Australian Government
Australian Digital Health Agency

My Health Record System Conformance Assessment Scheme

28 February 2025 v2.0

Approved for external use

Document ID: DH-3984:2024

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.aulwww.digitalhealth.gov.au

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

IHTSDO (SNOMED CT)
This material includes SNOMED Clinical Terms™ (SNOMED CT®) which is used by permission of the International Health Terminology Standards Development Organisation (IHTSDO). All rights reserved. SNOMED CT® was originally created by The College of American Pathologists. "SNOMED" and "SNOMED CT" are registered trademarks of the IHTSDO.

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.

OFFICIAL

Document information

Key information

Owner	Branch Manager, Customer Experience and 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
1.0	15/06/2012	Initial release
1.1	23/07/2012	Changed the use of digital credentials to 'recommended'
2.0	28/02/2025	Update to new Agency template and content added for NASH, Clinical document packaging, registered repository operator and Security Conformance Profile

Table of contents

1 Introduction

1.1 Purpose

This document describes the process for assessing a Clinical Information System (CIS), including repositories for conformance to the relevant specifications when connecting and interacting with the My Health Record (MHR) system.

Conformance assessment provides assurance that a software implementation adheres to digital health specifications. It provides users of conforming implementations confidence that an implementation will behave as expected, perform functions in a known manner, has interfaces or formats that adhere to the specifications and will interoperate with the My Health Record system.

A conformance assessment scheme describes how a software system will be assessed and tested for conformance to a digital health specification. It also describes software tools and documentation that support conformance assessment activities.

1.2 Intended audience

The intended audience are participants in the My Health Record system, including:

- Software developers, and registered contracted service providers (CSP) of CISs
- Health jurisdictions, health departments and registered healthcare providers that utilise CISs
- Registered repository operators.

1.3 Scope

The scope of My Health Record conformance assessment is testing the conformance of the behaviour of a software system that will access the My Health Record system directly or indirectly via the Business-to-Business (B2B) Gateway services.

1.4 Out of scope

The scope of My Health Record conformance assessment does not include testing the conformance of software that does not access the My Health Record system B2B Gateway services and does not include software using the Fast Healthcare Interoperability Resources® (FHIR®) Gateway (also previously known as the Mobile Gateway).

2 Conformance assessment

2.1 Approach to conformance testing

Use cases and conformance requirements have been developed to help software developers create a software system that:

- Minimises risks to patient safety, privacy and cyber security
- Implements good practice in exchanging clinical documents with the national My Health Record system.

Conformance testing provides one mechanism through which risks can be mitigated. Other mechanisms for risk mitigation may include, but not limited to, implementation guidelines, local policies or procedures, user education and training.

Risk mitigations other than conformance testing are out of scope for this document. Risks for deployment and implementation are also not covered within this document.

2.2 Object of conformance testing

A CIS focuses on the collection, storage, retrieval, communication, use of health-related data, information and knowledge pertaining to subjects of care. A CIS may include, but is not limited to, General Practitioner systems, pharmacy systems, hospital systems, patient administration systems, aged care systems and specialist systems.

A CIS may consist of a number of separate but interacting systems. In this case, the object of assessment refers to these separate interacting systems as a whole which make up an overall CIS and these may be one or more CISs.

A Contracted Service Provider (CSP) may provide a range of services but not limited to host a CIS on behalf of one or more healthcare provider organisations that wish to interact with the My Health Record system.

A CIS may be a producing system, which is a system that creates and uploads clinical documents to the My Health Record system. A CIS may also be a Consuming system, which is a system that downloads documents from the My Health Record system. A CSP acting as a CIS, or on behalf of a CIS, can also be subject to this assessment scheme.

A CIS may be a repository, which stores individuals' healthcare-related information where this information can be made available to the My Health Record system as clinical documents. [AGENCY2012a]

2.3 Relevant technical documents

Conformance requirements and relevant specifications for a CIS connecting to the My Health Record system are listed in the following documents:

1. *Use of Healthcare Identifiers in Health Software Systems – Software Conformance Profile* [AGENCY2024a]
2. *Clinical Documents – Common Conformance Profile* [AGENCY2017]
3. Conformance Profiles for Clinical Documents[1]

[1] Each My Health Record clinical document has a respective conformance profile for that clinical document.

