nehta

PCEHR Participation and Authorisation Functional Overview

Version 1.0 — 9 December 2011

Final

National E-Health Transition Authority

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

Document Information

Approver	PCEHR Design Authority
Owner	Head of PCEHR
Contact officer	eSolution Manager
Contributors	PCEHR Project Team

Version History

Date	Version	Name	Comments
9 December 2011	1.0	PCEHR Design Authority	Approved for release

This page is intentionally blank

Table of Contents

Preface

Purpose

The purpose of this document is to aid implementers of applications interfacing with the national PCEHR system, by contextualising the PCEHR B2B interface with the PCEHR's Participation and Authorisation (P&A) framework. This document complements the PCEHR interface specifications, by showing how the logical service interfaces relate to the Participation and Authorisation framework of PCEHR.

The PCEHR system has a range of controls available to individuals. What these controls do, impacts the behaviour of the B2B interface. For a third party implementer, it may not always be evident how a particular control is related to an operation in the interface. This document will, within the context of the logical service specifications, explain these relationships.

Intended audience

This specification is intended for:

- Developers and implementers of software products which seek to interact with the PCEHR System
- Developers and implementers of PCEHR Conformant Repositories, Clinical Information Systems and Conformant Provider and Consumer Portals.
- Jurisdictional eHealth programs
- The Australian health informatics standards development community

Document map

This document is to be read in conjunction with the logical service specifications (LSS) of the PCEHR system B2B interface specifications as highlighted in the figure below.

At the time of publication, the Registration Service and Account Management LSS are not available with the release of this document.

