# Clinical Information Systems Connecting to the PCEHR System

## Conformance Requirements

Version 1.5 — 6 September 2012

Approved for Release

(Review scheduled for December 2012)

**National E-Health Transition Authority Ltd**
Level 25
56 Pitt Street
Sydney, NSW, 2000
Australia.
www.nehta.gov.au

# Table of contents

**1 Introduction ..... 1**
1.1 Purpose ..... 1
1.2 Intended audience ..... 1
1.3 Related documents ..... 1
1.4 Development of these requirements ..... 1
1.5 Acknowledgements ..... 1
1.6 Contact details ..... 1

**2 General background and scope ..... 2**
2.1 Background ..... 2
2.2 Scope ..... 2
2.3 Glossary ..... 3
2.4 Acronyms and abbreviations ..... 5
2.5 Achievement of conformance ..... 5
2.6 Conformance to the PCEHR B2B Gateway Service ..... 5
2.7 Contracted Service Providers ..... 6

**3 Conformance requirements ..... 8**
3.1 Mandatory requirements ..... 8
3.2 Conditional requirements ..... 14
3.3 Recommended requirements ..... 17

**Appendix A: References ..... 20**

**Appendix B: Change Log ..... 21**

# Document version control

## Revision history

| Version | Date | Comments |
|---|---|---|
| 1.0 | 8 May 2012 | Updated to reflect the outcomes of discussions on 2 and 3 May 2012 and reviewer feedbacks 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 | See Change Log in Appendix B. |

# 1 Introduction

## 1.1 Purpose

This document specifies software conformance requirements for Clinical Information Systems (CIS) connecting to the Personally Controlled Electronic Health Records (PCEHR) System. These requirements are used to assess clinical information systems for conformance to help minimise risks to clinical safety, information privacy and security, and maximise the benefits of connecting to the PCEHR System.

## 1.2 Intended audience

The intended audience includes:

- Health software vendors and Contracted Service Providers (CSP); and
- Health jurisdictions and healthcare providers.

## 1.3 Related documents

This document forms a part of the document package for conformance assessment of Clinical Information Systems connecting to the PCEHR System. The package of documents also includes:

- Clinical Information Systems Connecting to the PCEHR System: Use Cases [NEHTA2012]; and
- Clinical Information Systems Connecting to the PCEHR System: Conformance Assessment Scheme [CCAGG2012].

## 1.4 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.

## 1.5 Acknowledgements

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

- Department of Health and Ageing (DOHA);
- State and territory health jurisdictions;
- Medical Software Industry Association (MSIA);
- Australian Information Industry Association (AIIA);
- Software vendors; and
- Clinical leads.

## 1.6 Contact details

Any comments or feedback should be sent to nehtasupport@nehta.gov.au.

# 2 General background and scope

## 2.1 Background

A Clinical Information System (CIS) traditionally contains discrete records of personal health information created and accessed by a healthcare provider organisation. A CIS 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 PCEHR System as information sent to the PCEHER 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 CIS connecting to the PCEHR System have been developed to minimise these risks and maximise the benefits of the PCEHR System to healthcare recipients 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 Scope

Conformance requirements in this document apply to CIS connecting to the PCEHR System. This document is intended to address areas such as:

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

Within the context of the PCEHR programme, a Clinical Information System (CIS) 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 [AS5021]. The CIS may comprise one or more applications or components. Some Clinical Information Systems may incorporate a provider or clinical portal.

This document does not contain conformance requirements for repositories, consumer portals and provider portals connecting to the PCEHR System, and does not include:

- Conformance requirements listed in the technical service specifications for the PCEHR System's B2B Gateway;
- Conformance requirements related to a specific type of clinical diocument;
- 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 clinical information system interacts with the PCEHR System. A set of use cases has been defined and correspond to functionality provided by the set of web services provided by the PCEHR B2B Gateway Service for connecting CIS. This document will be updated when additional use cases for the connecting CIS are identified and associated conformance requirements developed.

This document does not specify all requirements a CIS must meet in order to connect to the PCEHR System. For example, a series of PCEHR conformance profiles have been developed for each of the types of clinical documents that are exchanged between Clinical Information Systems and the PCEHR System. A PCEHR 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 Clinical Information Systems Connecting to the PCEHR System: Conformance Assessment Scheme [CCAGG2012].

