

CORE	EP	EH	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	TPs	WG LEAD(s)
			Proposed Stage 2 Objective	Proposed Stage 2 Measure						
CORE			Provide patients the ability to view online, download, and transmit their health information within 4 business days of the information being available to the EP.	EPs must satisfy both measures in order to meet the objective: 1. More than 50 percent of all unique patients seen by the EP during the EHR reporting period are provided timely (within 4 business days after the information is available to the EP) online access to their health information subject to the EP's discretion to withhold certain information. 2. More than 10 percent of all unique patients seen by the EP during the EHR reporting period (or their authorized representatives) view, download or transmit to a third party their health information.	1. The number of patients in the denominator who have timely (within 4 business days after the information is available to the EP) online access to their health information online. 2. The number of unique patients (or their authorized representatives) in the denominator who have viewed online or downloaded or transmitted to a third party the patient's health information.	1. Number of unique patients seen by the EP during the EHR reporting period. 2. Number of unique patients seen by the EP during the EHR reporting period.	§170.314(e)(1) <u>View, download, and transmit to 3<sup>rd</sup> party.</u> (i) Enable a user to provide patients (and their authorized representatives) with on line access to do all of the following: (A) <u>View</u> . Electronically view in accordance with the standard adopted at § 170.204(a), at a minimum, the following data elements: (1) Patient name; gender; date of birth; race; ethnicity; preferred language; smoking status; problem list; medication list; medication allergy list; procedures; vital signs; laboratory tests and values/results; provider's name and contact information; names and contact information of any additional care team members beyond the referring or transitioning provider and the receiving provider; and care plan, including goals and instructions. (2) <u>Inpatient setting only</u> . Admission and discharge dates and locations; reason(s) for hospitalization; names of providers of care during hospitalization; laboratory tests and values/results (available at time of discharge); and discharge instructions for patient. (B) <u>Download</u> . Electronically download: (1) A file in human readable format that includes, at a minimum: (i) <u>Ambulatory setting only</u> . All of the data elements specified in paragraph (e)(1)(i)(A)(1). (ii) <u>Inpatient setting only</u> . All of the data elements specified in paragraphs (e)(1)(i)(A)(1) and (e)(1)(i)(A)(2). (2) A summary care record formatted according to the standards adopted at § 170.205(a)(3) and that includes, at a minimum, the following data elements expressed, where applicable, according to the specified standard(s): (i) Patient name; gender; date of birth; medication allergies; vital signs; the provider's name and contact information; names and contact information of any additional care team members beyond the referring or transitioning provider and the receiving provider; care plan, including goals and instructions; (ii) <u>Race and ethnicity</u> . The standard specified in § 170.207(f); (iii) <u>Preferred language</u> . The standard specified in § 170.207(j); (iv) <u>Smoking status</u> . The standard specified in § 170.207(l); (v) <u>Problems</u> . At a minimum, the version of the standard specified in § 170.207(a)(3); (vi) <u>Encounter diagnoses</u> . The standard specified in § 170.207(m); (vii) <u>Procedures</u> . The standard specified in § 170.207(b)(2) or § 170.207(b)(3); (viii) <u>Laboratory test(s)</u> . At a minimum, the version of the standard specified in § 170.207(g); (ix) <u>Laboratory value(s)/result(s)</u> . The value(s)/results of the laboratory test(s) performed; (x) <u>Medications</u> . At a minimum, the version of the standard specified in § 170.207(h); and (xi) <u>Inpatient setting only</u> . The data elements specified in paragraph (e)(1)(i)(A)(2). (3) Images formatted according to the standard adopted at § 170.205(j). (C) <u>Transmit to third party</u> . Electronically transmit the summary care record created in paragraph (e)(1)(i)(B)(2) or images available to download in paragraph (e)(1)(i)(B)(3) in accordance with: (1) The standard specified in § 170.202(a)(1); and (2) The standard specified in § 170.202(a)(2). (ii) Patient accessible log. (A) When electronic health information is viewed, downloaded, or transmitted to a third-party using the capabilities included in paragraphs (e)(1)(i)(A)-(C), the following information must be recorded and made accessible to the patient: (1) The electronic health information affected by the action(s); (2) The date and time each action occurs in accordance with the standard specified at § 170.210(g); (3) The action(s) that occurred; and (4) User identification. (B) EHR technology presented for certification may demonstrate compliance with paragraph (e)(1)(ii)(A) if it is also certified to the certification criterion adopted at § 170.314(d)(2) and the information required to be recorded in paragraph (e)(1)(ii)(A) is accessible by the patient.	§ 170.204(a) (Web Content Accessibility Guidelines (WCAG) 2.0, Level AA Conformance); § 170.205(a)(3) (Consolidated CDA); § 170.205(j) (DICOM PS 3—2011); § 170.207(f) (OMB standards for the classification of federal data on race and ethnicity); § 170.207(j) (ISO 639-1:2002 (preferred language)); § 170.207(l) (smoking status types); § 170.207(a)(3) (SNOMED-CT® International Release January 2012); § 170.207(m) (ICD-10-CM); § 170.207(b)(2) (HCPCS and CPT-4) or § 170.207(b)(3) (ICD-10-PCS); § 170.207(g) (LOINC version 2.38); § 170.207(h) (RxNorm February 6, 2012 Release); § 170.202(a)(1) (Applicability Statement for Secure Health Transport) and § 170.202(a)(2) (XDR and XDM for Direct Messaging); and § 170.210(g) (synchronized clocks)	<b>NEW (Needed)</b> <b>Hospital – Electronic Copy of Health Information 170.306 (d)(1) (EH Link) and Hospital – Electronic Copy of Health Information – 170.306 (d)(1)- Errata (EH Errata):</b> This test evaluates the capability for a Complete EHR or EHR Module to create an electronic copy of a patient's clinical information, including, at a minimum, diagnostic test results, problem list, medication list, medication allergy list, and procedures, in the formats and vocabularies specified by the referenced standards. Per the FR criteria, the test procedure does not evaluate the capability to create an electronic copy that includes other types of patient information. The test procedure consists of one section: Create - evaluates the capability to create a copy of a patient's clinical information either on electronic media or some other electronic means and in HL7 CCD format or ASTM CCR format using the specified vocabularies. The patient's clinical information includes diagnostic test results, problems, medications, medication allergies, and procedures in human-readable form. Tester uses the Vendor-identified function(s) and Vendor-entered data to create a copy of patient clinical information, including diagnostic test