Test Procedure for §170.302 (p) Emergency Access

This document describes the draft test procedure for evaluating conformance of complete EHRs or EHR modules[1] to the certification criteria defined in 45 CFR Part 170 Subpart C of the Final Rule for Health Information Technology: Initial Set of standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology as published in the Federal Register on July 28, 2010. The document[2] is organized by test procedure and derived test requirements with traceability to the normative certification criteria as described in the Overview document located at http://healthcare.nist.gov/docs/TestProcedureOverview_v1.pdf. The test procedures may be updated to reflect on-going feedback received during the certification activities.

The HHS/Office of the National Coordinator for Health Information Technology (ONC) has defined the standards, implementation guides and certification criteria used in this test procedure. Applicability and interpretation of the standards, implementation guides and certification criteria to EHR technology is determined by ONC. Test procedures to evaluate conformance of EHR technology to ONC's requirements are defined by NIST. Testing of EHR technology is carried out by ONC-Authorized Testing and Certification Bodies (ATCBs), not NIST, as set forth in the final rule establishing the Temporary Certification Program (*Establishment of the Temporary Certification Program for Health Information Technology, 45 CFR Part 170; June 24, 2010*.)

Questions about the applicability of the standards, implementation guides or criteria should be directed to ONC at ONC.Certification@hhs.gov. Questions about the test procedures should be directed to NIST at hit-tst-fdbk@nist.gov. Note that NIST will automatically forward to ONC any questions regarding the applicability of the standards, implementation guides or criteria. Questions about functions and activities of the ATCBs should be directed to ONC at ONC.Certification@hhs.gov .

Certification Criteria

This Certification Criterion is from the Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology Final Rule issued by the Department of Health and Human Services (HHS) on July 28, 2010.

§170.302(p) Emergency Access. Permit authorized users (who are authorized for emergency situations) to access electronic health information during an emergency.

Per Section III.D of the preamble of the Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, Final Rule where the emergency access certification criterion is discussed:

[1] Department of Health and Human Services, 45 CFR Part 170 Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, Final Rule, July 28, 2010

[2] Disclaimer: Certain commercial products are identified in this document. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology.

- "We have adopted certification criteria to ensure that Certified EHR Technology includes certain capabilities, in this case that Certified EHR Technology be capable of permitting authorized users to access electronic health information during an emergency. The criterion is not intended to specify what constitutes an emergency or who would be authorized to access electronic health information in an emergency. In a medical emergency, those determinations would be made under specific factual circumstances and in accordance with applicable state and federal laws, organizational policies and procedures, and the relevant standard of care.
  With respect to emergency access, we note that HHS stated in the HIPAA Security Final Rule (68 FR 8355): 'We believe that emergency access is a necessary part of access controls and, therefore, is properly a required implementation specification of the ''Access controls'' standard. Access controls will still be necessary under emergency conditions, although they may be very different from those used in normal operational circumstances. For example, in a situation when normal environmental systems, including electrical power, have been severely damaged or rendered inoperative due to a natural or manmade disaster, procedures should be established beforehand to provide guidance on possible ways to gain access to needed electronic protected health information.'"
- "Some commenters appeared to interpret our reference to "emergency" in "emergency access" as solely constituting a clinical or life threatening emergency related to a patient for which access would be required. We believe that emergency could encompass that scenario, as well as a broader range of possibilities, including normal patient care when timely access to electronic health information becomes critical. Therefore, we have not sought to limit the development of emergency access capabilities for Certified EHR Technology to a particular scenario."

INFORMATIVE TEST DESCRIPTION

This section provides an informative description of how the test procedure is organized and conducted. It is not intended to provide normative statements of the certification requirements.

This test evaluates the capability for a Complete EHR or EHR Module to assign and permit emergency access authorizations and access to electronic health information during an emergency. The Vendor supplies the test data for this test procedure. The test data should consist of emergency and non-emergency test scenarios.

This test procedure consists of one section:

- <u>Assign authorization</u> – 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

Referenced Standards

None

Normative Test Procedures

Derived Test Requirements

DTR170.302.p – 1: Assign authorization

DTR170.302.p – 1: Assign authorization

Required Vendor Information

VE170.302.p – 1.01: The Vendor shall identify the EHR function(s) that are available to assign emergency access authorizations to user accounts

VE170.302.p – 1.02: The Vendor shall provide all necessary test data, including an existing user account, and emergency and non-emergency access scenarios

Required Test Procedure:

TE170.302.p – 1.01: Using the Vendor-identified EHR function(s), the Tester shall assign emergency access authorizations to an existing account

TE170.302.p – 1.02: In a non-emergency access scenario, the Tester shall perform an action authorized by the assigned emergency access authorizations

TE170.302.p – 1.03: The Tester shall verify that the emergency access was not permitted

TE170.302.p – 1.04: In an emergency access scenario, the Tester shall perform an action authorized by the assigned emergency access authorizations

TE170.302.p – 1.05: The Tester shall verify that the emergency access was permitted

Inspection Test Guide

IN170.302.p – 1.01: Tester shall verify that emergency access authorizations were assigned to an existing account

IN170.302.p – 1.02: Tester shall verify that authorized actions performed were permitted

IN170.302.p – 1.03: Tester shall verify that unauthorized actions performed were not permitted

Test Data

This Test Procedure requires the vendor to supply the test data. The Tester shall address the following:

- Vendor-supplied test data shall ensure that the functional and interoperable requirements identified in the criterion can be adequately evaluated for conformance
- Vendor-supplied test data shall strictly focus on meeting the basic capabilities required of an EHR relative to the certification criterion rather than exercising the full breadth/depth of capability that an installed EHR might be expected to support

- Tester shall record as part of the test documentation the specific Vendor-supplied test data that was utilized for testing

CONFORMANCE TEST TOOLS

None

Document History

Version Number	Description of Change	Date Published
0.2	Original draft version	April 9, 2010
1.0	Updated to reflect Final Rule	July 21, 2010
1.0	Updates include: • removed “Pending” in header • resolved numbering typographical error	August 13, 2010