## 2.3 Glossary

For the purpose of this document, the following definitions apply.

| Term | Definitions and usage |
|---|---|
| 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, eg 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. |
| Authorised Representative | For healthcare recipients under 18, an authorised representative is a person who the PCEHR System Operator is satisfied has parental responsibility for the healthcare recipient. In other cases it may be a person who the PCEHR System Operator is satisfied is authorised to act on behalf of the healthcare recipient under the law of the Commonwealth or a State or Territory, or a decision of an Australian court or tribunal or someone the PCEHR System Operator is satisfied is otherwise an appropriate person to be the authorised representative of the healthcare recipient [DOHA2011]. |
| B2B Gateway | A Business-to-Business Gateway that provides outward facing interfaces for participating systems to access the PCEHR System. |
| CIS User | Local users of the Clinical Information System connecting to the PCEHR System. The PCEHR System entrusts a participating healthcare provider organisation to grant access to individual healthcare providers and other local users who need to access the PCEHR System. These users are referred to as 'CIS Users' in this document. A CIS User must be an employee[1] who has a legitimate need to access the PCEHR System as part of their role in healthcare delivery. When the CIS Users access the PCEHR System, they are only permitted to access the PCEHR of consumers they are involved in delivering healthcare services to. All access to the PCEHR System is audited [DOHA2011].<br>The PCEHR System entrusts the participating organisation to verify the identity of the CIS Users prior to allowing them access the PCEHR System. The participating organisation may undertake a separate check or leverage existing verification of identity procedures (such as processes used by the organisation's Human Resources department) [DOHA2011]. |

[1] As per the Healthcare Identifiers Act 2010 [HIACT2010], an 'employee' is either an individual who provides services for the entity under a contract for services or an individual whose services are made available to the entity (including services made available free of charge).

| Term | Definitions and usage |
|---|---|
| Clinical document | A clinical document contains personal health information about an individual, in either a structured (atomic data elements) or unstructured form. The PCEHR System collects information in the form of clinical documents. Types of clinical documents may include:<br>• Shared Health Summary;<br>• Event Summary;<br>• Discharge Summary;<br>• Specialist Letter;<br>• Referral;<br>• Prescribing and Dispensing information;<br>• Medicare information; or<br>• Consumer entered information.<br>There will be additional types of clinical documents to be supported by the PCEHR System in future. |
| Clinical Information System | Within the context of the PCEHR programme, a Clinical Information System (CIS) 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 [AS5021]. The system may comprise one or more applications or components. |
| Conformance | Conformance is 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 organisation means an entity that provides:<br>• Information technology services relating to the PCEHR system; or<br>• Health information management services relating to the PCEHR system;<br>to the healthcare provider organisation under a contract with the healthcare provider organisation. |
| Healthcare recipient | A person who has received, receives or may receive healthcare [DOHA2011]. This is the same as the definition of healthcare recipient in the *Healthcare Identifiers Act 2010* [HIACT2010]. |
| Shall | This verb **shall** when appearing in a conformance requirement indicates a mandatory requirement. Its negative form **shall not** indicates a prohibition. |
| Should | The verb **should** when appearing in a conformance requirement indicates a recommendation. Its negative form **should not** indicates an option that should not be supported. |
| Supersede (a clinical document) | When the CIS supersedes a clinical document on the PCEHR System, it uploads a new clinical document overriding a previously uploaded document. To supersede a clinical document, the CIS specifies the document identifier of the previously uploaded document as part of the upload operation (provideAndRegisterDocumentSet-b) of the new document.<br>The PCEHR System maintains the superseded clinical documents and makes them available as part of getChangeHistoryView operation. |
| 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. |

## 2.4 Acronyms and abbreviations

| Acronym/ abbreviation | Explanation |
|---|---|
| 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. |
| CSP | Contracted Service Provider |
| HI | An identifier assigned to a healthcare provider (individual or organisation) or a healthcare recipient as defined in the *Healthcare Identifiers Act 2010* [HIACT2010].<br>Note: this term is used generally in healthcare to refer to any healthcare identifier including local numbers, but in this document is restricted to mean only the national healthcare identifier context. |
| IHI | Individual Healthcare Identifier |
| PACC | Provider Access Consent Code (PACC) is 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. [DOHA2011] |
| PACCX | Provider Access Consent Code eXtended is 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. [DOHA2011] |
| PCEHR | Personally Controlled Electronic Health Record |
| PCEHR System | The national system that contains Personally Controlled Electronic Health Records. |

## 2.5 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 developers of clinical information systems and aspects of a use case that must be supported by a clinical information system are explicitly stated as conformance requirements within this document.

