Australian Government
Australian Digital Health Agency

My Health Record Connecting Systems Conformance Profile

4 July 2024 v1.6

Approved for external use

Document ID: DH-3983:2024

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.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.

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	8 May 2012	Updated to reflect the outcomes of discussions on 2 and 3 May 2012 and reviewer feedback received in writing prior to 7 May 2012
1.1	1 June 2012	Updated during the CCA stakeholder workshops on 30 and 31 May 2012
1.2	6 June 2012	Updated based on additional stakeholder comments
1.3	13 June 2012	Updated based on the eHealth CCA Governance Group meeting on 13 June 2012
1.4	15 June 2012	Version approved for release
1.5	6 September 2012	Additional web services added to Table 1. Additional use cases added to Table 2. New use cases added to existing conformance requirements
1.6	4 July 2024	Update to new Agency template and content added for registered repository operator. Updated acronyms, glossary and references.

Table of contents

1 Introduction

1.1 Purpose

This document specifies software conformance requirements for systems connecting to the My Health Record (MHR) system. These requirements are used to assess software systems for conformance to help minimise risks to clinical safety, information privacy and security, and maximise the benefits of connecting to the My Health Record system.

1.2 Intended audience

The intended audience includes:

- Developers and software providers of connecting systems
- Health jurisdictions
- Health departments
- Healthcare providers, and
- Registered repository operators.

1.3 Scope

Conformance requirements in this document apply to systems connecting to the My Health Record system. This document is intended to address areas such as:

- Patient and clinical safety
- Privacy and
- Authentication and security.

Within the context of the My Health Record programme, a My Health Record connecting system ("the system") is defined as a system that may deal with the collection, storage, retrieval, communication, or use of health-related data, information and knowledge pertaining to subjects of care. The system may comprise one or more applications or components. Some systems may incorporate a provider or clinical portal.

This document does not contain conformance requirements for consumer portals and provider portals connecting to the My Health Record system, and does not include:

- Conformance requirements listed in the technical service specifications for the My Health Record system's B2B Gateway
- Conformance requirements related to a specific type of clinical document
- Anything that is covered by good software design (and which is therefore the responsibility of vendor, which is answerable to its client) and
- Anything that is specific to a site implementation.

The conformance requirements in this document apply to one or more use cases, where each use case describes a scenario in which a system interacts with the My Health Record system. A

set of use cases has been defined and correspond to functionality provided by the set of web services provided by the My Health Record B2B Gateway Service for systems. This document will be updated when additional use cases for the system are identified and associated conformance requirements developed.

This document does not specify all requirements a system must meet in order to connect to the My Health Record system. For example, a series of My Health Record conformance profiles have been developed for each of the types of clinical documents that are exchanged between systems and the My Health Record system. A My Health Record conformance profile for a type of clinical document may list conformance requirements related to that type of document.

For a complete list of specifications and requirements, the reader should refer to My Health Record System Conformance Assessment Scheme [AGENCY2024].

1.4 Relevant specifications

Related specifications are listed below:

1. My Health Record System Conformance Assessment Scheme [AGENCY2024].
2. Clinical Information Systems Connecting to the My Health Record System: Use Cases [AGENCY2012a].

1.5 Development of these requirements

Clinical safety hazards assessment, privacy impact assessment and international and Australian standards on information security and privacy have been used to identify risks and related mitigation controls informing the conformance requirements in this document. In addition, outcomes of consultation with industry associations, health jurisdictions and clinical leads have been incorporated in these conformance requirements.

1.6 Acknowledgements

The Agency would like to acknowledge the time and efforts of the following stakeholders for their valuable contributions by participating in workshops and submitting written feedback on this document:

- Department of Health and Aged Care (DoHAC)
- State and territory health jurisdictions
- Medical Software Industry Association (MSIA)
- Australian Information Industry Association (AIIA)
- Software vendors, and
- Clinical leads.

