



Australian Government

Australian Digital Health Agency

Clinical Information System - Common Requirements

9 September 2026 v.1.0

Approved for external use

Document ID: DH-4298:2026

Acknowledgements

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](http://www.ihtsd.org).

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, CDA and FHIR® 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 © 2026 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 Branch Manager - Informatics and Standards Branch

Contact for enquiries Australian Digital Health Agency Help Centre
Phone [1300 901 001](tel:1300901001)
Email help@digitalhealth.gov.au

Document version history

Document version	Date	Release comments
V1.0	9 September 2026	Initial publication as “Clinical Information System - Common Requirements”

Table of contents

1	Introduction.....	5
1.1	Purpose	5
1.2	Intended audience	5
1.3	Scope	6
1.3.1	Out of Scope	6
1.4	Overview.....	6
1.5	How to use this document with other CIS Requirements documents	7
2	Connections to national systems	8
3	Requirements for payload formats for exchange	10
4	Requirements for point-to-point exchange for information	11
5	Requirements for terminology code sets.....	13
6	Requirements for local software controls.....	15
	Acronyms	16
	Glossary	17
	References	18

1 Introduction

This document fits within a national program of work led by the Australian Digital Health Agency ('The Agency') that promotes use of digital health standards to enable safe, timely and accurate sharing of health information across the healthcare system. These requirements guide solution providers and implementers on the technical structures needed to support interoperability, data requirements, workflows and interfaces to be embedded within the technology we use in healthcare (ADHA2026d).

The Agency has created Common Clinical Information Systems (CIS) Requirements (this document) to ensure digital health solutions are interoperable and support the safe, secure, accurate and timely exchange of high-quality health information among healthcare providers, services, and consumers.

These Common CIS Requirements apply to CIS systems, across all healthcare professions and settings.

This document provides a shared national foundation that ensures consistency across the health system. Sector specific requirements can be layered on top of the common requirements to address distinct risks, regulatory obligations, and operational needs of each care setting. This dual, common-plus-sector specific model promotes national consistency while still enabling flexibility within individual sectors. This document should therefore be read and used alongside sector-specific requirements to understand how the Common CIS Requirements support and sector-specific frameworks work together.

The Agency will continue to develop tailored guidance for high priority sectors where specialised functionality, regulatory alignment or emerging technologies require additional clarity. The Aged Care CIS Requirements (ADHA2026a) and GP CIS Requirements (ADHA2026b) are examples where targeted guidance has already been developed and published.

This document outlines the software requirements with "must" and "should" statements providing guidance on the importance and priority of each requirement for those who choose to adopt it. While meeting the requirements in this document is voluntary, this document may become mandatory in the future at which point these "must" and "should" requirements would take on even greater significance and relevance.

1.1 Purpose

The Common CIS Requirements defines software requirements to improve interoperability. These requirements reference a broader set of technical requirements that collectively outline the specifications necessary for CISs to support interoperability and safe, secure, accurate and timely exchange of high-quality health information.

1.2 Intended audience

This document is intended for:

- Clinical Information Systems developers and implementers
- Clinical peak bodies
- Standards development organisations (SDO)
- Commonwealth Government Departments and Agencies
- State and Territory Health Departments and local health districts and networks.

1.3 Scope

This document outlines the requirements for Clinical Information Systems (CIS) that aim to support digital health initiatives and achieve national interoperability across the Australian healthcare system. The focus of this document is primarily on on-premises and desktop-based systems, which may or may not be deployed in cloud environments. The Agency recognises that, given the diversity of system architectures and levels of technical maturity, some requirements may present implementation challenges. However, software developers are encouraged to work towards the intent of each requirement, progressively aligning their systems to support interoperability, improved data exchange, and national digital health objectives.

1.3.1 Out of Scope

This document does not include:

- Local clinical practices or organisation specific workflows: Vendors may support these as required by customers, but they are not standardised in this document. Internal business or operational workflows used to run or manage a CIS.
- Requirements outside the healthcare domain or unrelated to health information exchange.
- Regulatory, compliance or policy obligations: Vendors remain responsible for meeting these independently of technical capabilities defined in this document.