The clinical information 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.

## 2.6 Conformance to the PCEHR B2B Gateway Service

A clinical information system may obtain access to the PCEHR B2B Gateway Service either:

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

If the clinical information 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 clinical information system and the B2B Gateway Service.

If the clinical information system does not access the B2B Gateway Service directly but does so indirectly via another software system then the clinical

information 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 vendors.nehta.gov.au. Conformance requirements associated with the B2B Gateway service relate to the web services and versions outlined in Table 1.

| PCEHR 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 | 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: PCEHR B2B Gateway Service**

Many conformance requirements are directly associated with web services in the PCEHR 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 clinical information systems connecting to the PCEHR System.

## 2.7 Contracted Service Providers

Conformance requirements in this document also apply to clinical information systems that may be hosted by a Contracted Service Provider (CSP). 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 PCEHR system; or
- Health information management services relating to the PCEHR system.

This information is based on the model that is in use for the HI service and is to be reviewed within 6 months. No additional conformance requirements specific for Contracted Service Providers have been identified.

# 3 Conformance requirements

This section contains conformance requirements applicable to clinical information systems connecting to the PCEHR 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 PCEHR exists | 019100 | None | 019378 |
| UC.CIS.002 | Gain access to PCEHR | 017836, 017941, 019048, 019100 | 019116 | 019378 |
| UC.CIS.201 | Upload 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 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 clinical information systems connecting to the PCEHR System.

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

| Req No | 017836 | Priority | Mandatory |
|---|---|---|---|

**Preventing healthcare provider access codes from being cached**

After gaining access to a PCEHR by using a PACC or a PACCX, the Clinical Information System **shall not** cache or store the healthcare recipient'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.

**Related use cases** UC.CIS.002

**Additional information** This requirement is derived from the recommendation 4.25 in the PCEHR Privacy Impact Assessment Report [PIA2011]. It is intended to mitigate the privacy risk faced by healthcare recipients where a provider organisation gains access to a healthcare recipient's PCEHR by re-using a previously supplied access code even though that healthcare recipient 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 recipient, the PCEHR System allows the healthcare recipient 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 recipient, the provider is to avoid re-using the access codes previously supplied by the healthcare recipient. Therefore the CIS, 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.

| Req No | 017839 | Priority | Mandatory |
|---|---|---|---|

**Automatic and manual document uploads to the PCEHR System**

The Clinical Information System **shall** either:

- Require an explicit command by the CIS User for uploading a clinical document to the PCEHR System;

OR

- Provide a mechanism to preclude any supported clinical document from being automatically uploaded to the PCEHR System.

**Related use cases** UC.CIS.201, UC.CIS.202

**Additional information** This requirement is derived from the recommendation 5.31 in the PCEHR Privacy Impact Assessment Report [PIA2011]. It allows for the clinician to make a decision regarding information that warrants uploading to the PCEHR and is intended to mitigate the risk of a healthcare provider organisation inadvertently uploading a clinical document potentially leading to:

- Disclosing sensitive information such as pregnancy termination, drug treatment, sexual or mental health

matters (at least without a specific consent from the healthcare recipient); or

- Violating certain restrictions placed upon by state and territory-based legislations on when a healthcare provider may upload some records, such as records which contain information about a healthcare recipient's HIV status.

This requirement does not mandate the system to provide a user interface for the CIS User to upload clinical documents, and does not preclude the use of batch processing.

This requirement applies before the provideAndRegisterDocumentSet-b service is invoked.

