Quality Payment
PROGRAM

Merit-Based Incentive Payment System (MIPS)
Promoting Interoperability Performance Category Measure
2026 Performance Period

Objective:	**Protect Patient Health Information** Protect electronic protected health information (ePHI) created or maintained by the certified electronic health record (EHR) technology (CEHRT) through the implementation of appropriate technical, administrative, and physical safeguards.
Measure:	**Security Risk Analysis** First, conduct or review a security risk analysis; and second, conduct security risk management activities, in accordance with the requirements under 45 CFR 164.308(a)(1)(ii)(A) and (B). Security risk analysis and management activities include addressing the security of data created or maintained by CEHRT (to include encryption), in accordance with 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3). The encryption implementation specified at 45 CFR 164.312(a)(2)(iv) must be implemented if it is reasonable and appropriate; if encryption isn't reasonable and appropriate, then the MIPS eligible clinician would adopt an equivalent alternative measure if it is reasonable and appropriate to do so.
Measure ID:	**PI_PPHI_1**

Definition of Terms

N/A

Reporting Requirements

"Yes"/"No" Response

The MIPS eligible clinician must attest "Yes" to the following statements:

- I conducted or reviewed a security risk analysis as required under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.308(a)(1)(ii)(A) during the year in which the performance period occurs.

- I conducted security risk management activities as required under the HIPAA Security Rule at 45 CFR 164.308(a)(1)(ii)(B), specifically the implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 45 CFR 164.306.

Scoring Information

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

NOTE: A MIPS eligible clinician must use technology certified to the Office of the National Coordinator for Health Information Technology (ONC) Certification Criteria for Health Information Technology (IT) (45 CFR 170.315) necessary to meet the CEHRT definition (42 CFR 414.1305(2)), and meet the following requirements to earn a score greater than zero for the MIPS Promoting Interoperability performance category:

- Provide their CMS EHR Certification ID from the Certified Health IT Product List (CHPL);
- Submit data for a minimum of 180 consecutive days within the calendar year;
- Submit a "Yes" attestation for the High Priority Practices Safety Assurance Factors for EHR Resilience (SAFER) Guide measure confirming the completion of an annual self-assessment using the 2025 High Priority Practices SAFER Guide during the calendar year in which the performance period occurs;
- Submit a "Yes" response for ONC Direct Review attestation;
- Submit a "Yes" response for the Actions to Limit or Restrict Compatibility or Interoperability of CEHRT attestation;
- Submit their complete count of numerators (report at least a "1" for all required measures with a numerator) and denominators or "Yes" response (for attestation measures) for all required measures (or claim an exclusion, if available and applicable); and
- Submit their level of active engagement for the required measures under the Public Health and Clinical Data Exchange objective.

Also, as an optional attestation, a MIPS eligible clinician can attest (if they received a request for surveillance) to work in good faith with an ONC-Authorized Certification Bodies (ACB) that conducts surveillance of their health IT certified under the ONC Health IT Certification Program.

Additional Information

- 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).
- Certified functionality must be used as needed for a measure action to count 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 conduct 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 isn't scored and doesn't contribute any points to the MIPS eligible clinician's, group's, virtual group's or Alternative Payment Model (APM) Entity'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 MIPS eligible clinician's risk management process and implemented or corrected as dictated by that process.

- The security risk analysis should be completed for each CEHRT the MIPS eligible clinician, group, virtual group or APM Entity is using to report the MIPS Promoting Interoperability performance category measures.
- 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.
- The HIPAA Security Rule implementation specification for risk management requires the implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 45 CFR 164.306(a).
- 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 doesn't 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.
- The United States Department of Health and Human Services (HHS) Office for Civil Rights (OCR) has issued guidance on conducting a security risk analysis in accordance with the HIPAA Security Rule.
- MIPS eligible clinicians, groups, and virtual groups may use the free Security Risk Assessment (SRA) Tool developed by ONC and OCR to assist them with this measure.
- APM Entities can choose to report MIPS Promoting Interoperability performance category data at the individual, group, virtual group, or APM Entity level when participating in MIPS. Review the Frequently Asked Questions on the Shared Savings Program Requirement to Report Objectives and Measures for the MIPS Promoting Interoperability Performance Category (PDF, 271KB) for more information.

Regulatory References

- The most recent regulatory references can be found in the Calendar Year (CY) 2026 Physician Fee Schedule final rule (90 FR 49874).
- There is no health IT certification criteria.

Version History Table

Date	Change Description
12/15/2025	Original posting.