results, problems, medications, medication allergies, and procedures on electronic media or via another electronic means formatted in HL7 CCD or ASTM CCR; Tester validates that the data rendered on the electronic media or via other electronic means are complete and in conformance <b>Hospital – Electronic Copy of Discharge Summary - 170.306 (d)(2) (EH Link 2):</b> TP consist of one section: Create - evaluates the capability to create a copy of a patient's discharge summary in human readable format and on electronic media or through some other electronic means. Tester enters the Vendor-supplied test data for discharge summary into a patient's EHR. Tester uses the Vendor-identified function(s) to create a copy of this patient clinical information on electronic media or via another electronic means; Tester validates that the discharge summary data rendered on the electronic media or via other electronic means are complete and in conformance <b>Hospital - Electronic Copy of Discharge Instructions – 170.306 (e) (EH Link):</b> TP consist of one section: Create Discharge Instructions – evaluates the capability to create an electronic copy of the discharge instructions for a patient, in human readable format on electronic media. The Tester creates an electronic copy of the discharge instructions for a patient on electronic media. Tester validates that the discharge instructions for the patient are created on electronic media and that the data are human readable and accurate and complete <b>Eligible Professional - Electronic Copy of Health Information - 170.304 (f) (EP Link) and Eligible Professional - Electronic Copy of Health Information – 170.304 (f) - Errata (EP Errata):</b> This test evaluates the capability for a Complete EHR or EHR Module to create an electronic copy of a patient's clinical information, including, at a minimum, diagnostic test results, problem list, medication list, and medication allergy list in the formats and vocabularies specified by the referenced standards. Per the FR criteria, the test procedure does not evaluate the capability to create an electronic copy that includes other types of patient information. The test procedure consists of one section: Create - evaluates the capability to create a copy of a patient's clinical information either on electronic media or some other electronic means and in HL7 CCD format or ASTM CCR format using the specified vocabularies. The patient's clinical information includes diagnostic test results, problems, medications, and medication allergies in human-readable form o The Tester uses the Vendor-identified function(s) and Vendor-entered data to create a copy of patient clinical information, including diagnostic test results, problems, medications, and medication allergies on electronic media or via another electronic means formatted in HL7 CCD or ASTM CCR; Tester validates that the data rendered on the electronic media or via other electronic means are complete and in conformance <b>Eligible Professional - Timely Access - 170.304 (g) (EP Link):</b> This test evaluates the capability for a Complete EHR or EHR Module to enable a user to provide patients with online access to their clinical information, including lab test results, problem list, medication list, and medication allergy list. Online access is evaluated in terms of the capability for the patient to access their health information online and either display or print the required clinical information. Other forms of online access are not evaluated in this test. This test procedure consists of one section: Provide Patient Online Access – evaluates the capability to provide patients with online access to their clinical information, including lab test results, problem list, medication list, and medication allergy list. Tester provides a patient with online access to their clinical information, including lab test results, problem list, medication list, and medication allergy list; Tester verifies that the patient accesses their clinical information, including lab test results, problem list, medication list, and medication allergy list	Andrea Sim Wes Rishel Rebecca Rockwood Cris Ross Bob Barker
			Provide patients the ability to view online, download, and transmit information about a hospital admission.	EHs and CAHs must satisfy both measures in order to meet the objective: 1. More than 50% of all patients who are discharged from the inpatient or emergency department (POS 21 or 23) of an eligible hospital or CAH have their information available online within 36 hours of discharge. 2. More than 10% of all patients who are discharged from the inpatient or emergency department (POS 21 or 23) of an eligible hospital or CAH view, download or transmit to a third party their information during the reporting period.	1. The number of patients in the denominator whose information is available online within 36 hours of discharge. 2. The number of patients in the denominator who view, download or transmit to a third party the information provided by the eligible hospital or CAH online during the EHR reporting period.	1. Number of unique patients seen by the EP during the EHR reporting period. 2. Number of unique patients seen by the EP during the EHR reporting period.				
<p><b>P&amp;S Workgroup Comments</b></p> <p><b>1) Is a change in the test procedures linked above suggested based on a change in criterion? If “yes,” what is the suggestion?</b> Yes, these are new certification criteria for Stage 2. Need new TPs to test capabilities to: a) <u>View and Download</u>: Adapt Timely Access TP for both view and download. Need to include all data element specified in criteria, and to apply to EHs as well as EPs. TP for download must include both creation of document (first 4 TPs) and download capability. b) <u>Transmit record to 3<sup>rd</sup> party [(i)(C)]</u> – The first 6 TP links above are related to creation of a clinical document – transmission is not covered. So they should be adaptable for testing transmissions from a patient portal using Direct. Also need to generate a CCDA (rather than CCD or CCR). Need to establish trust-chain for the recipient beforehand. Use of appropriate S/MIME and signatures. Consider using the send-functions of the reference implementation for Direct as TP. c) <u>Patient Accessible Logs</u>: Generation of audit trail for actions relating to patient login, viewing, downloading, transmitting to 3<sup>rd</sup> party, and viewing audit trail is not addressed in existing TPs. Need new TPs. <u>General comment</u>: Test procedures should respond to the lowest level of “what” (security need should be addressed) without prescribing “how” to address it beyond what is specified in prescribed standards and certification criteria. Consider that the “how” could be addressed by prevailing industry practices such as those documented in NIST guidance, and that such practices might change more often than Meaningful Use Criteria. Also consider that there might be only one or two alternatives to satisfy the requirement. But this, in and of itself, does not mean that the requirement is too prescriptive.</p> <p><b>2) Is a change in the test procedures linked above suggested based on either a criterion not considered or an update, advances in technology? If “yes,” what is the suggestion?</b> N/A</p>										

