Australian Government
Australian Digital Health Agency

Clinical Package Validator
Product Data Sheet

29 May 2017 v2.5
Approved for external information
Document ID: DH-2491:2017

Key features

- Automated validation of clinical documents and clinical packages
- Schema-based validation
- Schematron-based validation using dynamically loaded template packages
- Clinical package validation
- Clinical terminology validation
- Validations in interactive and batch mode

Usage (internal, external)

- Vendors and implementers of clinical information systems
- System Operator of the My Health Record system
- National Infrastructure Operator

Format

- ZIP file
- Documentation

1 Overview

The Clinical Package Validator[1] ("the Validator") is a tool to automate some of the tests needed to assess conformance of clinical documents and clinical packages with eHealth specifications.

The Validator does not test conformance against all requirements. This *Product Data Sheet* details the sets of tests that are supported, those that are partially supported, and contains a general description of the types of tests that are not supported (see section 5.2).

Results from the Validator must not be relied upon to determine software conformity when declaring conformity to the System Operator of the My Health Record system. A vendor will need to supplement results from the Validator with their own testing before declaring conformity.

2 Summary of functionality

The Validator performs automated tests of clinical documents, clinical packages and clinical packages embedded in HL7[2] MDM wrappers.

CDA documents are built to a certain level of conformance, ranging from a basic CDA header accompanied by an attachment, through to a fully populated CDA body with SNOMED CT-AU, Australian Medicines Terminology (AMT) or PBS coding.[3]

For the exchange of CDA documents, they need to be encapsulated as clinical packages. For point-to-point information exchange, clinical packages need to be wrapped in an HL7 MDM message.

The Validator provides automated, however non-comprehensive, test capabilities for all these cases.

Once the Validator tests have been performed, an onscreen report is generated and displayed along with a rendering of the CDA document, the XML document, an optional clinical packaging report, optional signature report, terminology report, a log and an optional test summary report. These documents can be saved as a record of the automated testing performed by the Validator. A software vendor is free to utilise these documents as part of their overall documentation of their work to determine software conformance.

As per the *Non-Production Disclaimer* provided as part of the Validator *Software Package*, the Validator should not be relied on to determine software conformance. The Validator tests need to be accompanied by other test artefacts to demonstrate how a vendor satisfied themselves that the software was conformant before declaring conformance to the My Health Record System Operator.

[1] The Validator was previously published under the name CDA Validator.
[2] HL7 and CDA are trademarks of Health Level Seven International and are registered with the United States Patent and Trademark Office.
[3] "SNOMED" and "SNOMED CT" are registered trademarks of the International Health Terminology Standards Development Organisation (IHTSDO).

2.1 Testing of clinical documents

The Validator tests a CDA document through:

- Validation against the XML schema for CDA documents;
- Validation against Schematron rules contained in template packages;
- Validation of usage of SNOMED CT-AU, AMT or PBS codes (partial testing only);
- Validation against other terminologies (partial testing only).

The scope of tests performed by the Validator against Schematron rules is dependent on the template packages loaded into the Validator at runtime. The Agency publishes template packages together with their corresponding specifications for clinical document types. Each template package contains Schematron rules to provide automated test coverage for a subset of the conformance requirements published in, for example, the CDA Implementation Guide, the Structured Content Specification or the My Health Record Conformance Profile for a particular document type.

Template packages do not cover all conformance requirements in these specifications. Consequently, the Validator cannot cover all conformance requirements. Its use is strictly limited, as described in section 5.1.

For the scope of terminology validation against SNOMED CT-AU, AMT, PBS other terminologies, please refer to section 5.3.

2.2 Testing of clinical packages

If provided with a clinical package or a clinical package embedded in an HL7 MDM wrapper, the Validator applies a subset of the test cases in *Conformance Test Specification for CDA Packaging v1.5*[4] for both the My Health Record and point-to-point (P2P) contexts. See section 5.1 for details.

For HL7 MDM messages (which contain the clinical package in Base64 format), there are currently no specific tests, except that the CDA package can be extracted from a specific element.

