Quality Payment Program

Merit-Based Incentive Payment System (MIPS) Advancing Care Information Performance Category Security Risk Analysis Measure Specifications

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 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.

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

BASE SCORE/PERFORMANCE SCORE/BONUS SCORE

- Required for Base Score (50%): **Yes**
- Percentage of Performance Score (up to 90%): **N/A**
- Eligible for bonus score: **No**

Note: MIPS eligible clinicians must earn the full base score in order to earn any score in the Advancing Care Information performance category. In addition to the base score, MIPS eligible clinicians have the opportunity to earn additional credit through a performance score and the bonus score.

Additional Information

- MIPS eligible clinicians can report the Advancing Care Information measures if they have technology certified to the 2015 Edition, or a combination of technologies from the 2014 and 2015 Editions that support these measures.
- This measure contributes to the base score for the Advancing Care Information performance category. MIPS eligible clinicians must submit a “yes” for the security risk analysis measure to receive credit toward the base score. More information about Advancing Care Information scoring is available on the QPP website.
- MIPS eligible clinicians must conduct or review a security risk analysis including addressing encryption/security of data created or maintained by CEHRT, and implement updates as necessary at least once each calendar year and attest to conducting the analysis or review.
- A MIPS eligible clinician must meet this measure to earn any score within the Advancing Care Information performance category. Failure to do so will result in a base score of zero as well as a performance score of zero and an Advancing Care Information performance category score of zero.
- It is acceptable for the security risk analysis to be conducted outside the MIPS performance period; however, the analysis must be unique for each MIPS 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 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 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 45 CFR 164.308(a)(1), which is part of the HIPAA Security Rule. The measure does not impose new or expanded requirements in addition to 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: http://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.
- Additional free tools and resources available to assist MIPS eligible clinicians include a Security Risk Assessment (SRA) Tool developed by ONC and OCR: http://www.healthit.gov/providers-professionals/security-risk-assessment-tool.
- When reporting as a group for the Advancing Care Information performance category, the group combines the performance of its MIPS eligible clinicians under one Taxpayer Identification Number (TIN). Therefore, the measure is not calculated based upon one MIPS eligible clinician's performance.

Regulatory References

- For further discussion, please see the Quality Payment Program final rule with comment period: 81 FR 77227.
- In order to meet this measure, MIPS eligible clinician must use the capabilities and standards of CEHRT at 45 CFR 170.314(d)(1) through (d)(9) or 45 CFR 170.315(d)(1) through (d)(9).

Certification and Standards Criteria

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

Certification Criteria	
§ 170.314(d)(1) Authentication, access control, and authorization	(i) Verify against a unique identifier(s) (e.g., username or number) that a person seeking access to electronic health information is the one claimed; and (ii) Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in paragraph (d)(1)(i) of this section, and the actions the user is permitted to perform with the EHR technology.
§ 170.314(d)(2) Auditable events and tamper-resistance	(i) *Record actions.* EHR technology must be able to: (A) Record actions related to electronic health information in accordance with the standard specified in §170.210(e)(1); (B) Record the audit log status (enabled or disabled) in accordance with the standard specified in §170.210(e)(2) unless it cannot be disabled by any user; and (C) Record the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by EHR technology in accordance with the standard specified in §170.210(e)(3) unless the EHR technology prevents electronic health information from being locally stored on end-user devices (see 170.314(d)(7) of this section). (ii) *Default setting.* EHR technology must be set by default to perform the capabilities specified in paragraph (d)(2)(i)(A) of this section and, where applicable, paragraphs (d)(2)(i)(B) or (C), or both paragraphs (d)(2)(i)(B) and (C). (iii) *When disabling the audit log is permitted.* For each capability specified in paragraphs (d)(2)(i)(A) through (C) of this section that EHR technology permits to be disabled, the ability to do so must be restricted to a limited set of identified users. (iv) *Audit log protection.* Actions and statuses recorded in accordance with paragraph (d)(2)(i) of this section must not be capable of being changed, overwritten, or deleted by the EHR technology. (v) *Detection.* EHR technology must be able to detect whether the audit log has been altered.
§ 170.314(d)(3) Audit report(s)	Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the data specified in the standards at §170.210(e).

§170.314(d)(4) Amendments	Enable a user to electronically select the record affected by a patient's request for amendment and perform the capabilities specified in paragraphs (d)(4)(i) or (ii) of this section. (i) *Accepted amendment.* For an accepted amendment, append the amendment to the affected record or include a link that indicates the amendment's location. (ii) *Denied amendment.* For a denied amendment, at a minimum, append the request and denial of the request to the affected record or include a link that indicates this information's location.
§ 170.314(d)(5) Automatic log-off	Prevent a user from gaining further access to an electronic session after a predetermined time of inactivity.
§ 170.314(d)(6) Emergency access	Permit an identified set of users to access electronic health information during an emergency.
§ 170.314(d)(7) End-user device encryption	Paragraph (d)(7)(i) or (ii) of this section must be met to satisfy this certification criterion. (i) EHR technology that is designed to locally store electronic health information on end-user devices must encrypt the electronic health information stored on such devices after use of EHR technology on those devices stops. (A) Electronic health information that is stored must be encrypted in accordance with the standard specified in §170.210(a)(1). (B) *Default setting.* EHR technology must be set by default to perform this capability and, unless this configuration cannot be disabled by any user, the ability to change the configuration must be restricted to a limited set of identified users. (ii) EHR technology is designed to prevent electronic health information from being locally stored on end-user devices after use of EHR technology on those devices stops.
§ 170.314(d)(8) Integrity	(i) Create a message digest in accordance with the standard specified in §170.210(c)(1). (ii) Verify in accordance with the standard specified in §170.210(c)(1) upon receipt of electronically exchanged health information that such information has not been altered.