	EP	EH	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	TPs	WG LEAD(s)
			Proposed Stage 2 Objective	Proposed Stage 2 Measure						
CORE	14	*	Use secure electronic messaging to communicate with patients on relevant health information.	A secure message was sent using the electronic messaging function of Certified EHR Technology by more than 10% of unique patients seen during the EHR reporting period.	The number of patients in the denominator who send a secure electronic message to the EP using the electronic messaging function of Certified EHR Technology during the EHR reporting period.	Number of unique patients seen by the EP during the EHR reporting period.	§170.314(e)(3) <u>Ambulatory setting only – secure messaging.</u> Enable a user to electronically send messages to, and receive messages from, a patient in a manner that ensures: (i) Both the patient and EHR technology are authenticated; and (ii) The message content is encrypted and integrity-protected in accordance with the standard for encryption and hashing algorithms specified at § 170.210(f).	§ 170.210(f) Any encryption and hashing 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.	NEW	Ken Tarkoff Cris Ross
	<p><b>P&amp;S Workgroup Comments</b></p> <p><b>1) Is a change in the test procedures linked above suggested based on a change in criterion? If “yes,” what is the suggestion?</b>                      Yes. This is a new criterion for Stage 2.  <u>Patient and EHR Technology are authenticated:</u> Since this criterion does not constrain implementation options, we see no way to objectively test conformance with this criterion. We suggest requiring the developer to document (attestation) how the EHR product meets this criterion. Service Organization Control (SOC) Type 2 reports and PCI third-party verification of controls are examples of approaches for addressing such “untestable” criteria, without thwarting market innovation or limiting architectural choices, such as cloud computing.  <u>Message Content Encrypted and Integrity-protected:</u> Here again, the criterion and the standard referenced is not specific enough to objectively test conformance. We suggest using a testing procedure based on attestation, similar to the current General Encryption TP</p> <p><b>2) Is a change in the test procedures linked above suggested based on either a criterion not considered or an update, advances in technology? If “yes,” what is the suggestion?</b>                      N/A</p>									