---

**Req No** 017841 **Priority** Mandatory

**Retaining clinical documents uploaded to the PCEHR**

The Clinical Information System **shall** either:

- Retain any clinical document uploaded to the PCEHR System; or
- Retain the original clinical information used to generate the clinical document uploaded to the PCEHR;

to meet requirements for relevant health records legislation, audit and business requirements.

**Related use cases** UC.CIS.201, UC.CIS.202

**Additional information** The intent of this requirement is to enable the healthcare provider organisation using the CIS to keep a record of the information shared with other healthcare providers.

This requirement applies before the provideAndRegisterDocumentSet-b service is invoked.

---

**Req No** 017842 **Priority** Mandatory

**Identifying clinical documents uploaded to the PCEHR System**

The Clinical Information System **shall** provide a mechanism to identify which clinical documents have been uploaded to the PCEHR System.

**Related use cases** UC.CIS.201, UC.CIS.202

**Additional information** The intent of this requirement is to enable the CIS User to identify a previously uploaded document that may need to be superseded or removed due to invalid or erroneous content. Without this capability in the local system, when the CIS User finds invalid or erroneous content in a clinical document but the CIS User is unaware that it has been uploaded to the PCEHR System, the CIS User may not attempt to supersede or remove that document on the PCEHR System.

The clinical information system may achieve this requirement by:

- Storing the document identifiers of the uploaded documents; or
- Storing the uploaded documents locally; or

---

- Other mechanisms.

This requirement applies after the provideAndRegisterDocumentSet-b service is invoked.

| **Req No** | 017941 | **Priority** | Mandatory |
|---|---|---|---|

**Handling errors received from the PCEHR System**

The Clinical Information System **shall** have a process to handle errors received from the PCEHR B2B Gateway Service.

**Related use cases** UC.CIS.002, UC.CIS.201, UC.CIS.202, UC.CIS.203

**Additional information** The intent of this requirement is to ensure that any error response from the PCEHR System from attempting to gain access to a PCEHR, upload, supersede or remove a clinical document is communicated to a relevant CIS User so that appropriate actions can be taken. When the CIS User finds invalid or erroneous content in a previously uploaded document and attempts to remove or supersede it on the PCEHR System, the CIS User will be unaware (without this capability in the CIS) that their request has failed, causing the invalid or erroneous information to remain in the PCEHR System. Similarly, when the CIS 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 CIS should alert the CIS User when it receives some of the PCEHR errors including, but not limited to:

- PCEHR_ERROR_2501: Document not found (when *attempting to remove a clinical document that no longer exists in the PCEHR System*);
- PCEHR_ERROR_5101: PCEHR not found (*when attempting to gain access to a PCEHR that does not exist or that is inactive*);
- PCEHR_ERROR_5102: PCEHR is found but access code is required (*when attempting to gain access to a PCEHR without a code but that PCEHR is protected with a PACC*);
- PCEHR_ERROR_5103: PCEHR 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 PCEHR where the provider organisation's access has been revoked by the healthcare recipient*);
- Any other error where the error description contains sufficient information to guide the CIS User to take an appropriate action.

For any other errors not listed above, a warning or alert may be raised with the CIS User. Such errors should be logged with sufficient details for review and resolution by a local

system administrator.

| Req No | 018634 | Priority | Mandatory |
|---|---|---|---|

**Validating the integrity of clinical documents downloaded from the PCEHR System**

The clinical information system **shall** verify the CDA package hash value of a clinical document package downloaded from the PCEHR System and it **shall** indicate if the downloaded clinical document has been modified.

**Related use cases** UC.CIS.204, UC.CIS.301

**Additional information** This is intended to mitigate the risk of a clinical document being tampered with or corrupted when it is downloaded from the PCEHR System to the local CIS.

This requirement applies after invoking the retrieveDocument service or after involking view services with download a clinical document (such as the getConsolidatedView service).

| Req No | 019041 | Priority | Mandatory |
|---|---|---|---|

**Ability to save or print clinical documents from the PCEHR System**

The Clinical Information System **shall** provide a capability to save or print a clinical document downloaded from the PCEHR System.

**Related use cases** UC.CIS.204, UC.CIS.301

**Additional information** 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 PCEHR because the healthcare recipient may have revoked that organisation’s access to their PCEHR.