§ 170.314(d)(9) Optional– accounting of disclosures	Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in §170.210(d).
§ 170.315(d)(1) Authentication, access control, and authorization	(i) Verify against a unique identifier(s) (e.g., username or number) that a user seeking access to electronic health information is the one claimed; and (ii) Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in paragraph (d)(1)(i) of this section, and the actions the user is permitted to perform with the EHR technology.
§ 170.315(d)(2) Auditable events and tamper-resistance	(i) Record actions. EHR technology must be able to: A) Record actions related to electronic health information in accordance with the standard specified in § 170.210(e)(1); B) Record the audit log status (enabled or disabled) in accordance with the standard specified in § 170.210(e)(2) unless it cannot be disabled by any user; and C) Record the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by EHR technology in accordance with the standard specified in § 170.210(e)(3) unless the EHR technology prevents electronic health information from being locally stored on end-user devices (see paragraph (d)(7) of this section). (ii) Default setting. Technology must be set by default to perform the capabilities specified in paragraph (d)(2)(i)(A) of this section and, where applicable, paragraphs (d)(2)(i)(B) and (d)(2)(i)(C), of this section. (iii) When disabling the audit log is permitted. For each capability specified in paragraphs (d)(2)(i)(A) through (C) of this section that technology permits to be disabled, the ability to do so must be restricted to a limited set of users. (iv) Audit log protection. Actions and statuses recorded in accordance with paragraph (d)(2)(i) of this section must not be capable of being changed, overwritten, or deleted by the EHR technology. (v) Detection. Technology must be able to detect whether the audit log has been altered.

§ 170.315(d)(3) Audit report(s)	Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the data specified in the standards at § 170.210(e).
§170.315(d)(4) Amendments	Enable a user to electronically select the record affected by a patient’s request for amendment and perform the capabilities specified in paragraphs (d)(4)(i) or (ii) of this section. (i) Accepted amendment -For an accepted amendment, append the amendment to the affected record or include a link that indicates the amendment’s location. (ii) Denied amendment -For a denied amendment, at a minimum, append the request and denial of the request in at least one of the following ways: (A) To the affected record. (B) Include a link that indicates this information's location.
§ 170.315(d)(5) Automatic access time-out	(i) Automatically stop user access to health information after a predetermined period of inactivity. (ii) Require user authentication in order to resume or regain the access that was stopped.
§ 170.315(d)(6) Emergency access	Permit an identified set of users to access electronic health information during an emergency.
§ 170.315(d)(7) End-user device encryption	The requirements specified in one of the following paragraphs (that is, paragraphs (d)(7)(i) and (d)(7)(ii) of this section) must be met to satisfy this certification criterion. (i) Technology that is designed to locally store electronic health information on end-user devices must encrypt the electronic health information stored on such devices after use of the technology on those devices stops. (A) Electronic health information that is stored must be encrypted in accordance with the standard specified in § 170.210(a)(2). (B) Default setting. Technology must be set by default to perform this capability and, unless this configuration cannot be disabled by any user, the ability to change the configuration must be restricted to a limited set of identified users.

	(ii) Technology is designed to prevent electronic health information from being locally stored on end-user devices after use of the technology on those devices stops.
§ 170.315(d)(8) Integrity	(i) Create a message digest in accordance with the standard specified in §170.210(c)(2). (ii) Verify in accordance with the standard specified in § 170.210(c)(2) upon receipt of electronically exchanged health information that such information has not been altered.
§ 170.315(d)(9) Trusted connection	Establish a trusted connection using one of the following methods: (i) Message-level. Encrypt and integrity protect message contents in accordance with the standards specified in §170.210(a)(2) and (c)(2). (ii) Transport-level. Use a trusted connection in accordance with the standards specified in §170.210(a)(2) and (c)(2).

For additional information, please review the ONC 2014 Standards Hub, ONC 2015 Standards Hub, and ONC Certification Companion Guides (CCGs).

Disclaimer: *This document is intended only for informational purposes. It does not provide a complete summary of the applicable regulations and policies. We refer readers to the final rule with comment period titled Medicare Program; Merit-Based Incentive Payment System (MIPS) and Alternative Payment Model (APM) Incentive Under the Physician Fee Schedule, and Criteria for Physician-Focused Payment Models, 81 Fed. Reg. 77008-77831 (Nov. 4, 2016).*