Quality Payment PROGRAM

Merit-Based Incentive Payment System (MIPS) Promoting Interoperability Performance Category Measure 2025 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:

- Complete the Security Risk Analysis measure
- Complete the High Priority Practices SAFER Guide measure
- Complete the ONC Direct Review attestation
- Attest to the "Actions to limit or restrict compatibility or interoperability of CEHRT" statement
- Submit their complete numerator and denominator or Yes/No data for all required measures
- Submit their CMS certification identification number
- Submit their level of active engagement for the Public Health and Clinical Data Exchange measures
- Failure to report at least a "1" in all required measures with a numerator or reporting a "No" for a Yes/No response measure will result in a total score of 0 points for the Promoting Interoperability performance category
- Submit data for a minimum of 180 consecutive days within the calendar year

Additional Information

- MIPS eligible clinicians must use technology certified to ONC Certification Criteria for Health IT necessary to meet the CEHRT definition (88 FR 79307).
- To check whether a health IT product has been certified to ONC Certification Criteria for Health IT, visit the Certified Health IT Product List (CHPL) at https://chpl.healthit.gov/.
- Certified functionality must be used as needed for a measure action to count in the numerator during a performance period. However, in some situations the product may be deployed during the performance period but pending certification. In such cases, the product must be certified by the last day of the performance period.
- 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.
- 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 performance period, and it must be conducted within the calendar year of the performance period (January 1st – December 31st).
- An analysis must be done upon installation or upgrade to a new system and a review must be conducted covering each 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 clinicians 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: 83 FR 59790.
- The requirements are a part of CEHRT specific to each certification criterion.

Certification Criteria

Below are the corresponding certification criteria for health IT that support this measure.

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