2 General background

2.1 Background

A My Health Record connecting system ("the system") traditionally contains discrete records of personal health information created and accessed by a healthcare provider organisation. A system may be well designed to mitigate the risks to clinical safety, information security and privacy within the organisational boundary of a provider organisation and even when exchanging health information with other selected healthcare provider organisations. However, there is an increased level and number of risks when sharing health information via the My Health Record system as information sent to the My Health Record system may be retrieved by many healthcare provider organisations that are unknown to, and have no relationship with, the source of the health information.

Conformance requirements for systems connecting to the My Health Record system have been developed to minimise these risks and maximise the benefits of the My Health Record system to healthcare individuals and healthcare providers.

Conformance testing provides one mechanism through which these 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.

2.2 Achievement of conformance

This document contains conformance requirements for a set of use cases. Each use case has conformance requirements, and each conformance requirement lists the use case(s) to which it applies.

Use cases are only intended as a guide for software developers and aspects of a use case that must be supported by a system are explicitly stated as conformance requirements within this document.

The systems must conform to the mandatory and any relevant conditional conformance requirements of use cases they support, and not implement any prohibited capabilities for these use cases.

2.3 Conformance to the My Health Record B2B Gateway Service

A My Health Record connecting system may obtain access to the My Health Record B2B Gateway Service either:

- Directly, through web services included in the B2B Gateway Service or
- Through conformant third-party software.

If the system accesses the B2B Gateway Service directly then it must conform to the logical and technical service specifications for the B2B Gateway Service. These specifications describe web services to access the B2B Gateway Service and data exchanged between a system and the B2B Gateway Service.

If the system does not access the B2B Gateway Service directly but does so indirectly via another software system, then the system does not need to conform to the web services, but the developer may need to review the specifications for the B2B gateway.

The logical and technical service specifications for the B2B Gateway Service may be obtained from Agency Developer Portal. Conformance requirements associated with the B2B Gateway service relate to the web services and versions outlined in Table 1.

Note: The My Health Record system was previously known as the Personally Controlled Electronic Health Record (PCEHR) and there may still be references to PCEHR in the various conformance and specification documents. These references will be updated over time.

MHR B2B Gateway Service Specification	Web service	Supported version of web service
Record Access Service	doesPCEHRExist	v1.0
Record Access Service	gainPCEHRAccess	v1.0
Document Exchange Service	retrieveDocument	v1.0
Document Exchange Service	provideAndRegisterDocumentSet-b	v1.0
Document Exchange Service	registerDocumentSet-b	v1.0
Document Exchange Service	removeDocument/DeregisterDocument	v1.0
View Service	getChangeHistoryView	v1.0
View Service	registryStoredQuery	v1.0
View Service	getConsolidatedView	v1.0
View Service	getAuditView	v1.0
View Service	getRepresentativeList	v1.0
Template Service	searchTemplate	v1.0
Template Service	getTemplate	v1.0

Table 1: My Health Record B2B Gateway Service

Many conformance requirements are directly associated with web services in the My Health Record B2B gateway. For these conformance requirements, the additional information specifies the name of the associated web service.

The B2B gateway specifications specify other web services that are not listed in this document but for which there may be conformance requirements developed in future. The

scope of this document version is the functionality provided by the set of available web services for systems connecting to the My Health Record system.

2.4 Contracted service providers and registered repository operators

Conformance requirements in this document also apply to software systems that may be hosted by a contracted service provider (CSP), and a registered repository operator.

A contracted service provider of a healthcare provider organisation is an entity that provides the following services under contract to the healthcare provider organisation:

- Information technology services relating to the My Health Record system or
- Health information management services relating to the My Health Record system.

Conformant repositories are systems storing individuals' healthcare-related information where this information can be made available to the My Health Record system as clinical documents. The systems required to operate and manage this information could be run directly by a business entity (such as a pathology provider organisation or registry agency), a government entity or by a third-party registered repository operator acting on behalf of one or more healthcare-related organisations. [AGENCY2012b]

No additional conformance requirements specific for CSP and registered repository operators have been identified.

3 Conformance requirements

This section contains conformance requirements applicable to systems connecting to the My Health Record system. Table 2 lists the use cases and the applicable mandatory, conditional and recommended conformance requirements specified in this section.