This requirement applies after invoking the retrieveDocument service or after involking view services with download a clinical document (such as the getConsolidatedView service).

| Req No | 019042 | Priority | Mandatory |
|---|---|---|---|

**Ability to support the withdrawal of consent to upload a clinical document to the PCEHR System**

The clinical information system **shall** provide an ability to support the withdrawal of the healthcare recipient's consent to upload clinical documents to the PCEHR System, and **shall** prevent them from being uploaded where the consent has been withdrawn.

**Related use cases** UC.CIS.201, UC.CIS.202

**Additional information** This requirement is intended to reduce the risk of a clinical document being uploaded to the PCEHR System despite the withdrawal of consent by the healthcare recipient, 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.

| **Req No** | 019048 | **Priority** | Mandatory |
|---|---|---|---|

**Ability to submit provider access consent codes (PACC or PACCX)**

The clinical information system **shall** provide the CIS User with an option to enter provider access consent codes (PACC or PACCX) to make initial and subsequent requests to gain access to a PCEHR or protected clinical documents.

NOTE: this requirement will be reviewed within 6 months – when the specification is reviewed.

**Related use cases** UC.CIS.002

**Additional information** With this capability in the CIS, the healthcare provider organisation will benefit from being able to access to potentially important clinical information the healthcare recipient has decided to share via the PCEHR System by supplying the healthcare provider with a PACC or PACCX.

Even after a healthcare provider organisation has gained access to a healthcare recipient's PCEHR, the CIS is to continue to allow the CIS User to resubmit the access requests for that PCEHR. Scenarios of successfully gaining access multiple times to a PCEHR 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 recipient has modified the healthcare provider access control settings after a healthcare provider organisation gained access to their PCEHR, additional access requests may be required in order to re-gain access to the healthcare recipient's PCEHR.

This requirement does not suggest that the CIS should store or cache provider access consent codes for the purpose of gaining access multiple times to a PCEHR. In fact, storing or caching PACC or PACCX is prohibited (refer to Requirement 017836).

This requirement invokes the gainPCEHRAccess service.

| **Req No** | 019100 | **Priority** | Mandatory |
|---|---|---|---|

**Use of a valid Individual Healthcare Identifier**

When accessing the PCEHR System the Clinical Information 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 PCEHR System) that is connected to the HI Service.

The relevant HI Use Cases and software requirements are documented in the PCEHR CIS Conformance Assessment Scheme [CCAGG2012].

| | |
|---|---|
| **Related use cases** | UC.CIS.201, UC.CIS.202, UC.CIS.203, UC.CIS.204, UC.CIS.001, UC.CIS.002, UC.CIS.301 |
| **Additional information** | This requirement is intended to mitigate the risk of a healthcare provider organisation associating health information sent to or retrieved from the PCEHR System to the wrong healthcare recipient due to an incorrect Healthcare Identifier allocation in the local system. This may lead to:<br>• Delay in or lack of treatment to the patient or delivery of treatment to the wrong patient; and<br>• 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 PCEHR. |

## 3.2 Conditional requirements

This section lists the conditional software conformance requirements for clinical information systems connecting to the PCEHR 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 clinical information system supports none of the use cases related to a conditional conformance requirement then the clinical information does not need to support that requirement.

| | | | |
|---|---|---|---|
| **Req No** | 017887 | **Priority** | Conditional |

**Identifying locally created documents removed from the PCEHR System**

If the Clinical Information System uploads clinical documents that are removed from the PCEHR System by the healthcare provider organisation, it **shall** provide an ability to identify which locally created clinical documents have been removed from the PCEHR System.

| | |
|---|---|
| **Related use cases** | UC.CIS.203 |
| **Additional information** | This is intended to minimise the risk of a CIS User re-uploading a document to the PCEHR System without realising that another CIS User has already removed it due to obsolete or erroneous content.<br><br>This requirement does not mandate a specific approach to identify locally created clinical documents removed from the PCEHR 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. |

| | | | |
|---|---|---|---|
| **Req No** | 018338 | **Priority** | Conditional |

**Ability to supersede clinical documents**

If the Clinical Information System supports the upload of documents other than Shared Health Summary, the Clinical Information System **shall** provide an ability to supersede previously uploaded clinical documents where there is a change or an error in the data used to create the uploaded clinical documents.

