Australian Digital Health Agency 2025.05.15 12:20:10 +10'00'

Australian Government
Australian Digital Health Agency

Clinical Documents
FAQ Hash value verification

4 March 2013 v1.0
Approved for external use
Document ID: NEHTA-1276:2013

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000
Telephone 1300 901 001 or email help@digitalhealth.gov.au
www.digitalhealth.gov.au

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

HL7 International
This document includes excerpts of HL7™ International standards and other HL7 International material. HL7 International is the publisher and holder of copyright in the excerpts. The publication, reproduction and use of such excerpts is governed by the HL7 IP Policy and the HL7 International License Agreement. HL7 and CDA are trademarks of Health Level Seven International and are registered with the United States Patent and Trademark Office.

Disclaimer
The Australian Digital Health Agency ("the Agency") makes the information and other material ("Information") in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control
This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

Copyright © 2025 Australian Digital Health Agency
This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the permission of the Australian Digital Health Agency. All copies of this document must include the copyright and other information contained on this page.

OFFICIAL

Document information

Key information

Owner Director, Interoperability Products

Contact for enquiries Australian Digital Health Agency Help Centre
Phone 1300 901 001
Email help@digitalhealth.gov.au

Product or document version history

Product or document version	Date	Release comments
v1.0	4 March 2013	Initial release
v1.0	23 January 2025	The document presentation has been enhanced to align with current branding guidelines, however the content has not been changed.

Transition of terms

Certain terms used within the context of this document have changed. The table provides a clear comparison of the historical terms used in text and their current equivalents for your reference.

Historical term	Current term
National eHealth Transition Authority (NEHTA)	The Australian Digital Health Agency (ADHA)
Personally controlled electronic health record (PCEHR)	My Health Record (MHR)

Clarification of conformance requirement 018634 regarding hash value

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 is downloaded to the local system for the purposes of rendering (i.e. viewing or printing), 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 but, as a document may be corrupted while in storage in the local CIS, it is recommended that the local CIS check the document for corruption immediately prior to the document being rendered.
4. The 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 the dynamically generated CDA packages from the Medicare repository.[2] By contrast the signature hash value for the clinical document can be reliably used, even if the document is dynamically generated.

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

[2] See Reference List for PCEHR B2B Gateway Services - FAQ Hash Value in Medicare Documents v1.0

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.

5 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>.

6 For all hash values, the Secure Hash Algorithm-1 (SHA-1) is used.

References

[NEHTA – 1172:2012] National E-Health Transition Authority, 5 December 2012, *PCEHR B2B Gateway Services - FAQ Hash Value in Medicare Documents v1.0*.