4. *My Health Record Connecting Systems Conformance Profile* [AGENCY2024b]
5. *Clinical Information Systems Connecting to the* My Health Record *System: Use Cases* [AGENCY2012b]
6. *CDA Package* specification – The CIS needs to conform to the mandatory CDA XML document, optional package attachments and optional repository metadata requirements [AGENCY2011]
7. *NASH SHA-2 - PKI Certificate Readiness Assessment* - A CIS needs to ensure that it supports the new NASH SHA-2 certificates described in the document [AGENCY2021a]
8. *My Health Record Connecting Systems Security Conformance Profile* – A CIS connecting with the My Health Record system via the B2B Gateway Services must conform to the security requirements [AGENCY2024d]

3 Requirements

This Conformance Assessment Scheme (CAS) identifies the expectations placed on software connecting to the My Health Record system. This CAS identifies and leverages other requirement documents that support the My Health Record system. Some of those requirement documents further refer to technical specifications relevant to that domain.

By referencing other profiles and technical specifications into this CAS, a layered approach to conformance is described to the software developer.

3.1 Digital certificates

The National Authentication Service for Health (NASH) makes it possible for healthcare providers and supporting organisations to securely access and exchange health information. NASH provides Public Key Infrastructure (PKI) certificates that help healthcare individuals and healthcare organisations access the My Health Record system and to send and receive messages securely using software that meets the requirements of Secure Message Delivery. NASH PKI certificates can be issued to healthcare providers and supporting organisations that are registered for the HI Service.

Healthcare providers and supporting organisations must support the new NASH SHA-2 certificates from 13 March 2022, as described in the NASH SHA-2 PKI Certificate Readiness Assessment [AGENCY2021a]. The software developer organisation is to create evidence of the testing undertaken and complete the statement of readiness in the NASH SHA-2 readiness test specification [AGENCY2021b].

3.2 HI Service

A CIS needs to use valid healthcare identifiers when interacting with the My Health Record system. Without a valid Individual Healthcare Identifier (IHI), a CIS may incorrectly associate information with the wrong healthcare individual on the My Health Record system or locally.

A valid Healthcare Provider Identifier Individual (HPI-I) is also required to identify the author of a clinical document uploaded to the My Health Record system. This does not apply to a repository which registers the clinical document with the My Health Record system.

3.2.1 HI Service NOC testing

HI Service Notice of Connection (NOC) testing confirms that the software connects successfully with the HI Service. Services Australia manages the NOC testing process.

Contact hi.itest@servicesaustralia.gov.au for more information on the NOC testing process.

3.2.2 HI Service requirements for My Health Record

A CIS must conform to HI Service requirements before gaining access to the My Health Record system.

a) A software connecting to the My Health Record SHALL have passed test cases for at least one of the following HI Service requirements [AGENCY2024a].

Requirement	Use Case	Description
005872	UC.015	IHI Validation - Revalidation of individual IHIs
005877	UC.025	IHI Validation – Batch refresh
005812	UC.010, UC.015	IHI Search – IHI Number search
005813	UC.010, UC.015	IHI Search – Medicare card search
005814	UC.010, UC.015	IHI Search – DVA File number search
005815	UC.010, UC.015	Detailed IHI search (uses addresses)

Table 1 – HI requirements for validating or searching for an IHI

b) A software connecting to My Health Record SHOULD pass test cases for at least one of the following HI Service requirements [AGENCY2024a].

Requirement	Use Case	Description
010041	UC.131	Search for an individual healthcare provider
010040	UC.131	Validation of healthcare provider identifiers with the HI Service

Table 2 – Object of conformance assessment

3.3 My Health Record

Software systems connecting to the My Health Record system need to meet the expectations stated below.

3.3.1 My Health Record NOC testing

Systems needed to connect to the My Health Record will require a Notice of Connection (NOC) testing.

The My Health Record Notice of Connection testing process is performed independently to the My Health Record conformance tests and is performed to determine that software can connect to the My Health Record without compromising national infrastructure.

It is recommended that NOC testing is performed before My Health Record Conformance testing.

Contact healthAPIGatewaySVT@deloitte.com.au to request a vendor pack and to be booked in to perform an observed NOC testing session.

3.3.2 Security Conformance Profile

The My Health Record Connecting Systems Security Conformance Profile (i.e. Security Profile) contains security requirements that are to be applied to connecting systems that access the My Health Record system via the B2B Gateway services.

All connecting systems must meet all the mandatory and relevant conditional requirements. Conditional requirements are deemed mandatory if the specific conditions are met by the implementation.

A software system must conform to the Security Conformance Profile before gaining production access to the My Health Record system.

