Merit-Based Incentive Payment System (MIPS) Promoting Interoperability Performance Category Measure 2020 Performance Period

Objective:	Protect Patient Health Information
Measure:	**Security Risk Analysis** Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI data created or maintained by certified electronic health record technology (CEHRT) in accordance with requirements in 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 MIPS eligible clinician's risk management process.
Measure ID:	PI_PPHI_1

Definition of Terms

N/A

Reporting Requirements

YES/NO

To meet this measure, MIPS eligible clinicians must attest YES to conducting or reviewing a security risk analysis and implementing security updates as necessary and correcting identified security deficiencies.

Scoring Information

- Required for Promoting Interoperability Performance Category Score: **Yes**
- Score: **N/A**
- Eligible for Bonus Score: **No**

Note: In order to earn a score greater than zero for the Promoting Interoperability performance category, MIPS eligible clinicians must:

- Submit a "yes" to the Prevention of Information Blocking Attestations; and

- Submit a "yes" to the ONC Direct Review Attestation, if applicable; and

- Submit a "yes" that they have completed the Security Risk Analysis measure during the calendar year in which the MIPS performance period occurs; and

- Report the required measures from each of the four objectives.

Additional Information

- MIPS eligible clinicians must use 2015 Edition CEHRT. The 2015 Edition functionality must be in place by the first day of the performance period and the product must be certified to the 2015 Edition criteria by the last day of the performance period. The MIPS eligible clinicians must be using the 2015 Edition functionality for the full performance period. In many situations, the product may be deployed, but pending certification.
- Failure to complete the required actions for the Security Risk Analysis will result in no score for the Promoting Interoperability performance category, regardless of whether other measures in this category are reported.
- The Security Risk Analysis measure is not scored and does not contribute any points to the MIPS eligible clinician's total score.
- More information about Promoting Interoperability performance category scoring is available on the QPP website.
- It is acceptable for the security risk analysis to be conducted or reviewed outside the performance period; however, the analysis must be unique for each performance period, the scope must include the full MIPS performance period, and it must be conducted within the calendar year of the MIPS performance period (January 1st – December 31st).
- An analysis must be conducted when 2015 Edition CEHRT is implemented.
- An analysis must be done upon installation or upgrade to a new system and a review must be conducted covering each MIPS performance period. Any security updates and deficiencies that are identified should be included in the clinician'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 a minimum, MIPS eligible clinicians 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 at 45 CFR 164.308(a)(1), which was created by the HIPAA Security Rule. MIPS 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 Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule: https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.
- Additional free tools and resources available to assist providers include a Security Risk Assessment (SRA) Tool developed by ONC and OCR: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.

Regulatory References

- For further discussion, please see the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) final rule: 81 FR 77227.
- For additional discussion, please see the 2018 Physician Fee Schedule final rule – Quality Payment Program final rule: 83 FR 59790.
- A security risk analysis should include review of the appropriate implementation of the capabilities and standards specific to each certification criterion.

Certification Criteria and Standards

Below are the corresponding certification criteria and standards for electronic health record technology that support this measure.

Certification Criteria
The requirements are a part of CEHRT specific to each certification criterion.

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