[4] https://www.nehta.gov.au/implementation-resources/clinical-documents/EP-2198-2015/NEHTA-2065-2015

3 Product components

Table 1: Clinical Package Validator product components

Component	**Comment**
Product Data Sheet	This document
Software Package	Contains: • Installer (an .exe file containing the Validator software); • `ISSetupPrerequisites` (a folder of installation scripts for prerequisite software); • Non-production disclaimer.
Installation and Configuration Guide	A PDF file containing instructions on how to successfully install and configure the Validator.
User Guide	A PDF file containing instructions on how to use the Validator to assist testing clinical documents and clinical packages.
Release Note	Notes specific to this release of the Validator.

4 System requirements

The Validator is a Microsoft Windows based tool and requires .NET 4 framework and SQL CE 3.5 to be installed on the machine, which are included as part of the installation (see the Validator's *Installation and Configuration Guide*). The user is responsible for ensuring relevant licences are in place.

5 Scope of tests

The Validator does not and cannot provide tests for all conformance requirements applicable to clinical documents and clinical packages. Vendors are responsible to perform additional tests for all remaining conformance requirements before declaring conformance of their product.

The following sections provide more details about the degree of requirements coverage provided by the Validator.

5.1 Scope of clinical package validation

Clinical package test cases are documented in the *Conformance Test Specification for CDA Packaging* v1.5. The Validator's in-scope tests include many of these test cases.

Table 2 specifies to which degree these test cases are automated by the Validator. Test cases not listed in the table are not in scope for this version of the Validator. The tests performed depend on whether the My Health Record or P2P context is selected (see the *User Guide* product component for details about contexts).

Vendors will need to run their own tests to determine conformance with the full set of requirements for clinical packages.

The following notations are used in Table 2: A (automated), M (manual), N/A (not applicable, NR (not reported). See the table notes on page 9 for further details of these notations.

Table 2: Scope of tests for clinical package validation

Test Case	My Health Record	P2P	Description
Test set: Context My Health Record			
DEXS-L_154	A	N/A	Verify the package contains only CDA_ROOT.XML, CDA_SIGN.XML and packaged attachments.
DEXS-L_155	A	N/A	Verify the package does not contain INDEX.HTM, README.TXT or repository metadata.
DEXS-L_156	A	N/A	Verify that any attachments are not CDA packages or CDA documents.
DEXS-T_121	A	N/A	Verify that the CDA package contains one, and only one, signature file.
DEXS-T_125	A	N/A	Verify that the packaged attachment files are located in the same folder as the CDA_ROOT.XML document.
CPCD_023741	A	N/A	Verify the CDA package only references attachments that are of the supported MIME type.
CPCD_024629	A_3	N/A	Verify the CDA package only references packaged attachments where the filename extensions are those listed for the supported MIME types.
CPCD_024630	A_3	N/A	Verify all packaged attachments have filename extensions which matches their MIME type.
CPCD_023743	A	N/A	Verify the CDA package is not larger than 10MB.