| | |
|---|---|
| **Related use cases** | UC.CIS.202 |
| **Additional information** | This requirement is intended to minimise the risk of the presence of inappropriate, invalid or obsolete clinical documents in the PCEHR System. When the CIS User finds errors or invalid information in an uploaded document, the CIS User will not be able to supersede that document on the PCEHR System (without this capability in the CIS) 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.<br><br>This requirement mandates that the CIS provides an ability to supersede existing clinical documents on the PCEHR System. The exception is a Shared Health Summary as it cannot be superseded[2]. If the CIS uploads Shared Health Summary only and not any other types of clinical documents, the CIS is not required to supersede clinical documents on the PCEHR System.<br><br>This requirement invokes the provideAndRegisterDocumentSet-b service. |

| | | | |
|---|---|---|---|
| **Req No** | 019377 | **Priority** | Conditional |

**Ability to remove clinical documents**

If the Clinical Information System has the ability to upload documents to the PCEHR System, the Clinical Information System **shall** provide an ability to remove previously uploaded clinical documents where there is a change or an error in the data used to create the uploaded clinical documents.

| | |
|---|---|
| **Related use cases** | UC.CIS.203 |
| **Additional information** | This requirement is intended to minimise the risk of the presence of inappropriate, invalid or obsolete clinical documents in the PCEHR System. When the CIS User finds errors or invalid information in an uploaded document, the CIS User will not be able to remove that document on the PCEHR System (without this capability in the CIS) and all healthcare providers who have access to that document may use the information in the document without knowing that it |

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

contains errors or invalid information.

This requirement mandates that the CIS provides an ability to remove existing clinical documents on the PCEHR System.

This requirement invokes the removeDocument/DeregisterDocument service.

| **Req No** | 018721 | **Priority** | Conditional |
|---|---|---|---|

**Identifying clinical documents downloaded from the PCEHR System**

If the clinical information system stores clinical documents downloaded from the PCEHR System, the clinical information system **shall** have a mechanism to indicate to the CIS User:

- That the clinical document being viewed was downloaded from the PCEHR System; and
- The date and time it was downloaded from the PCEHR System.

**Related use cases** UC.CIS.204, UC.CIS.301

**Additional information** This requirement enables the CIS User to be informed that the clinical document being viewed was downloaded from the PCEHR System and also when it was downloaded. This is to encourage the CIS User to make a better informed decision on whether they should check for a more up-to-date version on the PCEHR System.

This requirement applies after invoking the retrieveDocument service or after involking view services with download a clinical document (such as the getConsolidatedView service).

| **Req No** | 019116 | **Priority** | Conditional |
|---|---|---|---|

**Conditions of emergency access**

If the Clinical Information System supports gaining an emergency access to a healthcare recipient's PCEHR, it **shall** display the conditions of emergency access at time intervals appropriate to the clinical settings before asserting emergency access to the PCEHR.

**Related use cases** UC.CIS.002

**Additional information** The CIS User needs to be made aware that they need to abide by the emergency access conditions when gaining emergency access to a PCEHR.

Once emergency access has been asserted by an organisation to a PCEHR and provided that the emergency access has not expired, the CIS is not expected to display the message again.

Suggested text for the CIS 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 clinical information systems connecting to the PCEHR 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.

| **Req No** | 019108 | **Priority** | Recommended |
|---|---|---|---|

**Ability to retrieve a list of clinical documents and a list of historical versions of a document**

The Clinical Information System **should** provide a mechanism to retrieve:

- A list of clinical documents associated with a healthcare recipient's PCEHR (registryStoredQuery service); and
- A list of historical versions of a particular clinical document from the PCEHR System (getChangeHistoryView service).

**Related use cases** UC.CIS.204

**Additional information** The intent of this requirement is to help maximise the benefits of the PCEHR System to the healthcare provider organisation using the CIS. It is intended to facilitate:

- Retrieving a clinical document from the PCEHR System. (The local system needs to obtain the document identifier of an existing clinical document in order to retrieve it from the PCEHR System. The PCEHR System returns document identifiers to the CIS as part of the registryStoredQuery operation.); and
- Checking for a more up-to-date version of a document where the CIS stores the downloaded documents locally. (The PCEHR System returns the list of historical versions of a clinical document to the CIS as part of the getChangeHistoryView operation.)

| **Req No** | 019118 | **Priority** | Recommended |
|---|---|---|---|

**Sort and filter lists of clinical documents from the PCEHR System**

The Clinical Information System **should** provide an ability to sort and filter the lists of clinical documents retrieved from the PCEHR System.