Use case No	Use case description	Mandatory conformance requirements	Conditional conformance requirements	Recommended conformance requirements
UC.CIS.001	Check if an advertised MHR exists	019100	None	019378
UC.CIS.002	Gain access to MHR	017836, 017941, 019048, 019100	019116	019378
UC.CIS.201	Upload/register a clinical document	017839, 017841, 017842, 017941, 019042, 019100	None	019378, 019429
UC.CIS.202	Supersede a clinical document	017839, 017841, 017842, 017941, 019042, 019100	018338	019378, 019429
UC.CIS.203	Remove/deregister a clinical document	017941, 019100	017887, 019377	019378
UC.CIS.204	Download a clinical document	018634, 019041, 019100	018721	019108, 019118, 019119, 019378
UC.CIS.301	Access a View Service	018634, 019041, 019100	018721	019119, 019378
UC.CIS.401	Search for a Template Package	None	None	None
UC.CIS.402	Retrieve a Template Package	None	None	None
UC.CIS.403	Store Template-Metadata or a Template Package	None	None	None

Table 2: Use cases and conformance requirements

3.1 Mandatory requirements

This section lists the mandatory software conformance requirements for systems connecting to the My Health Record system.

Requirements listed as mandatory are mandatory within the context of the related use cases. A system that implements a use case must conform to the mandatory requirements for that use case. If a connecting system supports none of the use cases related to a conformance requirement, then the clinical information does not need to support that requirement.

017836	**Preventing healthcare provider access codes from being cached** After gaining access to a My Health Record by using a PACC or a PACCX, the system SHALL NOT cache or store the healthcare individual's access consent code (PACC or PACCX) except for auditing purposes. If the codes are stored for auditing purposes, it SHALL be encrypted or masked.
Priority	Mandatory
Related Use Case	UC.CIS.002
Additional Notes	This requirement is derived from the recommendation 4.25 in the My Health Record Privacy Impact Assessment Report [PIA2011]. It is intended to mitigate the privacy risk faced by healthcare individuals where a provider organisation gains access to a healthcare individual's My Health Record by re-using a previously supplied access code even though that healthcare individual has since removed that provider organisation from their access list. After a healthcare provider organisation gains access using the PACC or PACCX supplied by the healthcare individual, the My Health Record system allows the healthcare individual to revoke that organisation's access through a consumer portal without having to change the PACC or PACCX. In this case, in order to avoid violating the privacy of the healthcare individual, the provider is to avoid re-using the access codes previously supplied by the healthcare individual. Therefore, the system, used by the provider organisation, is to avoid caching or storing access codes, used in the initial gainPCEHRAccess operation, for the purpose of re-using them in future gainPCEHRAccess operations. This requirement applies after the gainPCEHRAccess service is invoked.

017839	**Automatic and manual document upload or register in the My Health Record system**
	The system SHALL either: • Require an explicit command by the system user for uploading or registering a clinical document to the My Health Record system OR • Provide a mechanism to preclude any supported clinical document from being automatically uploaded to or registered in the My Health Record system.
Priority	Mandatory
Related Use Case	UC.CIS.201, UC.CIS.202
Additional Notes	This requirement is derived from the recommendation 5.31 in the My Health Record Privacy Impact Assessment Report [PIA2011]. It allows for the clinician to make a decision regarding information that warrants uploading or registering in the My Health Record and is intended to mitigate the risk of a healthcare provider organisation inadvertently uploading or sharing a clinical document potentially leading to: • Disclosing sensitive information such as pregnancy termination, drug treatment, sexual or mental health matters or • Violating certain restrictions placed upon by state and territory-based legislations on when a healthcare provider may upload or register some records, such as records which contain information about a healthcare individual's HIV status. This requirement does not mandate the system to provide a user interface for the user to upload or register clinical documents, and does not preclude the use of batch processing. This requirement applies before the provideAndRegisterDocumentSet-b service is invoked for document upload, or before the registerDocumentSet-b service for document registration.