Test Case	My Health Record	P2P	Description
CPCD_023744	A_1	N/A	Verify the eSignature for the CDA package has been signed with a NASH PKI certificate for a healthcare provider organisation, or a supporting organisation (a CSP or GSO).
Test set: Context P2P			
P2P_T13	N/A	A	Verify that the CDA package zip does not contain repository metadata.
CPCD_023748	N/A	A_1	Verify that the eSignature for the signed CDA package has been signed with a NASH PKI certificate for a healthcare provider organisation.
Test set: Base CDA Package			
PKG_CDA_002	A	A	Verify the base CDA package contains one and only one root entry.
PKG_CDA_004	A	A_4	Verify that, for every reference to a packaged attachment, there is a corresponding document in the CDA package.
PKG_CDA_005	N/A	A	Verify that, for every reference to a CDA package packaged attachment, there is a corresponding item in the CDA package.
PKG_CDA_006	NR	M_1	Verify the list of eSignatures in a CDA package.
PKG_CDA_007	A	A_5	Verify all eSignatures are valid eSignatures.
Test set: Signed CDA Package			
PKG_CDA_013	A	A	Verify the CDA package contains one or more eSignatures.
Test set: XDM-ZIP Representation			
XDM_ZIP_105	N/A	N/A	Verify the zip file is a valid XDM-Zip CDA package.
XDM_ZIP_106	A	A	Verify there is one submission set.
XDM_ZIP_108	A	A	Verify the CDA document has the filename CDA_ROOT.XML.
XDM_ZIP_109	A	A	Verify that an eSignature has the filename CDA_SIGN.XML.
Test set: eSignature			
PKG_CDA_024	A	A	Verify eSignature XML document conforms to a Signed Container defined by ATS 5821-2010[5] and the root element is a signedPayload element.
PKG_CDA_025	A	A	Verify the Signed Payload contains only one ds:Signature element.
XSP_SCP_000	A	A	Verify that the eSignature Signed Payload is valid against the Signed Payload and Signed Payload Data XML schemas.
XSP_SCP_001	A	A	Verify the id attribute is unique within the signed XML document.
XSP_SCP_002	A	A	Verify the sp:signedPayloadData element is the only element signed by all the signatures.

[5] *ATS 5821-2010 E-health XML secured payload profiles*, Standards Australia, available from: http://infostore.saiglobal.com/store/details.aspx?ProductID=1391034

Test Case	My Health Record	P2P	Description
XSP_SDP_000	A_6	A_6	Verify that the Signature element of the signedPayload is valid against the XML Signature Schema.
XSP_SDP_001	A	A	Verify that a detached signature is used by ensuring the signature element references an XML document or element in the same document.
XSP_SDP_002	A	A	Verify that Exclusive XML Canonicalisation was used on the signed contents in the ds:SignedInfo element.
XSP_SDP_003	A	A	Verify the Algorithm attribute = 'http://www.w3.org/2001/10/xml-exc-c14n#' for the ds:CanonicalisationMethod element.
XSP_SDP_004	A	A	Verify the Algorithm attribute = 'http://www.w3.org/2000/09/xmldsig#rsa-sha1' for the ds:SignatureMethod element.
XSP_SDP_004_1	A	A	Verify the ds:SignatureMethod algorithm was used to calculate the signature value.
XSP_SDP_005	A	A	Verify there are one or more ds:Reference elements in the ds:SignedInfo element.
XSP_SDP_006	A	A	Verify that each ds:Reference element in ds:SignedInfo contains a URI attribute.
XSP_SDP_007	A	A	Verify the URI attribute of ds:Reference has a '#' character followed by a fragment identifier.
XSP_SDP_008	A	A	Verify the fragment identifier after the '#' character matches the id attribute in sp:signedPayloadData.
XSP_SDP_009	A	A	Verify a ds:Transforms element is present in ds:Reference element.
XSP_SDP_010	A	A	Verify there is only one ds:Transform element in the ds:Transforms element.
XSP_SDP_011	A	A	Verify the Exclusive XML Canonicalisation algorithm was used on the content being signed.
XSP_SDP_012	A	A	Verify the Algorithm attribute = 'http://www.w3.org/2001/10/xml-exc-c14n#' for the ds:Transform element.
XSP_SDP_013	A	A	Verify the value of ds:DigestValue element matches value calculated using SHA-1 algorithm on Exclusive XML Canonicalisation of signed payload.
XSP_SDP_014	A	A	Verify the Algorithm attribute = 'http://www.w3.org/2000/09/xmldsig#sha1' for the ds:DigestMethod element.
XSP_SDP_015	A	A	Verify the ds:KeyInfo element is present in ds:Signature.
XSP_SDP_016	A	A	Verify the ds:X509Data element is present in ds:KeyInfo element.
XSP_SDP_017	A	A	Verify the ds:X509Certificate element is present in ds:X509Data element.

