nehta

Supplementary Information

Conformance Tests for PCEHR Clinical Information Systems

12 August 2013

Purpose

This document provides supplementary information for use with version 1.6 of the Conformance Test Specification for Clinical Information Systems Connecting to the PCEHR System.

Conformance test data

Conformance test data (i.e. clinical documents) needed for PCEHR Clinical Information Systems (CIS) tests is in the PCEHR vendor test environment. Detailed information about the test data and the eHealth records used for the testing is provided in the spreadsheet titled Conformance Test Data: Clinical Information Systems Connecting to the PCEHR System.

Clarification of conformance requirement 018634

Clinical Information Systems Connecting to the PCEHR System conformance requirement 018634 states:

> *The clinical information system shall verify the CDA package hash value of a clinical document package downloaded from the PCEHR System and it shall indicate if the downloaded clinical document has been modified.*

The following clarifications should be noted:

1. There are a number of hash values associated with a CDA Package and its contents:
   a. A hash value in the XDS metadata which is the hash of the CDA package zip file.
   b. A hash value within the <Manifest> XML element in the signature file (CDA_SIGN.XML) included in the CDA package. This is the hash value used to test the integrity of the clinical document (CDA_ROOT.XML) included in the CDA package.

c. A hash value within the <SignedInfo> XML element in the signature file (CDA_SIGN.XML) which is the hash value used to test the integrity of the signature in CDA_SIGN.XML.

d. If the clinical document refers to attachments then the clinical document will include a hash value for each attachment included in the CDA package.

2. The intention of conformance requirement 018634 is to ensure that if a CDA Package was downloaded to the local system for the purposes of rendering (i.e. viewing or printing), that a hash value is used to ensure the clinical document has not been corrupted while in transit over a network or in storage in the local CIS. Therefore the hash value referred to by this requirement is the hash value in the <Manifest> XML element of the signature file (CDA_SIGN.XML) used to test the integrity of the clinical document (CDA_ROOT.XML), as it is the clinical document that is rendered and so the relevant hash value is the hash value for the document.

3. The requirement does not state when the hash value is to be checked. A document may be corrupted while in local storage so it is recommended that the local CIS check the document for corruption immediately prior to rendering the document.

4. This requirement does not refer to the hash value included in XDS metadata from a getDocumentList operation[1]. The XDS metadata hash value may be used to check the integrity of the entire CDA package. A CIS may be designed to check the hash value of the CDA package as well as the signature hash value for the clinical document within the CDA package however software developers should note that the XDS metadata hash value cannot be used to check the integrity of dynamically generated CDA packages[2]. By contrast the signature hash value for the clinical document can be reliably used even if the document is dynamically generated. At the time of writing this clarification the dynamically generated CDA packages are those created by Medicare, i.e. Medicare DVA Benefits Report, Pharmaceutical Benefits Report, Australian Organ Donor Register and Australian Childhood Immunisation Register.

5. The requirement does not refer to the hash value within the <SignedInfo> XML element in the signature file, however a CIS may use this hash value to check the integrity of the signature.

6. The requirement does not refer to hash values within the clinical document that are associated with attachments, however a CIS should use these hash values to check the integrity of any attachments in the CDA package before an attachment is rendered. An attachment will be referenced by a <reference> element and the hash value will be provided by the <integrityCheck> element. Both are found within an ED datatype, such as an <observationMedia>.

7. The Secure Hash Algorithm-1 (SHA-1) is used for all hash values.

Support

For support with the PCEHR CIS conformance tests please email the NEHTA Help Desk: help@nehta.gov.au.

[1] It is acknowledged that the wording of the requirement is misleading. This will be corrected in a future revision of the requirements.

[2] See the FAQ_Clarification_on_Hash_value_in_XDSMetadata_for_Medicare_Documents_rev001, published on vendors.nehta.gov.au in Vendor FAQs > CDA.