017841	**Retaining clinical documents uploaded to or registered in the My Health Record** The system SHALL either: • Retain any clinical document uploaded to or registered in the My Health Record system OR • Retain the original clinical information used to generate the clinical document uploaded to or registered in the My Health Record to meet requirements for relevant health records legislation, audit, and business requirements.
Priority	Mandatory
Related Use Case	UC.CIS.201, UC.CIS.202
Additional Notes	The intent of this requirement is to enable the healthcare provider organisation using the system to keep a record of the information shared with other healthcare providers. This requirement applies before the provideAndRegisterDocumentSet-b service is invoked for document upload, or before the registerDocumentSet-b service for document registration.

017842	**Identifying clinical documents uploaded to or registered in the My Health Record system** The system SHALL provide a mechanism to identify which clinical documents have been uploaded to or registered in the My Health Record system.
Priority	Mandatory
Related Use Case	UC.CIS.201, UC.CIS.202
Additional Notes	The intent of this requirement is to enable the system user to identify a previously uploaded or registered document that may need to be superseded, removed or deregistered due to invalid or erroneous content. Without this capability in the local system, when the system user finds invalid or erroneous content in a clinical document but the system user is unaware that it has been uploaded to or registered with the My Health Record system, the system user may not attempt to supersede, remove or deregister that document on the My Health Record system. The system may achieve this requirement by: • Storing the document identifiers of the uploaded or registered documents • Storing the uploaded or registered documents locally or • Other mechanisms. This requirement applies after the provideAndRegisterDocumentSet-b service is invoked for document upload, or after the registerDocumentSet-b service for document registration.

017941	**Handling errors received from the My Health Record system** The system SHALL have a process to handle errors received from the My Health Record B2B Gateway Service.
Priority	Mandatory
Related Use Case	UC.CIS.002, UC.CIS.201, UC.CIS.202, UC.CIS.203
Additional Notes	The intent of this requirement is to ensure that any error response from the My Health Record system from attempting to gain access to a My Health Record, upload/register, supersede, remove or deregister a clinical document is communicated to a relevant system user so that appropriate actions can be taken. When the system user finds invalid or erroneous content in a previously uploaded or registered document and attempts to remove, deregister or supersede it on the My Health Record system, the system user will be unaware (without this capability in the system) that their request has failed, causing the invalid or erroneous information to remain in the My Health Record system. Similarly, when the system user attempts to gain access and fails, they should be alerted immediately. Error handling processes will vary across different systems and organisations. There is no error handling process that is appropriate to all scenarios. Therefore, it is recommended that an error handling process be determined and implemented for each scenario. As a general guidance however, the system should alert the system user when it receives some of the My Health Record errors including, but not limited to: • PCEHR_ERROR_2501: Document not found (when attempting to remove or deregister a clinical document that no longer exists in the My Health Record system) • PCEHR_ERROR_5101: MHR not found (when attempting to gain access to a My Health Record that does not exist or that is inactive) • PCEHR_ERROR_5102: MHR is found but access code is required (when attempting to gain access to a My Health Record without a code but that My Health Record is protected with a PACC) • PCEHR_ERROR_5103: MHR is found but access code is invalid (when attempting to gain access with an incorrect access code) • PCEHR_ERROR_5104: You are not authorised to access this record (when attempting to gain access to a My Health Record where the provider organisation's access has been revoked by the healthcare individual) • Any other error where the error description contains sufficient information to guide the system user to take an appropriate action. For any other errors not listed above, a warning or alert may be raised with the system user. Such errors should be logged with sufficient details for review and resolution by a local system administrator.

018634	**Validating the integrity of clinical documents downloaded from the My Health Record system** The system SHALL verify the CDA package hash value of a clinical document package downloaded from the My Health Record system and it SHALL indicate if the downloaded clinical document has been modified.
Priority	Mandatory
Related Use Case	UC.CIS.204, UC.CIS.301
Additional Notes	This is intended to mitigate the risk of a clinical document being tampered with or corrupted when it is downloaded from the My Health Record system to the local system. This requirement applies after invoking the retrieveDocument service or after invoking view services with download a clinical document (such as the getConsolidatedView service).