Test Case	My Health Record	P2P	Description
XSP_SDP_018	A	A	Verify X509Certificate element contains the encoded value of the signing certificate.
XSP_SDP_019	A	A	Verify that ds:Signature element does not contain a ds:Object element.
PKG_CDA_026	A	A	Verify the sp:signedPayloadData element contains only one s:eSignature element.
PKG_CDA_027	A	A	Verify there is one ds:Reference element in the Manifest, and that it is set to the SHA-1 digest of the root XML document.
PKG_CDA_029	A_2	A_2	Verify that the person that approved the eSignature can be identified from the value contained in the s:approver element of the signature.
PKG_CDA_030	A	A	Verify the s:signingTime element contains a valid time.
PKG_CDA_031	A	A	Verify the s:signingTime element includes an explicit timezone.
Test set: CDA XML Document			
PKG_CDA_014	A	A	Verify the CDA document is valid for its document type.
PKG_CDA_015	A	A	Verify any packaged attachments are represented using an ED-type element.
PKG_CDA_016	A	A	Verify the ED-type element integrityCheckAlgortihm = 'SHA-1'.
PKG_CDA_017	A	A	Verify the ED-type element contains a single cda:reference element.
PKG_CDA_018	A	A	Verify reference element has a 'value' attribute containing a valid URI.
PKG_CDA_019	A	A	Verify that any ED-element using SHA-1, containing a single reference and the reference value is a URI identical to the name of a document in the CDA package, refers to a packaged attachment.
PKG_CDA_020	A	A	Verify the integrityCheck attribute of any ED-element matches the SHA-1 digest of the referenced atomic packaged attachment.
PKG_CDA_021	A_3	A_3	Verify the mediaType attribute of any ED-type elements is of an agreed Internet type.
PKG_CDA_022	N/A	A	Verify the integrityCheck attribute of any ED-type elements matches the SHA-1 digest of any one eSignature inside the CDA package packaged attachment.
PKG_CDA_023	N/A	A	Verify the mediaType attribute of any ED-type elements is 'application/x.electronichealth.cda.package' for a CDA package packaged attachment.
CDAR_AS_050	A	A	Verify that, for each linkHtml element in the CDA document, if the linkHtml element contains a relative reference, then verify the document being referenced exists in the CDA package.
CDAR_AS_053-06	M_2	M_2	Verify that no attachments contain executable code (e.g. JavaScript code in HTML documents).

Test Case	My Health Record	P2P	Description
CDAR_AS_053-07	A	A	Verify that no referenced attachments require resources to be downloaded from external network locations, unless the document is of the type that allows references to objects outside of the CDA package.
CDAR_AS_053-10	A	A_4	Verify that all referenced attachments are located within the CDA package and are in accordance with the *CDA Packaging* Specification, unless the document is of the type that allows references to objects outside of the CDA package.
PKG_024732	A	A	Verify that, where the document is of the type that allows references to objects outside of the CDA package and the reference is to an external location or website, the reference is a non-zero length string containing a Uniform Resource Identifier (URI).
PKG_024988	A	A	Verify that, where the document is of the type that allows references to an object outside the CDA package and the reference is to an external atomic attachment or website, the reference is represented by an ED-element.
PKG_025077	A	A	Verify that, where the document is of the type that allows references to objects outside of the CDA package and the reference is to an atomic attachment, it has an approved media type and filename extension.
PKG_024990	M_2	M_2	Verify that, where the document is of the type that allows references to attachments outside the CDA package and the reference is to an external atomic attachment and an integrityCheck is included, the integrityCheck attribute has a value that is the SHA-1 digest of the byte stream and the value of the integrityCheckAlgorithm attribute (if included) is SHA-1.
Test set: Clinical Package			
PKG_PKG_009	NR	M_1	Verify that each identifier associated with a member of the CDA package is not an empty value and conforms to the URI specification.
PKG_PKG_010	NR	M_1	Verify that each identifier associated with a member of the CDA package is unique.