CORE	E	P	EH	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	TPs	WG LEAD(s)
				Proposed Stage 2 Objective	Proposed Stage 2 Measure						
	20	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest 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 provider's risk management process.			<p>§170.314(d)(1)</p> <p><u>Authentication, access control, and authorization.</u></p> <p>(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</p> <p>(ii) Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in (d)(1)(i), and the actions the user is permitted to perform with the EHR technology.</p>	None.	<p><b>Access Control</b>  <a href="http://healthcare.nist.gov/docs/170.302.o_AccessControl_v1.1.pdf">http://healthcare.nist.gov/docs/170.302.o_AccessControl_v1.1.pdf</a>): TP consist of one section: Assign Unique Name/Number – Tester creates unique name/number; performs authorized actions based on permission; attempts to perform unauthorized actions and verify that they were note performed.</p> <p><b>Authentication</b>  <a href="http://healthcare.nist.gov/docs/170.302.t_Authentication_v1.1.pdf">http://healthcare.nist.gov/docs/170.302.t_Authentication_v1.1.pdf</a>):TP consist of one section: Verify Authorization – Tester creates a new user account and assigns permissions; performs an action authorized by assign permission and verifies action; attempts to performs action not authorized and verifies action not performed; deletes/deactivates user account; attempts to login to deleted/deactivated account and verify login failed; TP excludes identity proofing and verification across networks</p>	David Kates Liz Johnson Joe Heyman Ken Tarkoff Carol Diamond

**P&S Workgroup Comments**

**1) Is a change in the test procedures linked above suggested based on a change in criterion? If “yes,” what is the suggestion?**

No change in criteria.

**2) Is a change in the test procedures linked above suggested based on either a criterion not considered or an update, advances in technology? If “yes,” what is the suggestion?**

Authentication: TP does not authenticate the identity asserted by the user. TP needs to 1) confirm that the asserted identity is a user recognized by the EHR (identification); 2) confirm that actual identity is the one asserted (authentication); 3) confirm that the authenticated user has been authorized to perform the action being attempted (authorization). Current TP addresses only (1) and (3).

General Comment: There is very little difference between the Access Control and the Authentication TPs (neither addresses identification or authentication). Recommend re-drafting to create 3 separate TPs for 1) identification; 2) authentication; and 3) authorization.