019041	**Ability to save or print clinical documents from the My Health Record system** The system SHALL provide a capability to save or print a clinical document downloaded from the My Health Record system.
Priority	Mandatory
Related Use Case	UC.CIS.204, UC.CIS.301
Additional Notes	This is a potentially useful functionality for the viewing healthcare provider to manage clinical information in an appropriate manner. The healthcare provider may no longer have access to the My Health Record because the healthcare individual may have revoked that organisation's access to their My Health Record. This requirement applies after invoking the retrieveDocument service or after invoking view services with download a clinical document (such as the getConsolidatedView service).

019042	**Ability to support the withdrawal of consent to upload or register a clinical document in the My HealthRecord system** The system SHALL provide an ability to support the withdrawal of the healthcare individual's consent to upload or register clinical documents to the My Health Record system, and SHALL prevent them from being uploaded or registered where the consent has been withdrawn.
Priority	Mandatory
Related Use Case	UC.CIS.201, UC.CIS.202
Additional Notes	This requirement is intended to reduce the risk of a clinical document being uploaded or registered to the My Health Record system despite the withdrawal of consent by the healthcare individual, leading to a privacy breach by the provider organisation. This may be implemented at a number of different levels (for example document Type level or for an episode). This requirement applies before the provideAndRegisterDocumentSet-b service is invoked for document upload, or before the registerDocumentSet-b service for document registration.

019048	**Ability to submit provider access consent codes (PACC or PACCX)** The system SHALL provide the system user with an option to enter provider access consent codes (PACC or PACCX) to make initial and subsequent requests to gain access to a My Health Record or protected clinical documents.
Priority	Mandatory
Related Use Case	UC.CIS.002
Additional Notes	With this capability in the system, the healthcare provider organisation will benefit from being able to access to potentially important clinical information the healthcare individual has decided to share via the My Health Record system by supplying the healthcare provider with a PACC or PACCX. Even after a healthcare provider organisation has gained access to a healthcare individual's My Health Record, the system is to continue to allow the system user to resubmit the access requests for that My Health Record. Scenarios of successfully gaining access multiple times to a My Health Record include, but not limited to: • Initial access request without a code followed by an access request with a PACCX or an emergency access request • Initial access request with a PACC followed by an access request with a PACCX or an emergency access request and • Initial emergency access request followed by a subsequent access request with a PACC or a PACCX. In addition, where the healthcare individual has modified the healthcare provider access control settings after a healthcare provider organisation gained access to their My Health Record, additional access requests may be required in order to re-gain access to the healthcare individual's My Health Record. This requirement does not suggest that the system should store or cache provider access consent codes for the purpose of gaining access multiple times to a My Health Record. In fact, storing or caching PACC or PACCX is prohibited (refer to Requirement 017836). This requirement invokes the gainPCEHRAccess service.

019100	**Use of a valid Individual Healthcare Identifier**
	When accessing the My Health Record system the system SHALL only use an individual healthcare identifier (IHI) if it has been validated or obtained during a configurable period, with the period determined by the local healthcare provider's policy. This may be achieved by: • Being connected to the HI Service OR • Obtaining a valid IHI from another software system (other than the My Health Record System) that is connected to the HI Service. The relevant HI use cases and software requirements are documented in the My Health Record System Conformance Assessment Scheme [AGENCY2024].
Priority	Mandatory
Related Use Case	UC.CIS.201, UC.CIS.202, UC.CIS.203, UC.CIS.204, UC.CIS.001, UC.CIS.002, UC.CIS.301
Additional Notes	This requirement is intended to mitigate the risk of a healthcare provider organisation associating health information sent to or retrieved from the My Health Record system to the wrong healthcare individual due to an incorrect healthcare identifier allocation in the local system. This may lead to: • Delay in or lack of treatment to the patient or delivery of treatment to the wrong patient and • Violation of a person's privacy by disclosing personal health information to others (healthcare providers as well as authorised and nominated representatives) who have access to that person's My Health Record.

3.2 Conditional requirements

This section lists the conditional software conformance requirements for systems connecting to the My Health Record System.

Requirements listed as conditional are conditional within the context of the related use cases. Support for conditional requirements associated with a use case is mandatory, subject to the condition stated in the requirement. If a system supports none of the use cases related to a conditional conformance requirement, then the system does not need to support that requirement.

