# Test Criteria: 170.315.d.8 Integrity

|  |  |
| --- | --- |
| **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)](#_DTR_170.315(d)(8)_Integrity)
* [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:**  Health IT developer prepare patient health data file to generate message digest over. | |
| **Test Data:**  Developer-supplied and DG-supplied test data files. | |
| **Test Tools:**  Not applicable. | |

# Demonstrate Standards Support

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:** Health IT module needs to support FIPS 180-4 SHA-2 or greater. | |

|  |  |  |
| --- | --- | --- |
|  | **Standard** |  |
|  | §170.210(c)(2) | Hashing algorithm 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)(8) Integrity

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **P&S applies to all criteria:** | YES:  NO: |
| **If not, list applicable criteria:** |  |
| **Instructions:**   * User generates a hash over a message containing health information using health IT module functionality and sends message to Proctor for validation. * Health IT module receives electronically exchanged health information and validates message digest. | |
| **Expected Test Result:**   * Health IT module creates a hash (SHA-2 or greater) on a message in accordance with standard specified in §170.210(c)(2) which can then be verified by a receiver. * Health IT module must be able to verify in accordance with a hashing algorithm with security strength equal or greater than SHA-2 that information has not been altered or changed in any way. | |
| **Points to Remember:**   * Must test (d.8) in conjunction with Transition of Care (b.1) criteria. If not seeking certification to (b.1) then testing for should be in conjunction with any other Care Coordination (b.\*) criteria. If developer is not seeking certification to any (b.\*) criteria, then developer may test (d.8) any time they choose. * See “[EHR Test-128] Privacy and Security Framework” document provided by Drummond Group to verify instructions on submitting required P&S attestation. | |

### Test Procedures

**1.1 Integrity – Create message digest and transmit**

|  |  |
| --- | --- |
|  | Health IT module generates a message digest over patient health data using SHA-2 or greater and then electronically transmits both the patient health data file and the message digest to the Proctor. |
|  | Proctor computes message digest over the received patient health data and verifies it matches message digest provided by Health IT module. |

<INSERT SCREEN SHOT OR ATTACH FILE>

**1.2 Integrity – Verify upon receipt of electronically exchanged health information**

|  |  |
| --- | --- |
|  | 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 SHOT OR ATTACH FILE>

**1.3 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-Mar-2016 Additions

* The Health IT developer will need to provide the test data/file and the hash to the Proctor so that the Proctor can confirm the hash by computing the test data/file on a separate hashing tool, like HashCalc or other similar hashing evaluation tools. A separate hashing tool besides the health IT module must be used to verify the hash created by the health IT module under test.
* This criterion is intended to support the HIPAA Security Rule implementation specification provided at 45 CDR 164.312(e)(2)(i) “[i]mplement security measures to ensure the electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.” Besides this certification criterion specifies a capability that certified health IT must include, we do not believe that it is necessary or appropriate for us to address whether hashing is applicable to public and private networks.
* The 2015 Edition final rule does not require health IT developers to get their products certified to the SHA-2 requirement immediately, and we would expect health IT developers to not begin seeking certification to this criterion until later in 2016 for implementation in 2017 and 2018.
* Certification only ensures that a health IT module can create hashes using SHA-2. For example, users of certified health IT may find it appropriate to continue to use SHA-1 for backwards compatibility if their security risk analysis justifies the risk.

# 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)(8) Integrity.** (i) Create a message digest in accordance with the standard specified in § 170.210(c)(2).

(ii) Verify in accordance with the standard specified in § 170.210(c)(2) upon receipt of electronically exchanged health information that such information has not been altered.

**§ 170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.**

(c) Hashing of electronic health information. (2) Standard. A hashing algorithm with a security strength equal to or greater than SHA-2 as specified by NIST in FIPS Publication 180-4 (August 2015) (incorporated by reference in § 170.299).

# Change Log

|  |  |
| --- | --- |
| Revision | Change Description |
| 03-Apr-2017 | Added clarification that (d.8) must be tested with (b.\*) criteria. |
| 01-July-2016 | Added section 1.3 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