CORE	E	P	EH	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	TPs	WG LEAD(s)
				Proposed Stage 2 Objective	Proposed Stage 2 Measure						
21	*	*		Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest 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 provider's risk management process.			<p>§170.314(d)(2)</p> <p><u>Auditable events and tamper-resistance.</u></p> <ul style="list-style-type: none"> <li>(i) Enabled by default. The capability specified in paragraph (d)(2)(ii) must be enabled by default (i.e., turned on) and must only be permitted to be disabled (and re-enabled) by a limited set of identified users.</li> <li>(ii) Record actions. Record actions related to electronic health information, audit log status and, as applicable, encryption of end-user devices in accordance with the standard specified in § 170.210(e).</li> <li>(iii) Audit log protection. Actions recorded in accordance with paragraph (d)(2)(ii) must not be capable of being changed, overwritten, or deleted.</li> <li>(iv) Detection. Detect the alteration of audit logs.</li> </ul>	<p>§ 170.210(e) Record actions related to electronic health information, audit log status, and encryption of end-user devices.</p> <ul style="list-style-type: none"> <li>(1) When EHR technology is used to record, create, change, access, or delete electronic health information, the following information must be recorded:                             <ul style="list-style-type: none"> <li>(i) The electronic health information affected by the action(s);</li> <li>(ii) The date and time each action occurs in accordance with the standard specified at § 170.210(g);</li> <li>(iii) The actions(s) that occurred;</li> <li>(iv) Patient identification; and</li> <li>(v) User identification.</li> </ul> </li> <li>(2) When the audit log is enabled or disabled, the following must be recorded:                             <ul style="list-style-type: none"> <li>(i) The date and time each action occurs in accordance with the standard specified at § 170.210(g); and</li> <li>(ii) User identification.</li> </ul> </li> <li>(3) As applicable, when encryption of electronic health information managed by EHR technology on end-user devices is enabled or disabled, the following must be recorded:                             <ul style="list-style-type: none"> <li>(i) The date and time each actions occurs in accordance with the standard specified at § 170.210(g); and</li> <li>(ii) User identification.</li> </ul> </li> </ul>	<p><b>Audit Log</b>  <a href="http://healthcare.nist.gov/docs/170.302.r_AuditLog_v1.1.pdf">http://healthcare.nist.gov/docs/170.302.r_AuditLog_v1.1.pdf</a>:TP consist of four sections:</p> <p>Record Actions – Tester enters EHR; Tester records into the log the action taken (automatic function); Tester verifies data elements have been recorded in log;</p> <p>Modify Actions – Tester selects the EHR entered during Record Actions test, displays electronic health information, corrects/updates electronic health information; Tester records into the log the action taken (automatic function); Tester verifies data elements have been recorded in log</p> <p>Generate Audit Log –Tester generates an audit log for a specified time period that will result in audit log containing entries for the actions taken in Record and Modify tests; Tester verifies that audit log has been generated</p> <p>Sort Audit Log Entries – Tester generates audit log for the specified time period and sort audit log entries according to specified elements; Tester verifies that the audit log entries have been sorted</p>	David Kates Bob Barker Liz Johnson

**P&S Workgroup Comments**

1) Is a change in the test procedures linked above suggested based on a change in criterion? If “yes,” what is the suggestion?

No change to criterion.

2) Is a change in the test procedures linked above suggested based on either a criterion not considered or an update, advances in technology? If “yes,” what is the suggestion?

General Comment: Current TPs test only “(ii) Record actions.” Need TPs to test that EHR enables auditing by default (i); protects the audit log (iii); and detects alteration of audit logs (iv).

For (i), suggest checking to assure that system is configured to audit required actions when the system is initialized.

For (iii) and (iv) - audit protection and alteration detection - may need to be “tested” through attestation. Perhaps consider testing whether the access privileges (or roles) defined for the system prohibit write access by other than the audit system, or whether the system writes the audit log to write-once-read-many media.

Also, requiring a developer to implement the capability to “detect the alteration of audit logs” in a system that is “not capable of being changed, overwritten, or deleted” seems superfluous.