1.4 Overview

Standards enable healthcare providers and digital health systems to share and use health information in a secure, consistent, and meaningful way. By embedding standards into the design and delivery of digital health solutions, the Agency aims to ensure that health information flows securely and meaningfully across the system—supporting interoperability, empowering individuals, and driving continuous improvement in health outcomes.

This document describes the approach to developing the Common CIS Requirements. The document was developed through a collaborative stakeholder-driven process that leveraged established Agency engagement models. This approach followed a continuous cycle of soliciting input, communicating expectations, listening to feedback, and iteratively

refining the requirements to ensure alignment with industry best practices and unique needs of Agency stakeholders.

The Common CIS Requirements aligns with the priorities and principles that support interoperability stated in the National Healthcare Interoperability Plan (ADHA2023a) and the Agency guiding principles for digital health standards (ADHA2026d) by promoting consistent data structures and recognised terminologies, supporting the use of national healthcare identifiers, and encouraging adoption of national digital health standards. They also ensure compatibility with core national services such as the My Health Record and Provider Connect Australia, and are developed through strong collaboration across government, industry, vendors, and healthcare providers – reinforcing interoperability across the sector. The Agency provides resources to facilitate the onboarding of software developers operating in health on agency related digital health initiatives. The requirements in this document will have supporting information available in the public domain. In addition, the Common CIS Requirements reference several broader work programs – such as the HI Service and My Health Record – that provide more explicit, detailed guidance to software developers. For example, a software developer wishing to CCIS-015 requirement will need to be onboarded into the My Health Record program where they will receive the necessary technical details and conformance expectations relevant to that component of their solution.

1.5 How to use this document with other CIS Requirements documents

This document should be read and used alongside the Aged Care CIS Requirements and GP CIS Requirements. The Common CIS Requirements provide a national baseline for all clinical information systems, defining core capabilities such as interoperability, security, and connection to Australia's digital health infrastructure. The Common CIS Requirements should be implemented as a baseline for all CIS solutions, with the Aged Care CIS Requirements then applied to address aged care specific clinical and operational needs. Where information is shared between aged care services and general practitioners, the GP CIS Requirements are used alongside these documents to ensure GP clinical software supports consistent and interoperable exchange of information for residents of aged care homes. Together the CIS Requirement documents form a cohesive, layered approach that supports coordinated care across aged care and general practices while aligning with national digital health infrastructure.

2 Connections to national systems

This section describes the requirements for CIS to connect with Australia's national digital health infrastructure. Adhering to national standards and specifications ensures interoperability and secure data exchange across all healthcare systems. Prioritising standards-based solutions that integrate with national services – such as Healthcare Identifiers Service (HI Service) and Provider Connect Australia (PCA) – enable more efficient, seamless system connectivity and contributes to the development of a single, reliable national directory of healthcare providers and organisations. Consistent with the National Healthcare Interoperability Plan 2023-2028 (ADHA2023a), the use of national healthcare identifiers ensures individuals, providers and organisations are accurately identified when exchanging information. Linking PCA and HI Service enables validated identity matching using HPI-Os and HPI-Is, improving data accuracy, reducing errors and supporting near real time updates for better clinical decision making and continuity of care. These capabilities reduce clinical risk, lower costs and improve outcomes by ensuring timely access to accurate information. Streamlined integration and a single point of update model reduce administrative burden by minimising manual processes, while supporting more efficient and reliable information sharing. Strong security and privacy safeguards remain essential to protect sensitive data and maintain trust across the healthcare system.

CCIS-005 Connect to the Healthcare Identifiers Service (HI Service)

The software must connect to the HI Service web services that assigns identifiers to uniquely identify individuals, healthcare providers, healthcare provider organisations and healthcare support service providers. This requires software conformance to HI Service conformance use cases UC.010, UC.015, UC.131 and UC.306.

Applicable to: Clinical Information Systems

Notes: See the [Healthcare Identifiers Service Conformance Assessment Scheme](#) (ADHA2025a) for more information. The HI Service ensures accurate identification of individuals, providers and organisations, enabling secure and reliable health information exchange. For developers, connecting to the HI service is critical for interoperability and seamless integration with systems like My Health Record. This requirement recognises that large enterprises may use different architectures, including gateways or third-party partners. The intent of the requirement is met if the software can access the HI service in a conformant way. A direct connection to the HI service is not required in some circumstances.

