MEDICAID PROMOTING INTEROPERABILITY (PI) PROGRAM ELIGIBLE PROFESSIONALS OBJECTIVES AND MEASURES FOR 2020 AND 2021
OBJECTIVE 1 of 8

Protect Patient Health Information	
Objective	Protect electronic protected health information (ePHI) created or maintained by certified electronic health record technology (CEHRT) through the implementation of appropriate technical, administrative, and physical safeguards.
Measure	**Measure 1:** Conduct or review a security risk analysis 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.

Table of Contents

Attestation Requirements

Measure 1

Eligible professionals (EPs) must attest YES to conducting or reviewing a security risk analysis and implementing security updates as necessary and correcting identified security deficiencies to meet this measure.

Additional Information

- EPs must use 2015 Edition CEHRT to meet Stage 3 meaningful use.
- EPs must conduct or review a security risk analysis of CEHRT, including addressing encryption/security of data, implement updates as necessary at least once each calendar year, and attest to conducting the analysis or review.

- It is acceptable for the security risk analysis to be conducted outside the EHR reporting period; however, the analysis must be unique for each EHR reporting period, the scope must include the full EHR reporting period, and it must be conducted within the calendar year of the EHR reporting period.
- State Medicaid Agencies have the flexibility to require EPs to submit evidence that the security risk analysis has been completed after the incentive payment has been issued in program year 2021.
- An analysis must be done upon installation or upgrade to a new system and a review must be conducted covering each EHR reporting period. Any security updates and deficiencies that are identified should be included in the EP's risk management process and implemented or corrected as dictated by that process.
- The security risk analysis requirement under 45 CFR 164.308(a)(1) must assess the potential risks and vulnerabilities to the confidentiality, availability, and integrity of all ePHI that an organization creates, receives, maintains, or transmits. This includes ePHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media.
- At minimum, EPs should be able to show a plan for correcting or mitigating deficiencies and that steps are being taken to implement that plan.
- The parameters of the security risk analysis are defined 45 CFR 164.308(a)(1), which was created by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule. The PI Program does not impose new or expanded requirements on the HIPAA Security Rule nor does it require specific use of every certification and standard that is included in certification of EHR technology. More information on the HIPAA Security Rule can be found at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/.
- HHS Office for Civil Rights (OCR) has issued guidance on conducting a security risk analysis in accordance with the HIPAA Security Rule: http://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.
- The Office of the National Coordinator for Health Information Technology (ONC) and OCR developed a free Security Risk Assessment (SRA) Tool to assist EPs: http://www.healthit.gov/providers-professionals/security-risk-assessment-tool.

Regulatory References

This objective may be found at 42 C.F.R. § 495.24 (d)(1)(i)(A) and (B). For further discussion please see 80 FR 62851.

Certification Standards and Criteria

Below is the corresponding certification and standards criteria for EHR technology that supports achieving the meaningful use of this objective.

Certification Criteria
Information about certification for 2015 Edition CEHRT can be found at: https://www.healthit.gov/sites/default/files/2015edition_pstable_ml_11-4-15.pdf.

Standards Criteria
Standards for 2015 Edition CEHRT can be found at the ONC's 2015 Standards Hub: https://www.healthit.gov/topic/certification/2015-standards-hub.