Eligible Professional Meaningful Use Core Measures Measure 15 of 15

Stage 1

Date issued: November 7, 2010

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
- Attestation Requirements
- Additional Information
- Certification and Standards Criteria
- Related Certification FAQs

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	
§170.302(o) Access control	Assign a unique name and/or number for identifying and tracking user identity and establish controls that permit only authorized users to access electronic health information.
§170.302(p) Emergency access	Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency.
§170.302(q) Automatic log-off	Terminate an electronic session after a predetermined time of inactivity.
§170.302(r) Audit log	(1) Record actions. Record actions related to electronic health information in accordance with the standard specified in §170.210(b). .
	(2) Generate audit log. Enable a user to generate an audit log for a specific time period and to sort entries in the audit log according to any of the elements specified in the standard at §170.210(b).
§170.302(s) Integrity	(1) Create a message digest in accordance with the standard specified in §170.210(c).
	(2) 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.
	(3) Detection. Detect the alteration of audit logs.
§170.302(t) Authentication	Verify that a person or entity seeking access to electronic health information is the one claimed and is authorized to access such information.
§170.302(u) General	Encrypt and decrypt electronic health information in accordance with the standard specified in §170.210(a)(1), unless the Secretary determines that the use of such

encryption	algorithm would pose a significant security risk for Certified EHR Technology.
§170.302(v) Encryption when exchanging electronic health information	Encrypt and decrypt electronic health information when exchanged in accordance with the standard specified in §170.210(a)(2).
§170.302(w) 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	
Record actions related to electronic health information	• §170.210(b) - The date, time, patient identification, and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which actions(s) occurred and by whom must also be recorded.
Verification that electronic health information has not been altered in transit	• §170.210(c) - A hashing algorithm with a security strength equal to or greater than SHA-1 (Secure Hash Algorithm (SHA-1) as specified by the National Institute of Standards and Technology (NIST) in FIPS PUB 180-3 (October, 2008) must be used to verify that electronic health information has not been altered
Encryption and decryption of electronic health information	• §170.210(a)(1) - 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(a)(2) - Any encrypted and integrity protected link.
Record treatment, payment, and health care operations disclosures	• §170.210(d) - 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.

Related Certification FAQs

Click on the green numbers to view the answer to the FAQ.

- If an EHR Module addresses multiple certification criteria (thus providing multiple capabilities), does it need to be tested and certified to the applicable privacy and security certification criteria as a whole or for each capability? ***9-10-008-1***