CCIS-010**Connect to Provider Connect Australia**

The software should have the capability to connect to Provider Connect Australia via FHIR Publishing API's interface.

Applicable to: Clinical Information Systems

Notes: See Provider Connect Australia™ (PCA™) (ADHA2024a).

CCIS-015**Download and render documents My Health Record**

The software must have the capability to download and render the following My Health Record document types:

- Discharge Summary.

Applicable to: Clinical Information Systems

Notes: See Discharge Summary v1.6 (ADHA2026c).

See domain specific CIS Requirements for additional My Health Record upload/download requirements.

CCIS-020**Australian Immunisation Register**

The software could integrate to the Australian Immunisation Register (AIR) via B2B web services so that a patient's immunisation history can be uploaded, downloaded, and displayed.

Applicable to: Clinical Information Systems

Notes: Incorporating immunisation data into the local health record will assist with preventive health planning and improve quality of care.

Connecting to the AIR API also allows for a better user experience as it reduces reliance on web portals.

The developer should engage with Services Australia to identify and understand the available APIs for the AIR. This requirement recognises that large enterprises may use different architectures, including gateways or third-party partners. The intent of this requirement is met where the software enables access to AIR, regardless of whether the connection is direct or via a gateway.

3 Requirements for payload formats for exchange

This section describes the requirements for the structure of payloads for CIS and the types of data they should contain when exchanging payloads outside the organisational boundaries. Consistent payload formats are essential to ensure data is organised, labelled and transmitted in a way that receiving systems can accurately interpret. Without standardisation, information may become fragmented or misinterpreted, leading to errors and inefficiencies. Payload structures enable secure and reliable data exchange, ensuring the integrity of clinical information across all systems and providers.

CCIS-025**FHIR formats**

The software should be capable of generating and consuming information in published national FHIR AU Core formats.

Applicable to: Clinical Information Systems

Notes: Implementations should take into account that AUCDI (Australian Clinical Data for Interoperability) is available, providing general (core) and use case specific guidance on data requirements for information sharing. Developers are encouraged to align to AUCDI where relevant and appropriate, based on their use case and data exchange context. Refer to the latest published version of the [AU Core Implementation Guide](#) (HL7Aust2022a) for more information

4 Requirements for point-to-point exchange for information

This section describes requirements for point-to-point exchange for information. Point to-point is an exchange between healthcare providers and between healthcare providers and individuals. Current systems are often limited by poor interoperability, fragmented data and difficulties in aligning and accessing information across platforms. This can lead to incomplete information sharing and increased patient safety risks when providers lack timely access to accurate data. Many exchanges still rely on manual processes such as downloading forms, uploading to portals and re-entering data across systems, which are time consuming, can alter formatting and introduce errors. As the number of touchpoints increases, so do security risks and administrative burden. Improving interoperability is critical to enable secure, seamless information sharing and ensure healthcare providers have access to the right information at the right time.

CCIS-030 FHIR RESTful API Integration

The software should implement RESTful APIs that conform to the FHIR specification to enable the exchange of clinical data between systems.

Applicable to: Clinical Information Systems

Notes: RESTful APIs are not exclusively point to point but are essential part of the future FHIR enabled ecosystem. Where applicable, implementations should align with the latest published version of AU Core profiles to ensure consistency with nationally defined interoperability standards. Implementations should take into account that AUCDI (Australian Clinical Data for Interoperability) is available providing general (core) and use case specific guidance on data requirements for information sharing. Developers are encouraged to use AUCDI where relevant and appropriate, based on their use case and data exchange context. Refer to the latest published version of the [AU Core Implementation Guide](#) (HL7Aust2022a) for more information.

CCIS-035 Secure Authentication and Data Exchange via SMART on FHIR

The software should follow SMART on FHIR security standards, using protocols like OAuth 2.0 and OpenID Connect to securely authenticate users and apps and enable secure data exchange between SMART on FHIR apps and FHIR servers.