CORE	EP	EH	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	TPs	WG LEAD(s)
			Proposed Stage 2 Objective	Proposed Stage 2 Measure						
22	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest 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 provider's risk management process.			<p>§170.314(d)(3)</p> <p><u>Audit report(s)</u>. 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 elements specified in the standard at § 170.210(e).</p>	<p>§ 170.210(e) Record actions related to electronic health information, audit log status, and encryption of end-user devices.</p> <p>(B) When EHR technology is used to record, create, change, access, or delete electronic health information, the following information must be recorded:</p> <ul style="list-style-type: none"> <li>(i) The electronic health information affected by the action(s);</li> <li>(ii) The date and time each action occurs in accordance with the standard specified at § 170.210(g);</li> <li>(iii) The actions(s) that occurred;</li> <li>(iv) Patient identification; and</li> <li>(v) User identification.</li> </ul> <p>(C) When the audit log is enabled or disabled, the following must be recorded:</p> <ul style="list-style-type: none"> <li>(i) The date and time each action occurs in accordance with the standard specified at § 170.210(g); and</li> <li>(ii) User identification.</li> </ul> <p>(D) As applicable, when encryption of electronic health information managed by EHR technology on end-user devices is enabled or disabled, the following must be recorded:</p> <ul style="list-style-type: none"> <li>(i) The date and time each actions occurs in accordance with the standard specified at § 170.210(g); and</li> <li>(ii) User identification.</li> </ul>	<p><b>Audit Log</b>  <a href="http://healthcare.nist.gov/docs/170.302.r_AuditLog_v1.1.pdf">http://healthcare.nist.gov/docs/170.302.r_AuditLog_v1.1.pdf</a>:TP consist of four sections:</p> <p>Record Actions – Tester enters EHR; Tester records into the log the action taken (automatic function); Tester verifies data elements have been recorded in log;</p> <p>Modify Actions – Tester selects the EHR entered during Record Actions test, displays electronic health information, corrects/updates electronic health information; Tester records into the log the action taken (automatic function); Tester verifies data elements have been recorded in log</p> <p>Generate Audit Log –Tester generates an audit log for a specified time period that will result in audit log containing entries for the actions taken in Record and Modify tests; Tester verifies that audit log has been generated</p> <p>Sort Audit Log Entries – Tester generates audit log for the specified time period and sort audit log entries according to specified elements; Tester verifies that the audit log entries have been sorted</p>	David Kates Bob Barker Liz Johnson

**P&S Workgroup Comments**

**1) Is a change in the test procedures linked above suggested based on a change in criterion? If “yes,” what is the suggestion?**

No change to criterion.

**2) Is a change in the test procedures linked above suggested based on either a criterion not considered or an update, advances in technology? If “yes,” what is the suggestion?**

Link is for testing audit log. Needs to be reviewed.

Note that P&S WG has recommended changing this criterion to ref ASTM E2147-01.

Comments from Implementation WG:

- These criteria are very high level and vague, though they do explicitly establish information to be captured (date/time, user, patient, and “action taken”).
- We recommend being more explicit in describing the level of how the “action taken” should be captured (what was done, level of specificity viz. data, e.g., status change from/to, record level details, etc.). This level of detail would be necessary for the audit log to be valuable from a medico-legal perspective. Test procedures should address scenarios such as sequential changes to a record (e.g., problem list, medication history) to establish that actions taken can be tracked appropriately.

	EP	EH	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	TPs	WG LEAD(s)	
			Proposed Stage 2 Objective	Proposed Stage 2 Measure							
CORE	23	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest 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 provider's risk management process.			§170.314(d)(4)	None.	NEW	
	<p><b>P&amp;S Workgroup Comments</b></p> <p><b>1) Is a change in the test procedures linked above suggested based on a change in criterion? If “yes,” what is the suggestion?</b>  Yes. This is a new criterion for Stage 2. Need new TP to test capability to append content to a health record and to record the fact that the content was provided by the patient. Also need TP to test capability to append a response to the patient-provided information.  Also need a TP to test the EHR enables a user to replace existing information while preserving original information</p> <p><b>2) Is a change in the test procedures linked above suggested based on either a criterion not considered or an update, advances in technology? If “yes,” what is the suggestion?</b>  N/A</p>										

