Medicare Promoting Interoperability Program Stage 3
Eligible Hospitals, Critical Access Hospitals, and Dual-Eligible Hospitals Attesting to CMS
Objectives and Measures for 2018

Objective 1 of 6
Updated: July 2018

Protect Patient Health Information	
Objective	Protect electronic protected health information (ePHI) created or maintained by the certified electronic health record technology (CEHRT) through the implementation of appropriate technical, administrative, and physical safeguards.
Measure	**Security Risk Analysis:** Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the security (including encryption) of data created or maintained by CEHRT in accordance with requirements under 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 eligible hospital or critical access hospitals (CAH) risk management process.

Table of Contents

- Attestation Requirements
- Additional Information
- Regulatory References
- Certification and Standards Criteria

Attestation Requirements

YES/NO

Eligible hospitals and CAHs must attest YES to conducting or reviewing a security risk analysis and implementing security updates as necessary and correcting identified security deficiencies to meet this measure.

Additional Information

- To meet Stage 3 requirements, all eligible hospitals or CAHs must use technology certified to the 2015 Edition. An eligible hospital or CAH who has technology certified to a combination of the 2015 Edition and 2014 Edition may potentially attest to the Stage 3 requirements, if the mix of certified technologies would not prohibit them from meeting the Stage 3 measures. An eligible hospital or CAH who has technology certified to the 2014 Edition may not attest to Stage 3.
- Eligible hospitals and CAHs must conduct or review a security risk analysis of CEHRT including addressing encryption/security of data, and implement updates as necessary at least once each calendar year and attest to conducting the analysis or review.
- An analysis must be done upon installation or upgrade to a new system and a review must be conducted covering each Promoting Interoperability (PI) reporting period. Any security

updates and deficiencies that are identified should be included in the eligible hospital or CAHs risk management process and implemented or corrected as dictated by that process.

- It is acceptable for the security risk analysis to be conducted outside the PI reporting period; however, the analysis must be unique for each PI reporting period, the scope must include the full PI reporting period and must be conducted within the calendar year of the PI reporting period (January 1st – December 31st).
- 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, eligible hospitals or CAHs 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 in 45 CFR 164.308(a)(1), which was created by the HIPAA Security Rule. Meaningful use does not impose new or expanded requirements on the Health Insurance Portability and Accountability Act (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 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 eligible hospitals or CAHs include a Security Risk Assessment (SRA) Tool developed by the Office of National Coordinator for Health Information Technology (ONC) and OCR: http://www.healthit.gov/providers-professionals/security-risk-assessment-tool

Regulatory References

- This objective may be found in Section 42 of the code of the federal register at 495.24 (cd)(1)(i) and (ii). For further discussion please see 80 FR 62832.
- In order to meet this objective and measure, an eligible hospital or CAH must possess the capabilities and standards of CEHRT at 45 CFR 170.315 (d)(1) through (d)(9).

Objective 1 of 6
Updated: July 2018

Certification Standards and Criteria

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

Certification Criteria	
§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)(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). (i) 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. (ii) 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. (iii) 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.

	(iv) 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)(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)(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)(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.

Objective 1 of 6
Updated: July 2018

§ 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).

Standards Criteria	
§ 170.210(e)(1), § 170.210(e)(2) and § 170.210(e)(3) Record actions related to electronic health information, audit log status, and encryption of end-user devices.	(i) (1) 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 information technology (HIT) is in use. (i) The date and time must be recorded in accordance with the standard specified at § 170.210(g). (ii) (2) 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 audit log status is changed. (i) The date and time each action occurs in accordance with the standard specified at § 170.210(g). (i) (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 HIT 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).

Objective 1 of 6
Updated: July 2018

§ 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 is specified by the 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.