Applicable to: Clinical Information Systems

Notes: This implementation guide ([App Launch: Launch and Authorization - SMART App Launch v2.2.0](#)) describes a set of foundational patterns based on [OAuth 2.0](#) for client applications to authorise, authenticate, and integrate with FHIR-based data systems.

5 Requirements for terminology code sets

This section describes the requirements to implement terminology code set standards that reflect important health concepts. Common code sets enable interoperability by ensuring consistent representation of clinical information across systems, supporting accurate data exchange, documentation, billing and analysis.

CCIS-045 Native support for SNOMED CT-AU

The software must natively support SNOMED CT-AU.

Applicable to: Clinical Information Systems

Notes: Native support means that the clinical codes in the local data store are stored as SNOMED CT-AU codes directly, without mapping or translation to other formats. Where SNOMED CT-AU concepts exist, systems must store the corresponding SNOMED CT-AU codes directly within the local data store, rather than deriving them solely through mapping from other code systems. Systems may continue to use local or proprietary codes in parallel where required; however, the SNOMED CT-AU code should be retained alongside these codes to support the accurate and reliable information exchange without dependency on mapping tables at point of use.

Implementations should take into account that AUCDI (Australian Clinical Data for Interoperability) is available, providing general (core) and use case specific guidance on data requirements for information sharing. Developers are encouraged to use AUCDI where relevant and appropriate, based on their use case and data exchange context.

CCIS-050 Entering clinical information with SNOMED CT-AU

When entering clinical information, the software must be able to capture and exchange that clinical information using SNOMED CT-AU terms to facilitate interoperability and data quality.

Applicable to: Clinical Information Systems

Notes: Ensuring clinical information is expressed in SNOMED CT-AU terms at the point of care increases data interoperability. In some contexts, the use of SNOMED CT-AU is not clinically advisable or technically possible.

CCIS-065 FHIR terminology integration for SNOMED CT-AU

The software should support integration with terminology services such as SNOMED CT-AU using FHIR Terminology services such as

Ontoserver to enable the use of standardised clinical terminologies and semantic interoperability.

Applicable to: Clinical Information Systems

Notes: The National Clinical Terminology Service (NCTS), operated by the Australian Digital Health Agency, is responsible for managing, developing, and distributing national clinical terminologies such as SNOMED CT-AU and AMT, along with related tools and services. The National Terminology Server (NTS) provides an authoritative national access point for terminologies. This function is easily implemented using Commonwealth Scientific and Industrial Research Organisation's (CSIRO) Ontoserver, a FHIR-native, web-based terminology server that supports semantic interoperability through NCTS content syndication. The Australian Digital Health Agency sublicences Ontoserver for use within Australia and a free licence can be requested by emailing help@digitalhealth.gov.au.

While Ontoserver is preferred mechanism for maintaining up to date SNOMED CT-AU content through automated syndication, a broader approach should be considered to ensure continuity of access. Specifically, complementary methods such as the use RF2 files should be available as a backup in scenarios such as system downtime or connectivity issues. Ontoserver can also be set up to automatically syndicate new releases from a central terminology server instance, making it easy to provide the latest terminology data available to client applications. Refer to [Ontoserver](#) (CSIRO2026a).

6 Requirements for local software controls

This section describes the requirements for local software controls such as privacy, clinical safety, and cyber security standards. The current landscape is characterised by poor interoperability and fragmented data alignment, limiting efficient access to information across systems. This fragmentation can result in incomplete or inaccessible information, impacting clinical decision-making and patient safety. Many workflows still rely on manual processes, such as downloading sensitive forms and re-uploading them across multiple portals, increasing the risk of data inaccuracies and formatting issues. Each additional touchpoint or login expands the attack surface and introduces security vulnerabilities while also adding to administrative burden. Frequent system and UI updates can disrupt existing API integrations, reducing stability and undermining interoperability. Addressing these challenges require stronger alignment to national standards to support secure, reliable information sharing, protect sensitive data and ensure providers have timely access to accurate information.

