Quality Payment PROGRAM

Merit-Based Incentive Payment System (MIPS) Promoting Interoperability Performance Category Measure 2018 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 clinician 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: **Yes**
- Percentage of Performance Score: **0**
- Eligible for Bonus Score: **One-time bonus of 10% for MIPS eligible clinicians and groups who report using 2015 Edition CEHRT exclusively for the 2018 performance period and submit only Promoting Interoperability measures**

Note: MIPS eligible clinicians must fulfill the requirements of base score measures to earn a base score in order to earn any score in the Promoting Interoperability performance category. In addition to the base score, MIPS eligible clinicians have the opportunity to earn additional credit through the submission of performance measures and a bonus measure and/or activity.

Additional Information

- MIPS eligible clinicians can report the Promoting Interoperability objectives and 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 50% base score for the Promoting Interoperability performance category. MIPS eligible clinicians must submit a “yes” for the security risk analysis measure, and at least a 1 in the numerator for the numerator/denominator of the remaining measures or claim exclusions. More information about Promoting Interoperability scoring is available on the QPP website.
- A MIPS eligible clinician must meet this objective and measure to earn any score within the promoting interoperability performance category. Failure to do so will result in a base score of zero as well as a performance score of zero and a Promoting Interoperability performance category score of zero.
- It is acceptable for the security risk analysis to be conducted 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 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 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: http://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: http://www.healthit.gov/providers-professionals/security-risk-assessment-tool.
- When MIPS eligible clinicians choose to report as a group, data should be aggregated for all MIPS eligible clinicians under one Taxpayer Identification Number (TIN). This includes those MIPS eligible clinicians who may qualify for reweighting such as a significant hardship exception, hospital or ASC-based status, or in a specialty which is not required to report data to the Promoting Interoperability performance category. If these MIPS eligible clinicians choose to report as a part of a group practice, they will be scored on the Promoting Interoperability performance category like all other MIPS eligible clinicians.

Regulatory References

- For further discussion, please see the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) final rule: 81 FR 77227.
- In order to meet this objective and measure, MIPS eligible clinicians must use the capabilities and standards of CEHRT at 45 CFR 170.315 (d)(1) through (d)(9).

Certification and Standards Criteria

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

Certification Criteria*	
§ 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	(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).

**Depending on the type of certification issued to the EHR technology, it will also have been certified to the certification criterion adopted at 45 CFR 170.314 (g)(1), (g)(2), or both, in order to assist in the calculation of this meaningful use measure.*

Standards Criteria	
§ 170.210(e)(1) Record actions related to electronic health information, audit log status, and encryption of end-user devices	(1)(i) The audit log must record the information specified in sections 7.2 through 7.4, 7.6, and 7.7 of the standard specified in §170.210(h) and changes to user privileges when health IT is in use. (ii) The date and time must be recorded in accordance with the standard specified at §170.210(g).
§ 170.210(e)(2) Record actions related to electronic health information, audit log status, and encryption of end-user devices	(3) The audit log must record the information specified in sections 7.2 and 7.4 of the standard specified at §170.210(h) when the encryption status of electronic health information locally stored by health IT on end-user devices is changed. The date and time each action occurs in accordance with the standard specified at §170.210(g).
§ 170.210(a)(1) Encryption and decryption of electronic health information	Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2, (January 27, 2010) (incorporated by reference in §170.299).

§ 170.210(c) Hashing of electronic health information	A hashing algorithm with a security strength equal to or greater than SHA-1 (Secure Hash Algorithm (SHA-1)) as s specified by the National Institute of Standards and Technology (NIST) in FIPS PUB 180-4 (March 2012).
§ 170.210(d) Record treatment, payment, and health care operations disclosures	The date, time, patient identification, user identification, and a description of the disclosure must be recorded for disclosures for treatment, payment, and health care operations, as these terms are defined at 45 CFR 164.501.

Additional certification and standards criteria may apply. Review the ONC 2015 Edition Final Rule for more information.