Table 3: Table notes

A	The test case is automated without exceptions.
A_1	The test case is automated with the exception of the test step requiring the validation of the NASH certificate by accessing the NASH service to determine if the certificate is on the revocation list.
A_2	The test case is automated with the exception of the test step requiring the validation of the healthcare identifier by accessing the Healthcare Identifiers Service.
A_3	The test case is automated; however the Validator does not report the correct result if the clinical document attachment is compressed (requirements for compressed attachments are listed in the HL7 Version 3 Standard: Data Types – Abstract Specification, Release 1).
A_4	The test case is automated; however the Validator does not report the correct result if a clinical document attachment is in a different folder to the clinical document (this is allowed in the P2P context and disallowed in the My Health Record context).

A_5	The test case is automated with the exception that the only eSignature that is verified is the one with filename CDA_SIGN.XML (multiple eSignatures are allowed in the P2P context and disallowed in the My Health Record context).
A_6	The test case is automated but only covers verification of the most common errors. The full test case should be performed using the guidance provided in version 1.5 of the *Conformance Test Specification for CDA Packaging*.
M_1	The Validator does not report any outcome for the test case. The test result is determined only after a manual inspection of the package index if one is present in the clinical package (a package index is allowed in the P2P context and disallowed in the My Health Record context).
M_2	The Validator does not report any outcome for the test case. The test case may be performed using the guidance provided in version 1.5 of the *Conformance Test Specification for CDA Packaging*.
NR	The test result is not reported by the Validator as it cannot fail in the selected context.
N/A	The test result is not reported by the Validator as the test case is not applicable for the selected context.

5.2 Scope of Schematron validation

The Validator does not perform any tests of requirements for clinical documents by itself. Instead, it dynamically loads Schematron rules from template packages provided to it at runtime. The actual tests for clinical documents hence entirely depend on the template packages provided to the Validator by the vendor.

The Agency publishes template packages for the following types of clinical documents:

- Advance Care Directive Custodian Record
- Australian Childhood Immunisation Register
- Australian Immunisation Register
- Australian Organ Donor Register
- Birth Details
- Child Parent Questionnaire
- Consumer Entered Achievements
- Consumer Entered Measurements
- Discharge Summary
- eHealth Diagnostic Imaging Report
- eHealth Dispense Record
- eHealth Pathology Report
- eHealth Prescription and Dispense View
- eHealth Prescription Record
- eReferral
- Event Summary
- Health Check Assessment
- Health Check Schedule View
- Medicare DVA Benefits Report
- Medicare Overview

- Observation View
- Personal Health Notes (previously known as Consumer Entered Notes)
- Personal Health Summary (previously known as Consumer Entered Health Summary)
- Pharmaceutical Benefits Report
- Shared Health Summary
- Specialist Letter

Template packages for these document types are available from the Agency's website[6] or can be downloaded from the Software Vendor Test (SVT) environment of the My Health Record system. The Schematron rules provided by any of these template packages are not comprehensive in their coverage of conformance requirements for clinical documents. Vendors are responsible for performing their own testing to supplement the Validator's automated tests before declaring conformance for their product.

The following sections give general descriptions of the types of tests that are either fully or partially *excluded* from the Validator and its template packages.

5.2.1 Tests that must be done manually

The following types of tests are not (and cannot be) automated by the Validator:

- Tests for the equivalence between clinical information in a clinical document in atomic format versus the clinical information in the narrative blocks in a clinical document;
- Tests for consistency between the definition of a component of a clinical document (i.e. a section, data group or data element) and the information in that component;
- Clinical document tests that can only be performed by looking up an external software system (e.g. the healthcare identifiers service, the HL7 OID registry);
- Validation of the values of codes for most code systems (e.g. SNOMED CT-AU, AMT, PBS, clinical specialty codes, Australian vaccine codes). The exception is the validation of codes where the set of values is listed in the CDA implementation guides.