CCIS-040	Cyber security The software should implement cyber security controls described in the My Health Record Cyber security conformance profile (ADHA2026e). Applicable to: Clinical Information Systems Notes: The My Health Record Cybersecurity conformance profile provides detailed guidance on how careful software design can meet and exceed the “Essential 8” mitigation strategies (Department of Home Affairs 2023a) that help organisations protect themselves against various cyber threats.
CCIS-070	Cyber security The software should align with the ‘Secure-by-design’ principles as outlined by the Australian Cyber Security Centre (ACSC), including the ‘ACSC Secure by Design foundations’ (ACSC2024a) and the ‘ISM based Guidelines for Software Development’ (ACSC2026a) Applicable to: Clinical Information Systems Notes: The ACSC Secure by Design principles, including the Secure by Design Foundations and ISM based Guidelines for Software Development, provide broadly applicable expectations for secure design, testing and ongoing assurance while allowing flexibility in implementation.

Acronyms

Acronym	Description
AIR	Australian Immunisation Register
AMT	Australian Medicines Terminology
API	Application Programming Interface
AU Core R2	Australian Core Release 2
AUCDI	Australian Clinical Data for Interoperability
B2B	Business to Business
CIS	Clinical Information System
FHIR	Fast Healthcare Interoperability Resources
HI	Healthcare Identifiers
HI Service	Healthcare Identifiers Service
SDO	Standards developing organisations
SMART	Substitutable Medical Applications, Reusable Technologies
SNOMED	Systematized Nomenclature of Medicine
SNOMED CT-AU	Systematized Nomenclature of Medicine, Clinical Terminology Australian Release

Glossary

Term	Meaning
Australian Immunisation Register	The Australian Immunisation Register (AIR) is a national register which records vaccines given to all people Australia.
Clinical Information System	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. A CIS may also serve the role, or have similar features to, an electronic medicines management system.
Could	It is optional for the solution design to enable, support or make the stated requirement technically possible.
FHIR AU	Specifications developed for Australian Context (For example AU Core).
HI Service	The HI Service is a national system for identifying individuals, healthcare providers, and organisations, using a healthcare identifier. HIs are assigned to healthcare recipients (individuals), individual healthcare providers (also individuals), healthcare provider organisations and healthcare support service providers.
Must	The solution design is expected to enable, support or make the stated requirement technically possible.
Should	It is desirable for the solution design to enable, support or make the stated requirement technically possible.
Standard	Standards are voluntary documents that set out specifications, procedures and guidelines that aim to ensure products, services, and systems are safe, consistent, and reliable.

References

ADHA2023a	<u>National Healthcare Interoperability Plan 2023-2028</u> , Australian Digital Health Agency, 2023
ADHA2024a	<u>Provider Connect Australia™ (PCA™)</u> , Australian Digital Health Agency, 2024
ADHA2025a	<u>Healthcare Identifiers Service Conformance Assessment Scheme</u> , v5.0, Australian Digital Health Agency, December 2025
ADHA2026a	<u>Clinical Information System Requirements - Aged Care</u> , v1.0, Australian Digital Health Agency, June 2026
ADHA2026b	<u>Clinical Information System Requirements - General Practitioner</u> , v1.1, Australian Digital Health Agency, June 2026
ADHA2026c	<u>Discharge Summary</u> , v1.6, Australian Digital Health Agency, January 2026
ADHA2026d	<u>Digital Health Standards</u> , Australian Digital Health Agency, March 2026
ADHA2026e	<u>My Health Record Connecting Systems - Security Conformance Profile</u> , v1.0.1, Australian Digital Health Agency, April 2026
ACSC2024a	<u>Secure by Design Foundations</u> , Australian Cyber Security Centre, July 2024
ACSC2026a	<u>Guidelines for Software Development</u> , Australian Cyber Security Centre, March 2026
CSIRO2026a	<u>Onotoserver</u> , Commonwealth Scientific and Industrial Research Organisation, 2026
Department of Home Affairs 2023a	<u>2023-2030 Australian Cyber Security Strategy</u> , Department of Home Affairs, February 2023
HL7AUST2022a	<u>AU Core Implementation Guide 1.0.0 - Working Standard</u> , v1.0, HL7 Australia, 2022