

2015 Edition §170.315(e)(2) Secure Messaging					
Testing Components:					
					
Test Procedure Version 1.1 – Last Updated 10/22/15					

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

(e)(2) Secure Messaging. Enable a user to send messages to, and receive messages from, a patient in a secure manner.

Standard(s): None

Criteria ¶	System Under Test	Test Lab Verification
(e)(2)	<ol style="list-style-type: none"> 1. The Health IT Developer identifies the authentication method, encryption algorithm, and hashing algorithm to be used to send/receive secure messages. 2. The authenticated user sends at least one secure message to the identified test patient. 3. The authenticated user sends at least one secure message to the authorized patient representative. 4. The authenticated user receives at least one secure message from the identified test patient. 5. The authenticated user receives at least one message from the identified authorized patient representative. 6. If the Health IT Module supports patient users, the authenticated test patient sends at least one secure message to the identified authenticated user. 7. If the Health IT Module supports patient users, then the authenticated patient representative sends at least one secure message to the vendor identified user. 	<ol style="list-style-type: none"> 1. The tester verifies the authentication method, encryption algorithm, and hashing algorithm to send/receive secure messages. 2. The tester verifies that messages can be sent to an authenticated patient from the Health IT Module. 3. The tester verifies that messages can be sent to an authenticated patient representative from the Health IT Module. 4. The tester verifies that the authenticated user can receive messages from an authenticated test patient. 5. The tester verifies that the authenticated user can receive messages from an authenticated patient authorized representative. 6. If the Health IT Module supports patient users, the tester verifies that messages can be sent to an authenticated user from the authenticated patient user. 7. If the Health IT Module supports patient users, the tester verifies that messages can be sent to an authenticated user from the authenticated patient representative. 8. Negative Test: The tester verifies that the identified Health IT Module function(s) for sending secure messages is not available to an unauthenticated user. 9. Negative test: The tester verifies that messages sent to the patient cannot be retrieved by an unauthenticated user.

Document History

Version Number	Description of Change	Date
1.0	Released for Comment - NPRM	March 31, 2015
1.1	Released for Comment - FR	October 22, 2015

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