	EP	EH	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	TPs	WG LEAD(s)	
			Proposed Stage 2 Objective	Proposed Stage 2 Measure							
CORE	24	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest 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 provider's risk management process.			§170.314(d)(5) <u>Automatic log-off</u> . Terminate an electronic session after a predetermined time of inactivity.	None.	<b>Automatic Log-off</b> ( <a href="http://healthcare.nist.gov/docs/170.302.q_AutomaticLogOff_v1.1.pdf">http://healthcare.nist.gov/docs/170.302.q_AutomaticLogOff_v1.1.pdf</a> ):TP consist of one section: Terminate electronic session – evaluates the capability to terminate an electronic sessions after a predetermined time of inactivity – Tester establishes an electronic session; tester verifies that the electronic session has terminated after a predetermined time of inactivity	
	<p><b>P&amp;S Workgroup Comments</b></p> <p>1) Is a change in the test procedures linked above suggested based on a change in criterion? If “yes,” what is the suggestion? No change in criterion.</p> <p>2) Is a change in the test procedures linked above suggested based on either a criterion not considered or an update, advances in technology? If “yes,” what is the suggestion? P&amp;S WG needs to review TP.</p>										

	EP	EH	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	TPs	WG LEAD(s)	
			Proposed Stage 2 Objective	Proposed Stage 2 Measure							
CORE	25	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest 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 provider's risk management process.			§170.314(d)(6) <u>Emergency access</u> . Permit an identified set of users to access electronic health information during an emergency.	None.	<b>Emergency Access</b> ( <a href="http://healthcare.nist.gov/docs/170.302.p_EmergencyAccess_v1.1.pdf">http://healthcare.nist.gov/docs/170.302.p_EmergencyAccess_v1.1.pdf</a> ):TP consist of one section: Assign authorization – evaluates the capability to assign and permit emergency access authorizations and access to electronic health information during an emergency. Tester shall assign emergency access authorization to an existing account; Tester shall perform an authorized action against the account and verify that the authorized action was performed; Tester shall perform an unauthorized action against the account and verify that the unauthorized action was not performed	
	<p><b>P&amp;S Workgroup Comments</b></p> <p>1) Is a change in the test procedures linked above suggested based on a change in criterion? If “yes,” what is the suggestion? No change in criterion.</p> <p>2) Is a change in the test procedures linked above suggested based on either a criterion not considered or an update, advances in technology? If “yes,” what is the suggestion? P&amp;S WG needs to review TP.</p>										

CORE	EP	EH	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	TPs	WG LEAD(s)
			Proposed Stage 2 Objective	Proposed Stage 2 Measure						
26	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest 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 provider's risk management process.			<p>§170.314(d)(7)</p> <p><u>Encryption of data at rest.</u> Paragraph (d)(7)(i) or (d)(7)(ii) must be met to satisfy this certification criterion.</p> <p>(i) If EHR technology manages electronic health information on an end-user device and the electronic health information remains stored on the device after use of the EHR technology on that device has stopped, the electronic health information must be encrypted in accordance with the standard specified in § 170.210(a)(1). This capability must be enabled by default (i.e., turned on) and must only be permitted to be disabled (and re-enabled) by a limited set of identified users.</p> <p>(ii) Electronic health information managed by EHR technology never remains stored on end-user devices after use of the EHR technology on those devices has stopped.</p>	<p>§ 170.210(a)(1) <u>Encryption and decryption of electronic health information. General.</u> 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.</p>	<p><b>General Encryption</b>  <a href="http://healthcare.nist.gov/docs/170.302.u.GeneralEncryption_v1.1.pdf">http://healthcare.nist.gov/docs/170.302.u.GeneralEncryption_v1.1.pdf</a>:TP consist of two sections:</p> <p>Encrypt electronic health information – evaluates the capability to transform electronic health information into an unreadable format using an algorithm from the specified standard. Tester encrypts electronic health information according using a symmetric algorithm; Tester validates that the electronic health information is unreadable</p> <p>Decrypt electronic health information – evaluates the capability to transform electronic health information into a readable format. Tester decrypts the electronic health information using a decryption function; tester validates that the electronic health information is readable</p>	<p>Ken Tarkoff            Carol Diamond            Liz Johnson            Joe Heyman</p>
<p><b>P&amp;S Workgroup Comments</b></p> <p><b>1) Is a change in the test procedures linked above suggested based on a change in criterion? If “yes,” what is the suggestion?</b>            Yes, encryption of data at rest is a new certification criterion for Stage 2. Linked TP is for testing general capability to encrypt. New TPs are needed to test capability to a) encrypt data on end-user device managed by the EHR; and b) remove all data stored on end-user device during EHR session. TPs also are needed to test whether the EHR technology submitted for certification manages any data on end-user devices; if so, the product must meet one of the two criteria (i or ii).</p> <p><b>2) Is a change in the test procedures linked above suggested based on either a criterion not considered or an update, advances in technology? If “yes,” what is the suggestion?</b>            N/A</p>										