017887	**Identifying locally created documents removed or deregistered from the My Health Record system** If the system uploads or registers clinical documents that are removed or deregistered from the My Health Record system by the healthcare provider organisation, it SHALL provide an ability to identify which locally created clinical documents have been removed or deregistered from the My Health Record System.
Priority	Conditional
Related Use Case	UC.CIS.203
Additional Notes	This is intended to minimise the risk of a system user re-uploading or re-registering a document to the My Health Record system without realising that another system user has already removed or deregistered it due to obsolete or erroneous content. This requirement does not mandate a specific approach to identify locally created clinical documents removed or deregistered from the My Health Record system. It is up to each implementation to determine an appropriate design as long as conformance to this requirement can be demonstrated. This requirement applies after the removeDocument/DeregisterDocument service is invoked.

018338	**Ability to supersede clinical documents** If the system supports the upload or registration of documents other than Shared Health Summary, the system SHALL provide an ability to supersede previously uploaded or registered clinical documents where there is a change or an error in the data used to create the uploaded or registered clinical documents.
Priority	Conditional
Related Use Case	UC.CIS.203
Additional Notes	This requirement is intended to minimise the risk of the presence of inappropriate, invalid, or obsolete clinical documents in the My Health Record system. When the system user finds errors or invalid information in an uploaded or registered document, the system user will not be able to supersede that document on the My Health Record system (without this capability in the system) and all healthcare providers who have access to that document may use the information in the document without knowing that it contains errors or invalid information. This requirement mandates that the system provides an ability to supersede existing clinical documents on the My Health Record system. The exception is a Shared Health Summary as it cannot be superseded[1]. If the system uploads Shared Health Summary only and not any other types of clinical documents, the system is not required to supersede clinical documents on the My Health Record system. This requirement invokes the provideAndRegisterDocumentSet-b service.

[1] The National MHR System will regard only the most recently uploaded Shared Health Summary in a healthcare individual's My Health Record as the only active Shared Health Summary for that My Health Record. Any previously uploaded instances of Shared Health Summary are automatically treated as historical versions.

019377	**Ability to remove or deregister clinical documents** If the system has the ability to upload or register documents in the My Health Record system, the system SHALL provide an ability to remove or deregister previously uploaded or registered clinical documents where there is a change or an error in the data used to create the uploaded or registered clinical documents.
Priority	Conditional
Related Use Case	UC.CIS.203
Additional Notes	This requirement is intended to minimise the risk of the presence of inappropriate, invalid, or obsolete clinical documents in the My Health Record system. When the system user finds errors or invalid information in an uploaded or registered document, the system user will not be able to remove or deregister that document on the My Health Record system (without this capability in the system) and all healthcare providers who have access to that document may use the information in the document without knowing that it contains errors or invalid information. This requirement mandates that the system provides an ability to remove or deregister existing clinical documents on the My Health Record system. This requirement invokes the removeDocument/DeregisterDocument service.

018721	**Identifying clinical documents downloaded from the My Health Record system** If the system stores clinical documents downloaded from the My Health Record system, the system SHALL have a mechanism to indicate to the system user: • That the clinical document being viewed was downloaded from the My Health Record system and • The date and time it was downloaded from the My Health Record system.
Priority	Conditional
Related Use Case	UC.CIS.204, UC.CIS.301
Additional Notes	This requirement enables the system user to be informed that the clinical document being viewed was downloaded from the My Health Record system and also when it was downloaded. This is to encourage the system user to make a better informed decision on whether they should check for a more up-to-date version on the My Health Record system. This requirement applies after invoking the retrieveDocument service or after invoking view services with download a clinical document (such as the getConsolidatedView service).

