# Test Criteria: 170.315.d.7 – End-User Device Encryption

|  |  |
| --- | --- |
| **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)(7)_End-User_Device)
* [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-supplied. | |
| **Test Tools:**  Not applicable. | |

# Demonstrate Standards Support

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:** Implement standard to demonstrate end-user device encryption. For additional references, click [here](https://www.healthit.gov/policy-researchers-implementers/meaningful-use-stage-2-0/standards-hub) for the ONC Standards Hub. | |

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

# 170.315(d)(7) End-User Device Encryption – Alternative I

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Encryption Algorithm:** |  |
| **Authorized Users for disabling default encryption setting:** |  |
| **Instructions:**   * Health IT developer must test to one of the methods specified:  1. Demonstrates electronic health information locally stored on end-user device is encrypted after use of technology on the device stops. 2. Demonstrate electronic health information is NOT locally stored on end-user device after use of technology on the device stops. | |
| **Expected Test Result:**   * If technology is designed to prevent electronic health information from being locally stored on end-user device, skip and go to next section “170.315(d)(7) End-User Device Encryption Alternative II” below. * If technology is designed to locally store electronic health information on end-user devices, it must encrypt the electronic health information stored on those devices. This will be demonstrated by: * Health IT developer submits documentation specifying EHR encryption functions utilizes an 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. * If the health IT module relies on a third party solution, health IT developer submits supporting documentation that demonstrates that the third party solution encryption function utilizes an encryption algorithm specified by Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2 to locally store electronic health information from the health IT module technology on end-user devices. * Encryption configuration setting is enabled by default. * Default encryption configuration cannot disabled or changed. If it can, then this is limited to a set of users. * Unauthorized user cannot disable or change encryption default settings. | |
| **Points to Remember:**   * This module is eligible for gap certification. * 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 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>

### 1.2 Alternative I: Electronic Health Information Stored on End-User Device

|  |  |
| --- | --- |
|  | Using the framework document referenced above, health IT developer attests EHR utilizes an encryption algorithm specified by Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2 (<http://csrc.nist.gov/groups/STM/cmvp/standards.html>) to locally store electronic health information from the EHR technology on end-user devices. |

<ATTACH or INSERT LINK TO DOCUMENTATION>

### 1.3Alternative I: Encryption Default Settings

|  |  |
| --- | --- |
|  | Developer shows the configuration setting for the encryption of electronic health information on end-user devices is enabled at default. |
|  | Developer shows if the default setting can be disabled. If it can be disabled:   * Demonstrate only a restricted set of limited users can disable; and * Demonstrate an unauthorized user cannot disable default setting. |

<INSERT SCREENSHOTS >

### 1.4Alternative I: Demonstrate Encryption after Technology Stops

|  |  |
| --- | --- |
|  | Developer initiates from an end-user device, a health IT module session that is designed to store electronic health information on the end-user device. |
|  | Developer shows where electronic health information is being accessed on the end-user device when in use. This includes the database and any human readable files on the end-user device containing electronic health information used by the health IT module. |
|  | Developer stops health IT module session using the end-user device. |
|  | Proctor examines the end-user device to verify that electronic health information only remains on the end-user device in encrypted format based on the chosen encryption algorithm (i.e., viewing the on-disk data in raw format to verify it is non-readable). |
|  | Proctor will record the encryption algorithm and end-user device tested in specified section above. |

<INSERT SCREENSHOTS >

**170.315(d)(7) End-User Device Encryption - Alternative II**

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **P&S applies to all criteria:** | YES:  NO: |
| **If not, list applicable criteria:** |  |
| **Instructions:**   * Health IT developer must test to one of the methods specified:  1. Demonstrates electronic health information locally stored on end-user device is encrypted after use of technology on the device stops. 2. Demonstrate electronic health information is NOT locally stored on end-user device after use of technology on the device stops. | |
| **Expected Test Result:**   * Demonstrate health IT module prevents electronic health information from being locally stored on end-user device after use of health IT module stops. * Health IT developer submits documentation attesting no electronic health information is locally stored on the end-user device. See Appendix C for attestation template. * If the health IT module relies on a third party solution to prevent electronic health information from remaining on end-user devices after use of technology on those devices has stopped, developer submits documentation descibing how the third party solution(s) prevents electronic health information from remaining on end-user devices after use of health IT module technology on those devices has stopped. | |
| **Points to Remember:**   * This module is eligible for gap certification. * Many web-based health IT modules depend on local browser technology for the presentation of health information. This must be tested to make sure no health information is being left behind in the browser local cache directory. * 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. 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>

### 2.2Alternative II: Electronic Health Information NOT Stored on End-User Device

|  |  |
| --- | --- |
|  | Using the framework document referenced above, health IT developer attests the health IT module is not designed to locally store electronic health information from the health IT module technology on end-user devices. |

<ATTACH or INSERT LINK TO DOCUMENTATION>

### 2.3Alternative II: Demonstrate Electronic Health Information NOT Stored on End-User Device after Technology Stops

|  |  |
| --- | --- |
|  | Developer initiates a health IT module from an end-user device. |
|  | If applicable, developer shows where electronic health information is being accessed on the end-user device when technology is in use. This includes the database and any human readable files on the end-user device containing electronic health information used by the health IT module. |
|  | Developer stops health IT module session using the end-user device. |
|  | Proctor examines the end-user device to verify that electronic health information does not remain on the end-user device. |

<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-Mar-2016 Additions

* Locally stored electronic health information is intended to mean the storage actions that technology is programmed to take (i.e., creation of temp files, cookies, or other types of cache approaches) and not an individual or isolated user action to save or export a file to their personal electronic storage media.
* This criterion focuses on, and only applies with respect to, the storage capabilities that are designed for use with developer provided or supported technologies for desktop, laptop, or mobile technologies.
* The functionality included in this certification criterion does not focus on server-side or data center hosted technology. Rather, this criterion focuses on data locally stored on end-user devices after the use of the technology is stopped
* Information that has been sent to a print queue or downloaded by the user (e.g., download a PDF report) is no longer considered managed by the technology.
* The permissible encryption algorithms are found here: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf>.
* A Health IT developer can use Rijndael as their encryption algorithm ONLY if the Rijndael encryption algorithm uses data block size of 128 bits. Rijndael can handle different sizes of bit blocks, but AES encryption algorithm, which is based on the Rijndael symmetric block cipher, constraints it to the 128 bit data block. Refer to (<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>) for additional details.
* Consistent with NIST SP 800-111, “end-user devices” to include, but not be limited to: personal computers, laptops, smart phones, tablet computers, external memory devices and similar removable storage media (e.g., universal serial bus [USB] flash drive, memory card, external hard drive, writeable or re-writeable CD or DVD).

# 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)(7) End-User Device Encryption.**

The requirements specified in one of the following paragraphs (that is, paragraphs (d)(7)(i) and (d)(7)(ii) of this section) must be met to satisfy this certification

criterion.

(i) Technology that is designed to locally store electronic health information on end-user devicesmust encrypt the electronic health information stored on such devices after use of the technology on those devices stops.

(A) Electronic health information that is stored must be encrypted in accordance with the standard specified in § 170.210(a)(2).

(B) Default setting. Technology must be set by default to perform this capability and, unless this configuration cannot be disabled by any user, the ability to change the configuration must be restricted to a limited set of identified users.

(ii) Technology is designed to prevent electronic health information from being locally stored on end-user devices after use of the technology on those devices stops.

**§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

# Change Log

|  |  |
| --- | --- |
| Revision | Change Description |
| 01-July-2016 | Re-numbered sections. Added new sections to reference 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