	EP	EH	MEANINGFUL USE		NUMERAT OR	DENOMINAT OR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	TPs	WG LEAD(s)
			Proposed Stage 2 Objective	Proposed Stage 2 Measure						
CORE	27	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.			<p>§170.314(d)(8)</p> <p><u>Integrity.</u></p> <p>(i) Create a message digest in accordance with the standard specified in 170.210(c).</p> <p>(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.</p>	<p>§ 170.210(c) <u>Verification that electronic health information has not been altered in transit. Standard.</u> 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.</p>	<p><b>Integrity</b>  <a href="http://healthcare.nist.gov/docs/170.302.s_Integrity_v1.1.pdf">http://healthcare.nist.gov/docs/170.302.s_Integrity_v1.1.pdf</a>:TP consist of three sections:</p> <p><u>Generate hash values</u> – evaluates the capability to generate a hash value. Tester generates two hash values for comparison using Vendor-supplied test data; Tester modifies the Vendor-supplied test data set and generates a hash value for the modified data set</p> <p><u>Compare hash values</u> – evaluates the capability to compare hash values to ensure the electronic health information has not been altered in transit. Tester compares the generated hash values; Tester determines if the hash values are the same or different depending on the data sets</p> <p><u>Generate, Exchange, and Verify</u>– evaluates the capability to generate a hash of health information in accordance with the standard specified in 170.210(c), electronically exchange the health information and the generated message digest to a receiving system, and verify that the electronically exchanged health information has not been altered. Using Vendor-identified functions, Tester generates a message digest of the health information; Using Vendor-identified functions, Tester electronically exchanges the health information and the generated message digest to a receiving system (either a Tester’s receiving system or a vendor-identified system) using the Vendor-identified transport technology of the EHR. This may require configuration on the part of the Tester’s receiving system; Tester verifies that the electronically exchanged health information and generated message digest is the same.</p>	
	<p><b>P&amp;S Workgroup Comments</b></p> <p>1) Is a change in the test procedures linked above suggested based on a change in criterion? If “yes,” what is the suggestion?                      “Detection” deleted from criterion for Stage 2.</p> <p>2) Is a change in the test procedures linked above suggested based on either a criterion not considered or an update, advances in technology? If “yes,” what is the suggestion?                      P&amp;S WG needs to review TP.</p>									

	EP	EH	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	TPs	WG LEAD(s)	
			Proposed Stage 2 Objective	Proposed Stage 2 Measure							
CORE	28	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest 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 provider's risk management process.			§170.314(d)(9)  <u>Optional. Accounting of disclosures.</u> Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in §170.210(d).	§ 170.210(d) <u>Record treatment, payment, and health care operations disclosures.</u> 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.	<p><b>Accounting of Disclosures</b> (<a href="http://healthcare.nist.gov/docs/170.302.w.AccountingDisclosures_v1.1.pdf">http://healthcare.nist.gov/docs/170.302.w.AccountingDisclosures_v1.1.pdf</a>): This test evaluates the capability for a Complete EHR or EHR Module to 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.</p> <p>This test procedure is organized into one section: Record disclosures – evaluates the capability to enter treatment, payment, and health care operations disclosures into the HER. Tester enters the treatment, payment, and health care operations disclosures; Tester validates that the date, time, patient identification, user identification, and a description of the disclosure is recorded for each disclosure</p>	
	<p><b>P&amp;S Workgroup Comments</b></p> <p><b>1) Is a change in the test procedures linked above suggested based on a change in criterion? If “yes,” what is the suggestion?</b> No change in criterion.</p> <p><b>2) Is a change in the test procedures linked above suggested based on either a criterion not considered or an update, advances in technology? If “yes,” what is the suggestion?</b> Given that final rule on accounting of disclosures has not been issued, no change to this TP should be warranted.</p>										