# Test Criteria: 170.315.d.6 – Emergency Access

|  |  |
| --- | --- |
| **Testing Result** |  |
| Participant and Product-with-version |  |
| Setting (Ambulatory or Inpatient) |  |
| Test Proctor |  |
| Test Date |  |
| Test Result | Pass:  Fail:  No Attempt: |
| Error Description (if applicable) |  |
| Modifications to Product Under Test |  |
| Additional Software Used |  |
| Additional Proctor Notes |  |

### Overview

In this document you will find:

* [Test Data and Test Tools](#_Test_Data_and)
* [Standards Support](#_Demonstrate_Standards_Support)
* [Drummond Test Report (Instructions, Expected Results, Points to Remember)](#_170.315(d)(6)_Emergency_Access)
* [Test Procedures](#_Test_Procedure)
* [Appendix A: Testing Guide](#_Appendix_A:_Testing)
* [Appendix B: ONC Criteria](#_Appendix_B:_ONC)

### Version of ONC Test Method

1.0

### Scope of Proctoring Sheet

The ONC test method associated with this criterion is the only approved test method for EHR Meaningful Use certification. This Proctoring Sheet is not a replacement test method but a test procedure document for performing the ONC test method and recording the results. Proctoring Sheet describe test data, test criteria and expected results. It is assumed the Health IT developer or Participant under Test is familiar with the associated ONC test method.

# Robustness and Reliability Requirement

To satisfy the module criteria, it is expected that the Product-Under-Test is able to complete the testing requirements reliably, including repeat testing with the same result without error, and with a satisfactory level of robustness. This includes unexpected error messages produced through normal operation, multiple unintended restarts of the application or any other “buggy” facets of the product displayed while testing. These errors are record in the Additional Proctor Notes of the proctor sheet. Lack of reliability and robustness of design will result in failure of the module.

# Test Data and Tools

|  |  |
| --- | --- |
| **Test Data Source:** | ONC-Supplied  DG-Supplied:  Developer-Supplied: |
| **Pre-Test Data Setup:**  Not applicable. | |
| **Test Data:**  Developer-supplied. | |
| **Test Tools:**  Not applicable. | |

# Demonstrate Standards Support

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:** There are no standards required for this criterion. | |

# 170.315(d)(6) Emergency Access Configuration

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **P&S applies to all criteria:** | YES:  NO: |
| **If not, list applicable criteria:** |  |
| **Brief description of emergency access procedure:** |  |
| **Instructions:**   * Emergency access authorizations are limited to a set of identified users. * Enable emergency access for identified user and demonstrate user can access health information during an emergency. * Demonstrate authorized emergency access users can access health information and only during an emergency and NOT during a non-emergency. * Demonstrate unauthorized emergency access users cannot access health information during an emergency. | |
| **Expected Test Result:**   * Permit an identified set of users to access electronic health information during an emergency. * Emergency access authorization is limited to a set of identified users and assigned to an identified user. * User with emergency access authorization can only access health information in an emergency, and NOT during a non-emergency. * User NOT having emergency access authorization cannot access health information during an emergency. | |
| **Points to Remember:**   * This module is eligible for gap certification. * See “[EHR Test-125] Privacy and Security Framework” document provided by Drummond Group to verify instructions on submitting required P&S attestation. | |

### Test Procedure

### 1.1Emergency Scenario Description

|  |  |
| --- | --- |
|  | Health IT developer describes emergency access procedure. Proctor records procedure in designated section above. |
|  | Health IT developer creates, or identifies, an authorized user without emergency access. |
|  | Authorized user (without emergency access) logs in when it is not an emergency and demonstrates inability to perform developer-identified actions authorized for emergency access. |
|  | Health IT developer assigns authorized user emergency access role/permission. |
|  | Authorized user enables, or invokes, emergency access scenario (e.g., break the glass). |
|  | Authorized user demonstrates emergency access now active and performs developer-identified actions during an emergency scenario. |
|  | Unauthorized user (user without emergency access) logs in but cannot perform developer-identified actions during an emergency scenario. |

<INSERT SCREEN SHOTS>

**1.2 Privacy and Security Attestation**

|  |  |
| --- | --- |
|  | Health IT Developer submits Privacy and Security Framework document attesting to the approach used for certification testing. Additionally, attestation must specify if the criteria demonstrated in this test event applies to *all* certified modules or only specific modules. See “[EHR Test-128] Privacy Security Framework” provided by Drummond Group. |

<ATTACH or INSERT LINK TO DOCUMENTATION>

# Appendix A: Testing Guide

*This appendix contains more details and background on the testing requirements, including explanation on underlying standards, notable issues and best practice suggestions.*

Rev 01-Aug-2016 Additions

* Emergency access is part of a Health IT' Module's general access control and should be established before the emergency, potentially as a “pre-set” function. The goal of the capability is to ensure that there is a way for identified users to have access (e.g., by elevating their access privileges) in an emergency to gain or maintain access to patient health information, which should be an auditable event. In sum, the "emergency access" functionality should be demonstrated based on the access rules already built into the Health IT Module.
* Emergency access is intended to cover a broad range of scenarios, including life threatening emergencies related to the patient as well as normal patient care where timely access to electronic health information becomes critical.

Rev 01-Mar-2016 Additions

* The criterion is not intended to specify what constitutes an emergency or who would be authorized to access electronic health information in an emergency. Those determinations should be made with applicable state and federal laws, organizational policies and procedures, and the relevant standard of care. Likewise, an “emergency” is not limited to clinical or life threatening emergencies but could include other scenarios such as those related to normal patient care when timely access to electronic health information becomes critical.

# Appendix B: ONC Criteria and Standards

*This appendix contains copy of the relevant ONC criteria and standards for this proctor sheet as a reference. In the event of a discrepancy with the ONC Final Rule, the ONC Final Rule takes precedence.*

**§170.315(d)(6) Emergency Access.**

Permit an identified set of users to access electronic health information during an emergency.

# Change Log

|  |  |
| --- | --- |
| Revision | Change Description |
| 01-Nov-2016 | Created test step for unauthorized user without emergency access and distinguish between authorized and unauthorized users. |
| 01-Sept-2016 | Updated test procedures to clarify emergency access is invoked by user (e.g, break the glass) and not with any additional intervention by health IT developer or admin-type user. |
| 01-Aug-2016 | Added clarifications under “Appendix A: Testing Guide”. |
| 01-July-2016 | Re-numbered sections. Added section 1.2 for Privacy and Security attestation. |
| 01-Jun-2016 | Added text boxes to indicate if this P&S module applies to all certified criteria and reference to the attestation based on “Privacy and Security Framework” document. |
| 01-Mar-2016 | Initial Release. |
|  |  |
|  |  |

**About Drummond Group LLC**

Drummond Group LLC is a global software test and certification lab that serves a wide range of vertical industries.  In healthcare, Drummond Group tests and certifies Controlled Substance Ordering Systems (CSOS), Electronic Prescription of Controlled Substances (EPCS) software and processes, and Electronic Health Records (EHRs) – designating the trusted test lab as the only third-party certifier of all three initiatives designed to move the industry toward a digital future. Founded in 1999, and accredited for the Office of the National Coordinator Health IT Certification Program as an Authorized Certification Body (ACB) and an Authorized Test Lab (ATL), Drummond Group continues to build upon its deep experience and expertise necessary to deliver reliable and cost-effective services. For more information, please visit <http://www.drummondgroup.com> or email [ehr@drummondgroup.com](mailto:ehr@drummondgroup.com)

END OF DOCUMENT