5.2.2 Tests not included in this release

The following tests are not included in the Validator, but may be included in a future release:

- My Health Record usability recommendations related to the content of a clinical document;
- Requirements for terminology codes (e.g. a code must be a specific length for it to be an AMT code);
- Requirements for clinical document narrative blocks, stated in the CDA Rendering Specification7 and the HL7 CDA R2 specification8 (e.g. the requirement for the allowed set of mark-up content; the requirements for the inclusion of style codes);
- Data elements in a clinical document that are individually conformant but, when combined, do not make sense and are likely to result from an error in the clinical information system (e.g. having a fully structured address without the state; having a healthcare provider's contact details listed as their home details).

[6] https://www.digitalhealth.gov.au/implementation-resources/clinical-documents
[7] https://www.digitalhealth.gov.au/implementation-resources/clinical-documents/EP-2320-2016/NEHTA-1199-2012
[8] https://www.hl7.org/implement/standards/cda.cfm

5.2.3 Tests partially supported in this release

The following tests are only partially supported by the Validator in this release:

- Requirements in specifications not published by the Agency but which must be implemented in order to conform to the CDA implementation guides, e.g., Health Care Client Identification (SA 5017); HL7 Data Types v1 specification; HL7 CDA R2 specification;
- Requirements for identifiers in a clinical document (e.g. the same identifier should be used for every occurrence of an object in a clinical document, and different objects must not have the same identifier);
- Requirements for entity identifiers and entitlements (e.g. a Medicare card number cannot be used for an entity identifier for a person; a local entity identifier must contain the 'extension' attribute);
- Requirements for data types used in the Agency's structured content specifications (e.g. the requirements for CodeableText, CodedText, Duration, Quantity);
- Requirements in the conformance profile for a specific type of document. The coverage depends on the type of clinical document. For example, Agency-published template packages do not enforce any requirements in the conformance profile for eHealth Prescription Record.

Given conformance with these requirements is only partially tested by the Validator, a vendor needs to perform their own testing for these requirements.

5.3 Scope of clinical terminology validation

With some exceptions, the values of codes for code systems are *not tested* by the Validator. The exceptions are the validation of codes from the code systems listed in Table 4 where the set of values is listed in the CDA Implementation Guides.

Table 4: Scope of tests for clinical terminology validation

Code system	Version	Date of publication	Source
Australian Medicines Terminology (AMT)	V2.54 V2.55 V2.56 V3 20170228	28 Mar 2014 28 Apr 2014 30 May 2014 28 Feb 2017	https://www.healthterminologies.gov.au/ncts/#/learn?content=documentlibrary
Australian and New Zealand Standard Industrial Classification (ANZSIC)	2006	2006	http://www.abs.gov.au/ausstats/abs@.nsf/mf/1292.0
Australian and New Zealand Standard Classification of Occupations (ANZSCO)	First edition, revision 1	25 June 2009	http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/1220.0Main+Features1First%20Edition,%20Revision%201

Code system	Version	Date of publication	Source
Australian Vaccines codes	-	-	http://www.humanservices.gov.au/health-professionals/services/australian-childhood-immunisation-register/acir-vaccine-code-formats
Clinical specialty codes	-	21 Nov 2013	http://meteor.aihw.gov.au/content/index.phtml/itemId/329673
HL7 identifier types	V2.6	2007	https://www.hl7.org/special/committees/vocab/V26_Appendix_A.pdf
HL7 service delivery role types	V3	7 Aug 2008	https://www.hl7.org/implement/standards/fhir/v3/ServiceDeliveryLocationRoleType/index.html
PBS codes (Item codes and Manufacturer codes)	Mar 2017	1 Mar 2017	http://www.pbs.gov.au/browse/downloads
SNOMED CT-AU reference set	20170228	28 Feb 2017	https://www.healthterminologies.gov.au/ncts/#/learn?content=documentlibrary

6 Downloads

The Clinical Package Validator is available in the Implementation Resources area of the Agency's website under "eHealth Reference Platform", or simply through the following link:

https://www.digitalhealth.gov.au/implementation-resources/ehealth-reference-platform/clinical-package-validator

Publication date: 29 May 2017

Contact for enquiries
Telephone: 1300 901 001 or email: help@digitalhealth.gov.au

Acknowledgements

Council of Australian Governments
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.