019116	**Conditions of emergency access**
	If the system supports gaining an emergency access to a healthcare individual's My Health Record, it SHALL display the conditions of emergency access at time intervals appropriate to the clinical settings before asserting emergency access to the My Health Record.
Priority	Conditional
Related Use Case	UC.CIS.002
Additional Notes	The system user needs to be made aware that they need to abide by the emergency access conditions when gaining emergency access to a My Health Record. Once emergency access has been asserted by an organisation to a My Health Record and provided that the emergency access has not expired, the system is not expected to display the message again. Suggested text for the system to display to meet this requirement is as follows: *"By selecting the Emergency Access checkbox, you are declaring that access to this eHealth record is necessary to lessen or prevent a serious threat to an individual's life, health, or safety or to public health or public safety and your patient's consent cannot be obtained. This will override any access controls set by the individual and will permit access to all active documents for five days. Your Emergency Access will be recorded on the eHealth Record's audit log and the individual may be notified."* Please note that this is a suggested text only and the exact wording above is not mandatory to meet this requirement.

3.3 Recommended requirements

This section lists the recommended software conformance requirements for systems connecting to the My Health Record system.

Requirements listed as recommended are recommended within the context of the related use cases. Support for recommended requirements associated with a use case is strongly encouraged though not mandated.

019108	**Ability to retrieve a list of clinical documents and a list of historical versions of a document** The system SHOULD provide a mechanism to retrieve: • A list of clinical documents associated with a healthcare individual's My Health Record (registryStoredQuery service) and • A list of historical versions of a particular clinical document from the My Health Record system (getChangeHistoryView service).
Priority	Recommended
Related Use Case	UC.CIS.204
Additional Notes	The intent of this requirement is to help maximise the benefits of the My Health Record system to the healthcare provider organisation using the system. It is intended to facilitate: • Retrieving a clinical document from the My Health Record system. (The local system needs to obtain the document identifier of an existing clinical document in order to retrieve it from the My Health Record system. The My Health Record system returns document identifiers to the system as part of the registryStoredQuery operation.) and • Checking for a more up-to-date version of a document where the system stores the downloaded documents locally. (The My Health Record system returns the list of historical versions of a clinical document to the system as part of the getChangeHistoryView operation.)

019118	**Sort and filter lists of clinical documents from the My Health Record system** The system SHOULD provide an ability to sort and filter the lists of clinical documents retrieved from the My Health Record system.
Priority	Recommended
Related Use Case	UC.CIS.204
Additional Notes	This is intended to mitigate the risk of being unable to find relevant clinical documents for a particular event or care episode by the system user. This requirement applies after registryStoredQuery or getChangeHistoryView service is invoked.

019119	**Patient demographic information in downloaded clinical documents versus local records** The system SHOULD provide a warning to the system user if the healthcare individual's demographic information in a clinical document downloaded from the My Health Record system does not match the demographic information in the local healthcare individual's record.
Priority	Recommended
Related Use Case	UC.CIS.204, UC.CIS.301
Additional Notes	This is intended to mitigate the risk of a downloaded clinical document being associated to the wrong patient record in the system. Core demographic details of a healthcare individual include: • Family name • Sex and • Date of birth. This requirement applies after invoking the retrieveDocument service or after invoking view services with download a clinical document (such as the getConsolidatedView service).

019378	**Auditing capability** The system SHOULD have the capability to audit interactions with the My Health Record system.
Priority	Recommended
Related Use Case	UC.CIS.001, UC.CIS.002, UC.CIS.201, UC.CIS.202, UC.CIS.203, UC.CIS.204, UC.CIS.301
Additional Notes	Local auditing of significant transactions is considered good software practice, and may be important from a medico-legal perspective.

019429	**Use of a valid Individual Healthcare Provider Identifier**
	When accessing the My Health Record system the system SHOULD only use the clinical document author's individual healthcare provider identifier (HPI-I) if it has been validated or obtained during a configurable period, with the period determined by the local healthcare provider's policy. This may be achieved by: • Being connected to the HI Service or • Obtaining a valid HPI-I from another software system (other than the My Health Record system) that is connected to the HI Service. The relevant HI Use Cases and software requirements are documented in the My Health Record System Conformance Assessment Scheme [AGENCY2024].
Priority	Recommended
Related Use Case	UC.CIS.201, UC.CIS.202
Additional Notes	The requirement does not apply to the healthcare identifier of the healthcare provider organisation (HPI-O) as the HPI-O is validated by the My Health Record system. The requirement also does not apply to other HPI-Is in the clinical document, such as those of the receiving health provider.