3.3.3 Clinical documents

A software system may produce, upload or register clinical documents with the My Health Record system.

The software may also download, remove or deregister clinical documents from the My Health Record system.

a) A software system needing to produce, upload or register clinical documents with the My Health Record system SHALL conform to the mandatory and relevant conditional requirements in the following:

   1. All the following use cases [AGENCY2012b]:
      i. UC.CIS.001 Check if an advertised My Health Record exists
      ii. UC.CIS.201 Upload/register a clinical document
      iii. UC.CIS.202 Supersede a clinical document (not applicable for Shared Health Summary)
      iv. UC.CIS.203 Remove/deregister a clinical document
   2. The My Health Record conformance profiles for the types of clinical documents supported by the software system.

b) A software system needing to download, remove or deregister clinical documents with the My Health Record system SHALL conform to the mandatory and relevant conditional requirements in the following:

   1. All the following use cases [AGENCY2012b]:
      i. UC.CIS.001 Check if an advertised My Health Record exists
      ii. UC.CIS.002 Gain access to My Health Record
      iii. UC.CIS.204 Download a clinical document
   2. The My Health Record conformance profiles for the types of clinical documents supported by the software system.

The software system must conform to:

- Common conformance profile – Software needs to have addressed the common requirements for software systems that producing systems and consuming systems of clinical documents share [AGENCY2017]
- My Health Record connecting systems conformance profile - requirements associated with uploading, registering, downloading, removing and deregistering clinical documents to and from the My Health Record system [AGENCY2024b]
- Requirements for the content of clinical documents[2].

[2] Note that there are specific and different requirements for each clinical document type.

3.3.4 Clinical document packaging

A software system must package each clinical document correctly so it can be accepted by the My Health Record system. The CDA Packaging Specification [AGENCY2011] describes how a software can package a document for uploading or registering.

The Agency has developed a tool to assist vendors in determining software's conformance to the CDA Packaging specification. Software developers are encouraged to download and use the Clinical Package Validator [AGENCY2023d] during their development and testing cycles.

4 Conformance assessment method

This section describes the process of assessing an implementation for conformance to the requirements stated in section 3.

4.1 Self-assessment

The following components can be self-assessed:

- Digital certificates (section 3.1)
- My Health Record clinical documents (section3.3.3)
- My Health Record clinical document packaging (section3.3.4)

See the following documents contained within the My Health Record Software Vendor Welcome Pack for a description of the self-assessment process:

- My Health Record Conformance Vendor Declaration Form [AGENCY2025a]
- My Health Record Conformance Vendor Declaration Form Instructions [AGENCY2025b]
- Software Vendor Guide to the Connection Process [AGENCY2025c].

4.2 Evidence verification

The following components require test evidence verification:

- My Health Record Connecting Systems Security Conformance Profile (section 3.3.2)

Component	Assessor
Security Conformance Profile	Australian Digital Health Agency

4.3 Observed self-assessment

The following components require observed self-assessment:

Component	Observer
HI Service NOC testing	Services Australia
HI Service conformance assessment	Australian Digital Health Agency
My Health Record NOC testing	Gateway Operator

4.4 Conformance test specifications

In most cases, a conformance profile will have a conformance test specification that can be used to demonstrate conformance to that profile. Conformance test specifications provide the details of tests performed during the assessment activities.

Conformance test specifications include:

1. Test cases:
    a. A test case is a set of inputs, execution conditions and expected results
    b. Each test case translates a conformance requirement into a concise, insular test with a clear objective and criteria for passing.
2. Test data (if needed) - data used to apply the test cases Conformance test specifications for a CIS connecting to the My Health Record system.
3. Test summary report – a summary of the test results that are in the conformance test specification.

4.5 Success criteria

Criteria for successfully claiming conformance to the My Health Record conformance profiles are:

1. The implementation must support the mandatory and relevant conditional requirements that correspond to the relevant use cases
2. A 100% pass rate is required for the test cases corresponding to these requirements
3. A 100% pass rate is required for all tests for recommended requirements for which a developer wants to claim conformance.

4.6 Test Completion Report (Security Conformance Profile only)

When a software system seeks conformance to the Security Conformance Profile, the following process steps are to be utilised:

1) Conduct software developer testing against all mandatory and relevant conditional requirements
2) Complete the My Health Record Connecting Systems Security Conformance Profile - Conformance Test Specification with test evidence (section 4.4)
3) Submit test evidence to the Agency for evidence verification.

