.	164.306, 164.316(b)(2)(iii)	CMS Objective 1 Tip Sheet
Scope	The analysis should include all e-PHI that an organization creates, receives, maintains, or transmits. (45 C.F.R. § 164.306(a).)	164.306(a), 164.308(a)(1)(ii)(A), 164.316(b)(1)	OCR Guidance
Safeguards	Organizations should assess and document the security measures an entity uses to safeguard e-PHI. The Security Rule requires that you put into place reasonable and appropriate administrative, physical and technical safeguards to protect your patients' ePHI. The Security Rule allows you to tailor security policies, procedures, and technologies for safeguarding ePHI based on your medical practice's size, complexity, and capabilities—as well as its technical, hardware, and software infrastructure.	164.308 164.310 164.312	CMS SRA Tip Sheet

Requirement	Explanation	Regulation Reference 45 C.F.R §§	Source
Encryption	Assess whether implementing a mechanism to encrypt and decrypt ePHI is a reasonable and appropriate safeguard in its environment. If reasonable, implement the mechanism. If not reasonable, document why it is not reasonable and implement an equivalent alternative measure.	164.312(a)(2)(iv), 164.306(d)(3)	CMS Objective 1 Tip Sheet
Threats/ Vulnerabilities	Organizations must identify and document reasonably anticipated threats to e-PHI. Organizations may identify different threats that are unique to the circumstances of their environment. 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.	164.308(a)(1)(ii)(A), 164.316(b)(1)(ii)	OCR Guidance
Level of risk	Organizations should assign risk levels for all threat and vulnerability combinations identified during the risk analysis based on the likelihood and impact of threat occurrence.	164.306(a)(2), 164.308(a)(1)(ii)(A), 164.316(b)(1)	OCR Guidance
Final report	The Security Rule requires the risk analysis to be documented but does not require a specific format.	164.316(b)	OCR Guidance
Action plan	The SRA should include a list of corrective actions to be performed to mitigate each risk level. Any security updates and deficiencies that are identified in the review should be included in the provider's risk management process and implemented or corrected as dictated by that process.	164.316(b)	CMS SRA Tip Sheet
	All deficiencies do not have to be mitigated prior to attestation. The EHR incentive program requires correcting any deficiencies (identified during the risk analysis) according to the timeline established in the provider's risk management process, not the date the provider chooses to submit meaningful use attestation. The timeline needs to meet the requirements under 45 CFR 164.308(a)(1), including the requirement to "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [45 CFR]§164.306(a)."	164.316(b)	CMS SRA Tip Sheet