# Test Criteria: 170.315.e.2 – Secure Messaging

|  |  |
| --- | --- |
| **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(e)(2)_Secure_Messaging)
* [Test Procedures](#_Test_Procedures_1)
* [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:**  Health IT developer configures messaging accounts for:   * + SM-User1: Non-patient, authenticated HIT Module user (provider or hospital user)   + SM-User2: Patient (authenticated HIT Module user or external messaging)   + SM-User3: An unauthenticated user (non-existent) | |
| **Test Data:**  Developer-supplied. | |
| **Test Tools:**  Not applicable. | |

# Demonstrate Standards Support

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:** Implement standards to demonstrate secure messaging. | |

|  |  |  |
| --- | --- | --- |
|  | **Standard** | By reference to required privacy and security 170.315(d)(9) module: |
|  | 170.210(a)(2) | [Annex A: Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, October 8, 2014](http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf) |
|  | 170.210(c)(2) | [FIPS PUB 180-4, Secure Hash Standard, 180-4 (August 2015)](http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf) |

# 170.315(e)(2) Secure Messaging

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Authentication Method:** |  |
| **Encryption Algorithm:** |  |
| **Hashing Algorithm:** |  |
| **Instructions:**   * Health IT developer identifies encrypting and hashing technologies used. * Authenticated user sends/receives secure message to/from an authenticated patient. | |
| **Expected Test Result:**   * Enable a user to send messages to, and receive messages from, an authenticated patient in a secure manner. * Sending/receiving securely using hashing level of at least SHA2 is utilized and encryption algorithm specified by Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2 to store electronic health information from the EHR technology on an end-user device. * Unauthenticated users cannot access HIT Module functionality for sending secured messages. * Unauthenticated users cannot read secure messages sent to authenticated patients. | |
| **Points to Remember:**   * Secure email, a secure portal, even some type of mobile application could all be examples for secure messaging methods that could potentially meet this certification criterion. * A Health IT Module presented for certification to this criterion must be separately tested to the privacy and security criterion for “trusted connection” at § 170.315(d)(9). A health IT developer can choose between message-level or transport-level “trusted connection” certification in accordance with §170.315(d)(9). * While the ONC certification criteria does not require the testing of the patient’s authorized representative for (315.e.2) Secure Messaging, the CMS program permits providers to use this method for this measure objective. | |

### Test Procedures

**1.1 Secure Messaging: Patient**

|  |  |
| --- | --- |
|  | Health IT developer identifies authentication method, hashing algorithm, and encryption algorithms. Proctor records in designated sections above. |
|  | Authenticated provider-type user (SM-User1) sends a secure message to an authenticated test patient (SM-User2). |
|  | Test patient (SM-User2) receives message from provider-type user (SM-User1). |
|  | Test patient (SM-User2) sends messages to provider-type user (SM-User1). |
|  | Provider-type user (SM-User1) receives messages from test patient (SM-User2). |

<INSERT SCREEN SHOT – Secure trusted connection established to patient OR BRIEF DESCRIPTION – If encryption and hashing process is not easily captured through screen shot, Proctor will attest to the method of encryption/decryption>

<INSERT SCREEN SHOT – Provider-type user sending message to patient>

<INSERT SCREEN SHOT – Patient receives message from provider-type user>

<INSERT SCREEN SHOT – Patient sending message to provider-type user>

<INSERT SCREEN SHOT – Provider-type user receives message from patient>

**1.2 Secure Messaging: Non-Existent User**

|  |  |
| --- | --- |
|  | Authenticated provider-type user (SM-User1) attempts to send a secure message to a non-existent user (SM-User4). |
|  | Provider-type user (SM-User1) is notified that attempts to send to a non-existent user are unsuccessful. |

<INSERT SCREEN SHOTS – Non-existent User Notification>

# 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-Mar-2016 Additions

* The encryption requirements of this certification criterion only apply to the message content and not to the patient’s device(s).
* This criterion is not eligible for gap certification as the new hashing standard (a hashing algorithm with a security strength equal to or greater than SHA-2) applies to this criterion per the standard required at § 170.210(c)(2).
* Secure email, a secure portal, even some type of mobile application could all be examples for secure messaging methods that could potentially meet this certification criterion.
* We will test that the health IT has the capability as a whole to send and receive secure messages for certification in order for providers to have assurance that health IT can enable bidirectional communication.
* As noted in Annex A: FIPS 140-2, only encryption and hashing algorithms are in scope for this certification criterion. Random number generator standards are not in scope.

# 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(e)(2) Secure Messaging.**

Enable a user to send messages to, and receive messages from, a patient in a secure manner.

**Standards required for § 170.315(d)(9) Trusted connection:**

* 170.210(a)(2) [Annex A: Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, October 8, 2014](http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf)
* 170.210(c)(2) [FIPS PUB 180-4, Secure Hash Standard, 180-4 (August 2015)](http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf)

# Change Log

|  |  |
| --- | --- |
| Revision | Change Description |
| 01-Dec-2016 | Removed test steps involving authorized representative to align with ONC test procedure. Added comment about authorized representative as it relates to CMS program in Appendix A. |
| 01-Oct-2016 | Added screenshot placeholder for secure trusted connection. |
| 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