Acronyms

Acronym	Description
CDA	Clinical Document Architecture
CSP	Contracted Service Provider
HI Service	Healthcare Identifier Service
HPI-I	Healthcare Provider Identifier – Individual
HPI-O	Healthcare Provider Identifier – Organisation
IHI	Individual Healthcare Identifier
PACC	Provider Access Consent Code
PACCX	Provider Access Consent Code eXtended
PCEHR	Personally Controlled Electronic Health Record (Former name of My Health Record)
MHR	My Health Record

Glossary

Term	Meaning
Alert	An electronic notification of an exception or event with immediate action required. An alert may be displayed on a user interface and/or communicated to a responsible party through other means (e.g. via a pager, email or mobile phone). An alert will persist until the underlying exception or event is acknowledged and/or addressed, or the operator explicitly cancels the alert. An unresolved alert persists until the initial error condition for that alert has been addressed. Acknowledging an alert is not resolving an alert. An action or event must take place to address the initial reason for the alert.
Authorised Representative	An authorised representative (legally appointed), in relation to an individual, means: a) a guardian or person responsible as defined within relevant state/territory legislation, or b) an attorney for the individual under an enduring power of attorney, or c) a person who is otherwise empowered under law to exercise any functions as an agent of or in the best interests of the individual.
B2B Gateway	The business-to-business gateway is an access channel by which external systems can interact with the My Health Record system.
Clinical document	A clinical document is a document that provides personal health information about an individual. Examples include shared health summary, event summary, discharge summary, referrals and pathology result report.
Clinical Document Architecture	An HL7 standard intended to specify the encoding, structure, and semantics of clinical documents for exchange.
Conformance	A measurement (by testing) of the adherence of an implementation to a specification or standard.
Contracted Service Provider	Contracted service provider, of a healthcare provider, means an entity that provides information technology services relating to the communication of health information or health information management services to the healthcare provider under a contract with the healthcare provider [HIACT2021].
Healthcare individual	An individual who is, or could be, the subject of care in the context of a healthcare event.
Healthcare Identifier	An identifier assigned to a healthcare provider (individual or organisation) or a healthcare individual.
Provider Access Consent Code	A code (i.e. PIN or passphrase) an individual can provide to an authorised user, in order to have the participating organisation added to the access list.
Provider Access Consent Code extended	A code (i.e. PIN or passphrase) an individual can provide to an authorised user in order to enable the participating organisation to have access to 'limited access' clinical documents.
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.

Term	Meaning
Repository operator	A person that holds, or can hold, records of information included in My Health Records for the purposes of the My Health Record system. [MHRACT2012]
SHALL	This word, or the term REQUIRED, means that the statement is an absolute requirement of the specification.
SHOULD	This word, or the term RECOMMENDED, means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
System	A system that deals with the collection, storage, retrieval, communication and optimal use of health-related data, information, and knowledge. A 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.
System user	Local users of the system connecting to the My Health Record system.
Warning	Electronic notification of an exception or event that may require user attention. A warning will typically be displayed on the user interface and acknowledged by the operator. The software system shall allow the user to cancel a warning.

References

[AGENCY2012a]	Clinical Information Systems Connecting to the My Health Record System: Use Cases, Australian Digital Health Agency, 2012
[AGENCY2012b]	Repository Overview for the My Health Record B2B Gateway, Australian Digital Health Agency, 2012
[AGENCY2024]	My Health Record System Conformance Assessment Scheme, Digital Health Agency, 2024
[HIACT2021]	Healthcare Identifiers Act 2010, Federal Register of Legislation, Australian Government, 2021. https://www.legislation.gov.au/C2010A00072/latest/text
[MHRACT2012]	My Health Record Act 2012, Federal Register of Legislation, Australian Government, 2012. https://www.legislation.gov.au/C2012A00063/latest/text
[PIA2011]	MHR Privacy Impact Assessment Report, Department of Health and Aged Care, 2011