Eligible Hospitals, Critical Access Hospitals and Dual-Eligible Hospitals Attesting To CMS EHR Incentive Program Modified Stage 2 Objectives and Measures for 2017
Objective 1 of 7
Updated: November 2016

Protect Patient Health Information	
Objective	Protect electronic protected health information (ePHI) created or maintained by the CEHRT through the implementation of appropriate technical capabilities.
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 created or maintained by CEHRT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the eligible hospital or CAH's risk management process.

Table of Contents

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

Attestation Requirements
YES/NO

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
- 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 EHR reporting period. Any security updates and deficiencies that are identified should be included in the provider's 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 EHR reporting period; however, the analysis must be unique for each EHR reporting period, the scope must include the full EHR reporting period and must be conducted within the calendar year of the EHR reporting period (January 1st – December 31st.).
- The parameters of the security risk analysis are defined 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 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

Regulatory References

- This objective may be found in Section 42 of the code of the federal register at 495.22 (f)(1)(i) and (ii). For further discussion please see 80 FR 62793.
- In order to meet this objective and measure, an eligible hospital or CAH must possess the capabilities and standards of CEHRT at 45 CFR 170.314 (d)(4), (d)(2), (d)(3), (d)(7), (d)(1), (d)(5), (d)(6), (d)(8), and optionally (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 objective.

Certification Criteria	
§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)(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), (B), and (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)(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)(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)(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)(8) Integrity	(i) Create a message digest in accordance with the standard specified in §170.210(c). (ii) Verify in accordance with the standard specified in § 170.210(c) 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).

Standards Criteria	
§ 170.210(e)(1), § 170.210(e)(2) and § 170.210(e)(3)	(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 at § 170.210(h) when EHR technology is in use. (ii) The date and time must be recorded in accordance with the standard specified at § 170.210(g).
Record actions related to electronic health information, audit log status, and encryption status	(i) 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. (ii) The date and time each action occurs in accordance with the standard specified at § 170.210(g). 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 EHR technology 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 (incorporated by reference in §170.299).
§ 170.210(c) Create message digest	A hashing algorithm with a security strength equal to or greater than SHA-1 (Secure Hash Algorithm) as specified by the NIST in FIPS PUB 180-4 (March, 2012) must be used to verify that electronic health information has not been altered.
§ 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.