**Related use cases** UC.CIS.204

**Additional information** This is intended to mitigate the risk of being unable to find relevant clinical documents for a particular event or care

episode by the CIS User.

This requirement applies after registryStoredQuery or getChangeHistoryView service is invoked.

| **Req No** | 019119 | **Priority** | Recommended |
|---|---|---|---|

**Patient demographic information in downloaded clinical documents versus local records**

The Clinical Information System **should** provide a warning to the CIS User if the healthcare recipient's demographic information in a clinical document downloaded from the PCEHR System does not match the demographic information in the local healthcare recipient's record.

**Related use cases** UC.CIS.204, UC.CIS.301

**Additional information** This is intended to mitigate the risk of a downloaded clinical document being associated to the wrong patient record in the CIS. Core demographic details of a healthcare recipient include:

- Family name;
- Sex; and
- Date of birth.

This requirement applies after invoking the retrieveDocument service or after involking view services with download a clinical document (such as the getConsolidatedView service).

| **Req No** | 019378 | **Priority** | Recommended |
|---|---|---|---|

**Auditing capability**

The Clinical Information System **should** have the capability to audit interactions with the PCEHR System.

**Related use cases** UC.CIS.001, UC.CIS.002, UC.CIS.201, UC.CIS.202, UC.CIS.203, UC.CIS.204, UC.CIS.301

**Additional information** Local auditing of significant transactions is considered good software practice, and may be important from a medico-legal perspective.

| **Req No** | 019429 | **Priority** | Recommended |
|---|---|---|---|

**Use of a valid Individual Healthcare Provider Identifier**

When accessing the PCEHR System the Clinical Information 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 PCEHR System) that is connected to the HI Service.

The relevant HI Use Cases and software requirements are documented in

| | |
|---|---|
| | the PCEHR CIS Conformance Assessment Scheme [CCAGG2012]. |
| **Related use cases** | UC.CIS.201, UC.CIS.202 |
| **Additional information** | The requirement does not apply to the healthcare identifier of the healthcare provider organisation (HPI-O) as the HPI-O is validated by the PCEHR System. The requirement also does not apply to other HPI-Is in the clinical document, such as those of the receiving health provider. |

# Appendix A: References

Appendix B lists all the documents referred to by this document. At the time of publication, the document versions listed below were valid. However, readers are encouraged to refer to most recent version of these documents.


| | |
|---|---|
| [AS5021] | AS 5021:2005 - The language of health concept representation, Standards Australia, 2005 |
| [CCAGG2012] | Clinical Information Systems Connecting to the PCEHR System: Conformance Assessment Scheme, eHealth CCA Governance Group, 2012 |
| [DOHA2011] | Concept of Operations: Relating to the introduction of a Personally Controlled Electronic Health Record System – September 2011 Release, Department of Health and Ageing & NEHTA, 2011 |
| [HIACT2010] | Healthcare Identifiers Act 2010 |
| [NEHTA2012] | Clinical Information Systems Connecting to the PCEHR System: Use Cases, NEHTA, 2012 |
| [PIA2011] | PCEHR Privacy Impact Assessment Report, Department of Health and Ageing, 2011 |

# Appendix B: Change Log

This appendix lists the major changes and fixes applied to this document.

| ID | Section | Change Detail | Rationale |
|---|---|---|---|
| 1 | 2.6 | Additional web services have been added to Table 1. | Risks with using these web services have been mitigated in version 1.5 of the document. |
| 2 | 3 | Additional use cases have been added to Table 2. | More use cases have been defined for a clinical information system to use PCEHR services. |
| 3 | 3.1 | New use cases were added to existing conformance requirements. | Additional use cases were needed for the additional PCEHR services. |

**Changes from Version 1.4 (15 June 2012) to Version 1.5 (6 September 2012)**