# Test Criteria: 170.315.d.9 – Trusted Connection

|  |  |
| --- | --- |
| **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.9_(i)_–)
* [Test Procedures](#_Test_Procedures)
* [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 supplies authorized user and patient test data as needed to demonstrate Trusted Connection functionality. | |
| **Test Tools:**   * Not applicable. | |

# Demonstrate Standards Support

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:** Verify health IT module supports the required standards. See “Appendix B” for further details. | |

|  |  |  |
| --- | --- | --- |
|  | **Standard** |  |
|  | §170.210(a)(2) | Encryption and decryption of electronic health information. [Annex A: Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, October 2014](http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf) |
|  | §170.210(c)(2) | Encryption and decryption of electronic health information. A hashing algorithm with a security strength equal to or greater than SHA-2 as specified by NIST in [FIPS Publication 180-4, Secure Hash Standard, 180-4 (August 2015)](http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf). |

# 170.315.d.9 (i) – Trusted Connection: Message-level

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **P&S applies to all criteria:** | YES:  NO: |
| **If not, list applicable criteria:** |  |
| **Encryption and Hashing Algorithm:** |  |
| **Instructions:**   * Health IT developer uses the HIT module to send/receive encrypted and integrity protected messages. | |
| **Expected Test Result:**   * Encrypt and integrity protect message contents in accordance with the standards specified at §170.210(a)(2) and §170.210(c)(2). * Demonstrate either through visual inspection or through system documentation that all messages sent are in conformance to standards §170.210(a)(2) and (c)(2). * Message digest electronically exchanged by the sending HIT Module matches the message digest created on the health data in the receiving system. | |
| **Points to Remember:**   * **Health IT developer must test either Message-level or Transport-level**. Please note a separate privacy and security attestation is still required even if testing message-level. * See “[EHR Test-128] Privacy and Security Framework” document provided by Drummond Group to verify instructions on submitting required P&S attestation. * §170.315(d)(9) must be explicitly demonstrated with § 170.315(e)(1) and (e)(2) because of the specific capabilities for secure electronic transmission and secure electronic messaging included in each of these two criteria, respectively. For the other certification criteria (§ 170.315(e)(3), (g)(7), (g)(8), and (g)(9)), this criterion at §170.315(d)(9) only needs to be demonstrated once as part of the overall scope of the certificate sought. | |

### Test Procedures

**1.1 Privacy and Security Attestation**

|  |  |
| --- | --- |
|  | Health IT Developer submits Privacy and Security Framework document attesting to the approach used for certification testing. See “[EHR Test-128] Privacy Security Framework” provided by Drummond Group. Attestation must specify which criteria this demonstration applies to. *At a minimum, Trusted Connection (d.9) must be tested separately for §170.315(e)(1) and (e)(2).* *Additional testing of (d.9) may be conducted, if applicable.* |

<INSERT LINK TO DOCUMENTATION>

### 1.2 Message-Level: Demonstrate Electronically Exchanged Message Digest

|  |  |
| --- | --- |
|  | User identifies the encryption and hashing algorithms used. Proctor records in designated section above. |
|  | Health IT module encrypts and integrity protects message contents including generating a message digest over patient health data using SHA-2 or greater. |
|  | User electronically transmits both the patient health data file and the message digest to a receiving system (e.g., Proctor’s PC or receiving system set up by developer). |
|  | Proctor verifies message is sent in conformance with the encryption and hashing algorithm identified by the developer. Computes message digest over the received patient health data and verifies it matches message digest generated by Health IT module. |
|  | Proctor generates message digest for a DG-supplied test data file and electronically transmits to health IT developer. |
|  | Within health IT module, user generates message digest over the received patient health data. |
|  | Proctor verifies message digest generated by health IT module matches message digest computed by Proctor. |

