

Testing Tool Supplement: 170.314(b)(1) Transitions of Care – Receive, Display, and Incorporate Transition of Care/Referral Summaries

Last Updated: November 8, 2012

Overview and Tool Instructions:

This document is designed to guide EHR vendors and ATLS through the process of testing a System Under Test (“SUT”) for conformance to the MU2 criteria for “Transitions of Care — Receive, Display, and Incorporate Transition of Care/Referral Summaries” also known as “170.314(b)(1)”. The primary tool used in this test is the “NIST Transport Testing Tool” referred to henceforth as the “TTT”.

Multiple browsers may be used to access this tool; if the tool does not load completely using Internet Explorer 8 or Internet Explorer 9, alternative browsers such as Firefox, Google Chrome, or Safari are recommended.

The TTT service is running on port 9100. If your firewall blocks HTTP traffic on any port other than 80 (or 443 for HTTPS), this tool may not be accessible. Please retry access from a location without a firewall that blocks these ports.

The goal of this test is to certify that an EHR, or EHR module, is capable of allowing a user to receive, display, and incorporate patient information sent to the user in the C-CDA standard via transport protocols supported by certified EHR technology (Direct send (required) and Direct send with XDR/XDM, SOAP (optional)). A SUT must have the ability to receive, display, and incorporate information received in the aforementioned C-CDA format to meet this criterion. To facilitate this test, test data has been provided in human-readable and C-CDA format. The Tester will then verify that the SUT certificates are discoverable by other parties (in either DNS CERT records or LDAP servers using the Direct Certificate Discovery Tool (DCDT)). The Tester will select the appropriate C-CDA test data via a Direct (and optional via Direct with XDR/XDM or SOAP) from the TTT to the SUT and invoke the SUT-specific operation to receive, display, and incorporate the patient information contained in the C-CDA into the existing patient record(s) within the EHR. The SUT will generate a message delivery notification (MDN) upon receipt of the C-CDA (via Direct or Direct with XDR/XDM only) and send it to the TTT for verification by the Tester.

The following steps outline the process.

Ensuring the SUT Certificates are Discoverable by Others

1. Navigate to http://www.testteam.us/ModularSpecPhase3_Tool/
2. To verify a SUT’s certificates are hosted correctly and discoverable, click “Hosting”.
3. Follow the on screen instructions.
4. Select the appropriate test case.
5. Enter the Direct address.

6. Click "Submit". The output will be displayed on-screen.

Questions regarding the DCDT tool should be directed to Avinash Shanbhag, Director, Nationwide Health Information Network Division at Avinash.Shanbhag@hhs.gov.

Sending a Message from the TTT to the SUT

1. Prior to Direct testing, certificates must be created and installed for Direct email addresses that will be used in the test. See <http://api.nhindirect.org/java/site/agent/1.2/users-guide/dev-cert-gen.html> and http://api.nhindirect.org/java/site/assembly/stock/1.3.1/users-guide/depl-hisp-only.html#HISP_Only_Deployment_no_source for information on generating certificates.
2. Navigate to <http://hit-testing.nist.gov:9100/ttt/>.
3. Click "Send Direct Message."
4. Choose the correct "From" and "To" addresses for the SUT.
5. Select the 170.314(b)(1) message from the drop down menu. Toggle the option for wrapped or unwrapped for inclusion of a Direct RFC8222 wrapper around the message. By default, Direct send is set to unwrapped. Optionally SAML can be enabled or disabled. TLS may also be toggled. By default SAML is disabled and TLS is enabled.
6. Under "Certificates to be used" header, provide the SUT's "Signing Cert." This should be the SUT's certificate used for digital signing. This file should have a .p12 extension. Only provide a password if the certificate is protected with a password.
7. Under the "Certificates to be used" header, provide the SUT's "Encryption Cert." This is the SUT's public key for encryption. This file should have the file extension ".der".
8. Click "Submit" to cause the TTT to send the Direct message to the SUT.
9. The tester should verify the SUT received the message and was able to display and incorporate the information contained therein.
10. The SUT should create an MDN and reply to the "From" address in step 4.
11. The MDN received by the TTT will be verified by the Tester.

[\[close\]](#) [\[help\]](#) [\[reload\]](#) Environment: -- Choose -- TestSession: -- Choose --

Send Direct Message

Direct System Server Name Direct system to send message to on port 25
 Direct From Address From: field of message header
 To Address To: field of message header
 Message Selection -- Choose -- Document to be sent as attachment
 Message format Unwrapped Wrapped

Certificates to be used

Signing Cert Password This cert will be used to sign the message. It must be in PKCS12 format and include the private key. The password field should be left blank if the key is not password protected
 Encryption Cert This cert is the public key of the receiver that will be used to encrypt the message. It must be in DER format.

Questions regarding the transport tool should be directed to transport-testing-tool@googlegroups.com.

TTT Known Errors

There are the following known errors in the current release of the TTT that will be addressed in subsequent tool release(s):

92| Mu2consol Functional Status Section SHALL satisfy: cognitiveStatus error

Release Notes for C-CDA Validator (contained within the TTT) Released on 09_20_2012-1:

Defects fixed in this release:

- Updated Preferred Language Value Set to remove “B” codes and only validate for “T” codes related to ISO639-2.

Known Issues in the release that impact users:

- No known issues.

TTT Tool Development Status and Releases:

The TTT tool is under ongoing development to support additional 2014 EHR certification criteria. The release and publishing of this tool for public comment is intended for use of the tool for the Message Validator and Direct Sender functions only. Although other capabilities are visible within the tool, and may be accessed, they are not intended for use and are under development.

ONC's release strategy and approach for publishing of the TTT Tool is to continue to publish updated releases on an ongoing basis to obtain timely feedback and support timely resolution of identified issues as well as development of expanded functionality.