When the submitted test evidence is verified by the Agency, the Agency will produce a test completion report that records the result of the evidence verification process.

4.7 Declaring conformance

The prerequisite for declaring the conformance of an implementation is that the conformance test success criteria has been met.

The developer organisation then declares the conformance of their software systems (the implementation) by completing and submitting an My Health Record Conformance Vendor Declaration Form [AGENCY2025a] or a Registered Repository Operator Production Environment Access Request (PEAR) Form [AGENCY2024c] to the Agency.

For conformance declaration of the Security Conformance Profile, the test completion report (section 4.6) must be submitted to the Agency along with the My Health Record Conformance Vendor Declaration Form.

The conformance test specification provides the evidence that the claim of conformance is valid. The Agency, upon review, may request additional evidence from the developer to support the developer organisation's claim of conformance.

5 Ongoing validity of conformance

5.1 Obligations of re-testing

Re-testing will be triggered by any of the following:

1. If a version of the software conformance requirements is superseded by a new version, an implementation that has been declared conformant must conform to the new version twelve (12) months after the date of publication of the new version of the software conformance requirements. Note this does not replace the need to reassess conformance if an implementation is modified (section 5.2).
2. There are material changes to the functionality or to the source code of the My Health Record functionality that has been conformance tested.
3. Software is behaving in a non-conformant manner, for example, as a result of investigating an incident or system vulnerability.

5.2 Conformance and implementation versioning

A developer may revise their implementation to create a new version, including:

1. A major version, which may contain significant new functionality compared to the preceding version
2. A minor version, which may contain incremental additional functionality compared to the preceding version
3. A maintenance version, which may correct one or more defects in a previously issued version.

Regardless of whether a new version is major, minor or a maintenance version, the new version must be retested for conformance if:

- A conforming system is enhanced to support one or more use cases that were not supported by the preceding version of the system. The new version will require conformance testing against every applicable conformance requirement associated with that use case(s).
- A conforming system is enhanced to include sub-sections of use cases that were not tested in the conforming version of the system. The new version will require conformance testing against every applicable conformance requirement associated with the whole use case(s).
- A conforming system is modified so its existing support for software conformance requirements may be impacted. The new version will require conformance testing against every applicable conformance requirement associated with the whole use case(s).

5.3 Validity period

The implementation will remain conformant until one of the below conditions apply:

- The conformance profile or related technical documents including the conformance assessment scheme (this document) relevant to the declaration of conformance is sunsetted or declared superseded.

- The software is not re-tested in accordance with section 5.1 of this document.
- The software is subject to investigation or incident and the software developer fails to demonstrate an action plan for resolution.
- Three (3) years have elapsed since the previous declaration of the My Health Record Connecting Systems Security Conformance Profile was submitted to the Agency, noting aspects of the Security Conformance Profile refer to annual security testing in some circumstances.
- The software developer does not comply with the obligations specified in the My Health Record Conformance Vendor Declaration Form vendor deed poll.

The declaration only applies to the version of the implementation and the version of the My Health Record connecting systems conformance requirements, identified in the My Health Record Conformance Vendor Declaration Form and the Registered Repository Operator Production Environment Access Request Form.

If the connecting system needs to re-undertake the My Health Record NOC testing process, the software developer should review whether the software should be retested, along with the resubmission of the My Health Record Conformance Vendor Declaration Form.

Acronyms

Acronym	Description
B2B	Business-to-business
CDA	Clinical Document Architecture
CIS	Clinical Information System
CSP	Contracted Service Provider
FHIR	Fast Healthcare Interoperability Resources
HI	Healthcare Identifier
HPI-I	Healthcare Provider Identifier Individual
HPI-O	Healthcare Provider Identifier Organisation
IHI	Individual Healthcare Identifier
MHR	My Heath Record
NASH	National Authentication Service for Health
NOC	Notice of Connection
PKI	Public Key Infrastructure
SHA-2	Security Hash Algorithm 2
XML	Extensible Markup Language