<INSERT SCREEN SHOTS OR ATTACH FILES>

# 170.315.d.9 (ii) – Trusted Connection: Transport-level

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **P&S applies to all criteria:** | YES:  NO: |
| **If not, list applicable criteria:** |  |
| **Encryption and Hashing Algorithm:** |  |
| **Instructions:**   * Health IT developer uses the HIT functionality to establish a trusted connection. | |
| **Expected Test Result:**   * Establish a trusted connection in accordance with the standards specified at §170.210(a)(2) and §170.210(c)(2). * Demonstrate either through visual inspection or via documentation that a trusted connection is established in conformance to standards §170.210(a)(2) and (c)(2). * Message digest electronically exchanged by the sending HIT Module matches the message digest created on the health data in the receiving system. | |
| **Points to Remember:**   * **Health IT developer must test either Message-level or Transport-level**. * Inspection of the certificate and encryption connection through a browser, or use of a network analyzer to inspect the packets involved in the encryption handshake are both acceptable methods for verification. * §170.315(d)(9) must be explicitly demonstrated with §170.315(e)(1) and (e)(2) because of the specific capabilities for secure electronic transmission and secure electronic messaging included in each of these two criteria, respectively. For the other certification criteria (§ 170.315(e)(3), (g)(7), (g)(8), and (g)(9)), this criterion at §170.315(d)(9) only needs to be demonstrated once as part of the overall scope of the certificate sought. * See “[EHR Test-128] Privacy and Security Framework” document provided by Drummond Group to verify instructions on submitting required P&S attestation | |

### Test Procedures

**2.1 Privacy and Security Attestation**

|  |  |
| --- | --- |
|  | Health IT Developer submits Privacy and Security Framework document attesting to the approach used for certification testing. See “[EHR Test-128] Privacy Security Framework” provided by Drummond Group. Attestation must specify which criteria this demonstration applies to. *At a minimum, Trusted Connection (d.9) must be tested separately for §170.315(e)(1) and (e)(2).* *Additional testing of (d.9) may be conducted, if applicable.* |

<ATTACH or LINK DOCUMENTATION>

### 2.1Transport-Level: Trusted Connection

|  |  |
| --- | --- |
|  | Health IT developer identifies the encryption and hashing algorithms used. Proctor records in designated section above. |
|  | Health IT module establishes at least one trusted connection in accordance with §170.210(a)(2) and (c)(2). |
|  | Proctor views the encryption handshake to ensure that the digital certificates are being invoked during the connection. |

<INSERT SCREENSHOTS>

# 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-Apr-2016 Additions

* Developers have freedom to demonstrate the encryption handshake based on the technology they are using. For example, if a developer has a browser-based module that uses HTTP, the developer could demonstrate the "lock" icon in the browser that indicates that HTTP is present and working properly.

Rev 01-Mar-2016 Additions

* Health IT needs to provide a level of trusted connection using either 1) encrypted and integrity message protection or 2) a trusted connection for transport. Either of these methods must be demonstrated in accordance with the following standards: Annex A: FIPS Publication 140-2, Security Requirements for Cryptographic Modules and FIPS PUB 180-4, Secure Hash Standard, 180-4.
* A “trusted connection” means the link is encrypted/integrity protected according to § 170.210(a)(2) or (c)(2). As such, we do not believe it is necessary to specifically name HTTPS and/or SSL/TLS as this standard already covers encryption and integrity protection for data in motion.

# 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.*

**§170.314(d)(9) Trusted Connection.**

Establish a trusted connection using one of the following methods:

(i) Message-level. Encrypt and integrity protect message contents in accordance with the standards specified in § 170.210(a)(2) and (c)(2).

(ii) Transport-level. Use a trusted connection in accordance with the standards specified in §170.210(a)(2) and (c)(2).

**§170.210(a)(2) Encryption and decryption of electronic health information.**

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](http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf), October 8, 2014

**§170.210(c)(2) Encryption and decryption of electronic health information.**

A hashing algorithm with a security strength equal to or greater than SHA-2 as

specified by NIST in [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 | Updated Message Level test section 1.2 to include encrypting message content in addition to integrity protecting. |
| 01-July-2016 | Re-numbered sections. Removed “documentation” sections and replaced with sections further describing Privacy and Security attestation (1.1 and 2.1). |
| 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-Apr-2016 | Added clarification regarding encryption demonstration under Appendix A. |
| 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