

2015 Edition §170.315(d)(7) End-user Device Encryption				
Testing Components:				
Gap				
Test Procedure Version 1.0 – Last Updated 1/08/16				

Please consult the Final Rule entitled: *2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications* for a detailed description of the certification criterion with which these testing steps are associated. We also encourage developers to consult the Certification Companion Guide in tandem with the test procedure as they provide clarifications that may be useful for product development and testing.

Note: The order in which the test steps are listed reflects the sequence of the certification criterion and does not necessarily prescribe the order in which the test should take place.

Required Tests

(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 devices must 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.

Standard(s):

§ 170.210(a)(2): 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](#), October 8, 2014.

Testing must be conducted for one of the Alternatives outlined below to satisfy the requirements for this criteria.

Criteria ¶	System Under Test	Test Lab Verification
(i) (Alternative)	<ol style="list-style-type: none"> 1. The health IT developer provides documentation outlining how electronic health information stored on end-user devices, after normal use of the Health IT Module technology on those devices stops, is encrypted with algorithm(s) in accordance with the standard specified in § 170.210(a)(2), FIPS 140-2 Annex A: Approved Security Functions (Draft, October 8, 2014) for Federal Information Processing Standards (FIPS) Publication 140-2. 2. The user demonstrates that the default configuration for the Health IT Module is the capability in step 1. 3. The user demonstrates that the Health IT Module configuration cannot be changed, or that the ability to change the configuration is restricted to a limited set of identified users. 4. Negative Testing: The unauthorized user attempts to change the configuration identified in step 1. 	<ol style="list-style-type: none"> 1. The tester verifies that information stored on end user devices after normal use of the Health IT Module technology on those devices stops, is encrypted with algorithm(s) in accordance with the standard specified in § 170.210(a)(2), FIPS 140-2 Annex A: Approved Security Functions (Draft, October 8, 2014) for Federal Information Processing Standards (FIPS) Publication 140-2 by: <ol style="list-style-type: none"> a. reviewing submitted documentation that electronic health information stored on end-user devices, after normal use of the Health IT Module on those devices stops, is encrypted with algorithm(s) in accordance with the standard specified in § 170.210(a)(2); and b. verifying via demonstration that the setting on-disk information is encrypted by viewing the on-disk data in raw form to illustrate that it is non-readable. 2. The tester verifies that the default configuration for the Health IT Module is the capability in step 1. 3. The tester verifies that the configuration of the Health IT Module cannot be changed, or that the ability to change the configuration is restricted to a limited set of identified users. 4. Negative Testing: The tester verifies that an unauthorized user cannot change the configuration identified in step 1.

(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.

Standard(s): None

Criteria ¶	System Under Test	Test Lab Verification
(ii) (Alternative)	The user demonstrates that no electronic health information is locally stored on the end-user device after use of the Health IT Module stops.	The Tester verifies that the Health IT Module prevents electronic health information from being stored locally on the end-user device after the use of the device stops.

Document History

Version Number	Description of Change	Date
1.0	Final Test Procedure	January 08, 2016

Dependencies: For all related and required criteria, please refer to the [Master Table of Related and Required Criteria](#).