Eligible Professional Meaningful Use Core Measures Measure 13 of 13

Stage 1 (2014 Definition)
Last updated: May 2014

Protect Electronic Health Information	
Objective	Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.
Measure	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.
Exclusion	No exclusion.

Table of Contents

Definition of Terms

Appropriate Technical Capabilities – A technical capability would be appropriate if it protected the electronic health information created or maintained by the certified EHR technology. All of these capabilities could be part of the certified HER technology or outside systems and programs that support the privacy and security of certified EHR technology.

Attestation Requirements

YES / NO

Eligible professionals (EPs) must attest YES to having conducted or reviewed a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implemented security updates as necessary and corrected identified security deficiencies prior to or during the EHR reporting period to meet this measure.

Additional Information

- EPs must conduct or review a security risk analysis of certified EHR technology and implement updates as necessary at least once prior to the end of the EHR reporting period and attest to that conduct or review. The testing could occur prior to the beginning of the first EHR reporting period. However, a new review would have to occur for each subsequent reporting period.

- A security update would be required if any security deficiencies were identified during the risk analysis. A security update could be updated software for certified EHR technology to be implemented as soon as available, changes in workflow processes or storage methods, or any other necessary corrective action that needs to take place in order to eliminate the security deficiency or deficiencies identified in the risk analysis.

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)(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 (d)(2)(i)(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) 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.

*Additional certification criteria may apply. Review the ONC 2014 Edition EHR Certification Criteria Grid Mapped to Meaningful Use Stage 1 for more information.

Standards Criteria	
§170.210(e)(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 at § 170.210(h) when EHR technology is in use.
§170.210(e)(1)(ii)	The date and time must be recorded in accordance with the standard specified at § 170.210(g).
§170.210(e)(2)(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.
§170.210(e)(2)(ii)	The date and time each action occurs in accordance with the standard specified at § 170.210(g).
§170.210(e)(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 the 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)