Test Procedure for §170.314(d)(6) Emergency access

This document describes the test procedure for evaluating conformance of electronic health record (EHR) technology to the certification criteria defined in 45 CFR Part 170 Subpart C of the Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology, Final Rule. The document[1] 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://www.healthit.gov/certification (navigation: 2014 Edition Test Method). The test procedures may be updated to reflect on-going feedback received during the certification activities.

The Department of Health and Human Services (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. Testing of EHR technology in the Permanent Certification Program, henceforth referred to as the ONC Health Information Technology (HIT) Certification Program[2], is carried out by National Voluntary Laboratory Accreditation Program (NVLAP)-Accredited Testing Laboratories (ATLs) as set forth in the final rule establishing the Permanent Certification Program (*Establishment of the Permanent Certification Program for Health Information Technology, 45 CFR Part 170; February 7, 2011*).

Questions or concerns regarding the ONC HIT Certification Program should be directed to ONC at ONC.Certification@hhs.gov.

CERTIFICATION CRITERION

This certification criterion is from the Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology, Final Rule issued by the Department of Health and Human Services (HHS) on September 4, 2012. This certification criterion is included in the definition of a Base EHR.

§170.314(d)(6) Emergency Access. Permit an identified set of users to access electronic health information during an emergency.

Per Section III.A of the preamble of the Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions

[1] Disclaimer: Certain commercial products may be identified in this document. Such identification does not imply recommendation or endorsement by ONC.

[2] Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology, Final Rule.

to the Permanent Certification Program for Health Information Technology, Final Rule, the 2014 Edition of this certification criterion is classified as unchanged with refinements from the 2011 Edition. This certification criterion meets the three factors of unchanged certification criteria: (1) the certification criterion includes only the same capabilities that were specified in previously adopted certification criteria, (2) the certification criterion's capabilities apply to the same setting as they did in previously adopted certification criteria, and (3) the certification criterion remains designated as "mandatory," or it is re-designated as "optional," for the same setting for which it was previously adopted certification criterion.

2014 EDITION PREAMBLE LANGUAGE

Per Section III.A of the preamble of the Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology, Final Rule (September 4, 2012) where the emergency access certification criterion is discussed:

- "The clarifying language…as well as our prior responses to comments included in the S&CC July 2010 Final Rule (75 FR 44617) for the 2011 Edition version of this certification criterion provide ample specificity for EHR technology developers. They also include for the benefit of commenters the citation to the HIPAA Security Rule requirement on which this certification criterion is modeled (68 FR 8355)."
- "We explained that the purpose of this certification criterion is to provide certain users ("identified set of users") with the ability to override normal access controls in the case of an emergency."

2011 EDITION PREAMBLE LANGUAGE

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 (July 28, 2010) where the emergency access certification criterion is discussed:

- "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."

CHANGES FROM 2011 TO 2014 EDITION

Per Section III.A of the preamble of the Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 2014 Edition; Revisions to the Permanent Certification Program for Health Information Technology, Final Rule (September 4, 2012) where the emergency access certification criterion is discussed:

- "We proposed to remove the parenthetical "who are authorized for emergency situations" from the certification criterion and include the phrase "identified set of users."

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 EHR technology 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:

- 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

REFERENCED STANDARDS

None

NORMATIVE TEST PROCEDURES

Derived Test Requirements

DTR170.314(d)(6) – 1: Assign Authorization

DTR170.314(d)(6) – 1: Assign Authorization

Required Vendor Information

VE170.314(d)(6) – 1.01: The Vendor shall identify the EHR function(s) that are available to assign emergency access authorizations to user accounts

VE170.314(d)(6) – 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

TE170.314(d)(6) – 1.01: Using the Vendor-identified EHR function(s), the Tester shall assign emergency access authorizations to an existing account

TE170.314(d)(6) – 1.02: In a non-emergency access scenario, the Tester shall perform an action authorized by the assigned emergency access authorizations

TE170.314(d)(6) – 1.03: The Tester shall verify that the emergency access was not permitted

TE170.314(d)(6) – 1.04: In an emergency access scenario, the Tester shall perform an action authorized by the assigned emergency access authorizations

TE170.314(d)(6) – 1.05: The Tester shall verify that the emergency access was permitted

Inspection Test Guide

IN170.314(d)(6) – 1.01: Tester shall verify that emergency access authorizations were assigned to an existing account

IN170.314(d)(6) – 1.02: Tester shall verify that authorized actions performed were permitted

IN170.314(d)(6) – 1.03: Tester shall verify that unauthorized actions performed were not permitted

TEST DATA

The Vendor shall supply the test data for this test procedure.

Vendor-supplied test data shall focus on meeting the basic capabilities required of EHR technology relative to the certification criterion rather than exercising the full breadth/depth of capability that installed EHR technology might be expected to support.

The test procedures require that the Tester enter the applicable test data into the EHR technology being evaluated for conformance. The intent is that the Tester fully controls the process of entering the test

data in order to ensure that the data are correctly entered as specified in the test procedure. If a situation arises where it is impractical for a Tester to directly enter the test data, the Tester, at the Tester's discretion, may instruct the Vendor to enter the test data, so long as the Tester remains in full control of the testing process, directly observes the test data being entered by the Vendor, and validates that the test data are entered correctly as specified in the test procedure.

For Vendor-supplied test data, the Tester shall address the following:

- Vendor-supplied test data shall ensure that the 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	Date Published
1.0	Released for public comment	September 14, 2012
1.1	Delivered for National Coordinator Approval	December 4, 2012
1.2	Posted Approved Test Procedure	December 14, 2012