Glossary

Term	Meaning
CDA	HL7 Clinical Document Architecture; an XML-based standard that specifies the encoding, structure and semantics of clinical documents exchanged between health software systems described in a CDA Implementation Guide.
CIS	Within the context of the My Health Record, a Clinical Information System (CIS) is defined as a system that deals with the collection, storage, retrieval, communication and optimal use of health-related data, information, and knowledge. A Clinical Information System may provide access to information contained in an electronic health record, but it may also provide other functions such as workflow, order entry, and results reporting.
Clinical Package Validator	Test tool that checks the level of conformance of a clinical document to the CDA implementation guide, structured content specification and some requirements within the conformance profile specifications. The tool includes validation of the Australian Medicines Terminology and SNOMED CT-AU concepts used in the clinical documents. The Clinical Package Validator consists of CDA validation software, schematron libraries, CDA schemas and an installation guide.
Conformance	Conformance is a measurement (by testing) of the adherence of an implementation to a specification or standard.
CSP	Contracted Service Provider of a healthcare provider organisation means an entity that provides: • Information technology services relating to the My Health Record system • Health information management services relating to the My Health Record system to the healthcare provider organisation under a contract with the healthcare provider organisation. A CSP may provide a range of services but not limited to host a CIS on behalf of one or more healthcare provider organisations that wish to interact with the My Health Record system. A CSP acting as a CIS, or on behalf of a CIS, can also be subject to the same assessment as a CIS.
Evidence verification	Health technology developer tests and submits evidence to the Agency to validate and assess the product against conformance requirements [AGENCY2024e**].**
Gateway Operator	The gateway operator operates and manages the My Health Record B2B and FHIR gateway.
HI	A national identifier assigned to a healthcare provider (individual or organisation) or a healthcare recipient as defined in the Healthcare Identifiers Act [HIACT2021].
Implementation	A software system created by a developer to conform to a specification or standard.
My Health Record System	The system that is used for the operation of functions under the My Health Records Act by the System Operator.
Object of assessment	A digital health system or service, or a component of a digital health system or service, which will be assessed for conformance.

Term	Meaning
Repository	A third-party repository used to store clinical documents and other clinical data that connects to the My Health Record system. A repository may store clinical documents in either a proprietary format or a CDA format.
Secure Message Delivery	A set of specifications that support secure messaging between healthcare providers.
SNOMED CT-AU	Australian extension of SNOMED CT (Systematised Nomenclature of Medicine – Clinical Terms).
Software developer	An organisation that creates an implementation using the My Health Record specifications. A developer may be an organisation that develops a software product, or a provider of digital health services. The conformance assessment process applies to all of these organisations.
Test	The determination of one or more characteristics of an object of conformance assessment according to a documented procedure. Testing is a process applied to software in a test environment.

References

[AGENCY2011] *CDA Package*, v1.0, Australian Digital Health Agency, 2011

[AGENCY2012a] *Repository Overview for the My Health Record B2B Gateway*, Australian Digital Health Agency, 2012

[AGENCY2012b] *Clinical Information Systems Connecting to the My Health Record System: Use Cases*, Australian Digital Health Agency, 2012

[AGENCY2017] *Clinical Documents Common Conformance Profile*, v1.7, Australian Digital Health Agency, 2017

[AGENCY2021a] *NASH SHA-2 - PKI Certificate Readiness Assessment*, v1.0, Australian Digital Health Agency, 2021

[AGENCY2021b] *NASH SHA-2 - Readiness Test Specification*, v1.2, Australian Digital Health Agency, 2021

[AGENCY2023d] *Clinical Package Validator*, v3.3, Australian Digital Health Agency, 2023

[AGENCY2024a] *Use of Healthcare Identifiers in Health Software Systems – Software Conformance Profile*, v4.1, Australian Digital Health Agency, 2024

[AGENCY2024b] *My Health Record Connecting Systems Conformance Profile*, v1.6, Australian Digital Health Agency, 2024

[AGENCY2024c] *Registered Repository Operator Production Environment Access Request Form*, Australian Digital Health Agency, 2024

[AGENCY2024d] *My Health Record Connecting Systems Security Conformance Profile v1.0, Australian Digital Health Agency, 2024*

[AGENCY2024e] *Conformance Framework – Connecting Australian Healthcare National Healthcare Interoperability 2023-2028*, 2024

[AGENCY2025a] *My Health Record Software Vendor Welcome Pack - Conformance Vendor Declaration Form*, Australian Digital Health Agency, 2025

[AGENCY2025b] *My Health Record Software Vendor Welcome Pack - Conformance Vendor Declaration Form Instructions,* Australian Digital Health Agency, 2025

[AGENCY2025c] *My Health Record Software Vendor Welcome Pack - Software Vendor Guide to the Connection Process* v2.0, Australian Digital Health Agency, 2025

[HIACT2021] *Healthcare Identifiers Act 2010*, Federal Register of Legislation, Australian Government, 2021. https://www.legislation.gov.au/C2010A00072/latst/text