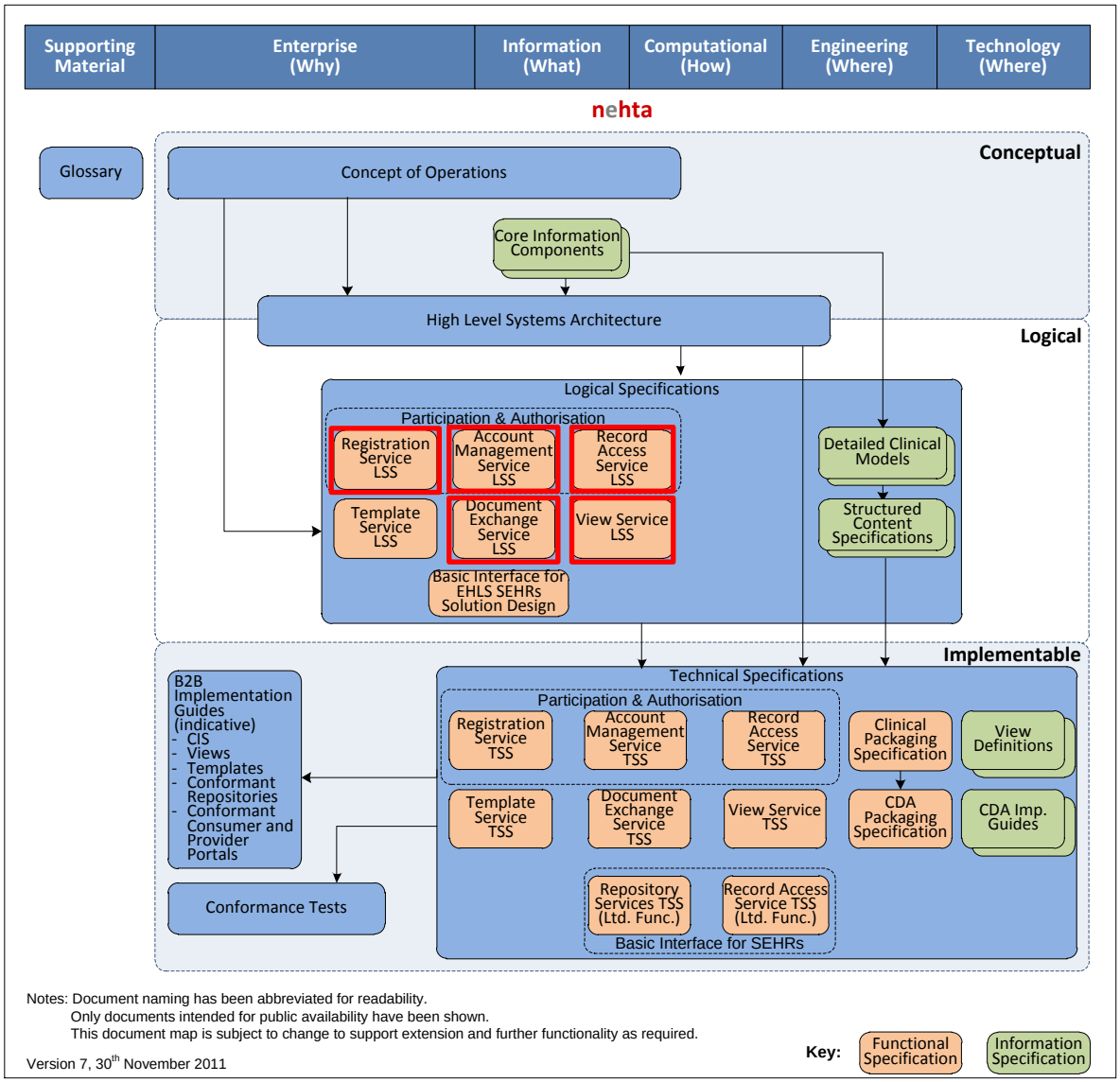

Figure 1 – Document map

Acronyms and Terminology

Please refer to Appendix A for definitions of the acronyms and terminology used in this document.

The keywords SHALL, SHALL NOT, SHOULD and SHOULD NOT in this document are to be interpreted as described in IETF's RFC 2119 [RFC2119].

References

Please refer to Appendix B for details of the references used within this document.

1 Introduction

1.1 Context

The Personally Controlled Electronic Healthcare Record (PCHER) System will be launched in July 2012 and will allow individuals, their representatives, healthcare organisations and providers, to manage and share electronic health records based on a regime of personally controlled access and user entitlements that promote a high level of maturity and interoperability.

The PCEHR system will expose a B2B (business to business) Interface where applications such as clinical information systems can connect.

Details of the operations exposed via the B2B Interface are organised and defined in a series of logical and technical service specifications covering:

- Registration
- Account Management
- Record Access [PCEHR_RAS_LSS]
- View [PCEHR_VS_LSS]
- Document Exchange [PCEHR_DE_LSS].

This document supplements these specifications by showing their context within the Participation and Authorisation framework of the PCEHR System.

For further information on the PCEHR System, please refer to the Concept of Operations [PCEHR_CON_OPS].

1.2 Scope of Document

1.2.1 In Scope

This document explains the relationship between the participation and authorisation rules of the PCEHR System, and the operations exposed through the B2B Interface.

1.2.2 Out of Scope

The following are out of scope of this document.

- The complete set of requirements for the PCEHR system.
- The internal design for national PCEHR components.
- The specification of Conformant Repositories, Conformant Portals or Clinical Information Systems.
- The full listing of all system interfaces for interacting with the PCEHR System.
- Business processes associated with interactions with, and usage of, the PCEHR System.
- Logical Service Specifications (refer to appropriate LSS)
- Technical Service Specifications (refer to appropriate TSS)
- P&A administrative and support related operations which are internal to the PCEHR System and performed by the PCEHR System Operator.

2 Key PCEHR Roles

This section provides a short overview of the key roles involved with the PCEHR System. For a more comprehensive view, please refer to the PCEHR Concept of Operations [PCEHR_CON_OPS].

The core set of terms used within the PCEHR are specified in the PCEHR System - Glossary [PCEHR-SYSTEM-GLOSSARY].

2.1 Authorised Representative

An "Authorised Representative", in relation to an Individual, means:

- an attorney for the Individual under an enduring power of attorney, or
- a guardian or person responsible as defined within relevant state/territory legislation, or
- a person having parental responsibility for that Individual, if the Individual is a Child, or
- a person who is otherwise empowered under law to exercise any functions as an agent of or in the best interests of the Individual.

An Authorised Representative is thus a person recognised under law, with the authority to "stand in the shoes" of another. Examples of Authorised Representatives include parents of minors and those holding a Medical Power of Attorney.

In relation to the PCEHR, Authorised Representatives have all access rights, privileges and permissions that would otherwise be afforded to the Individual.

Individuals under such an authority are considered to lack decision making capacity and are denied any access to their record unless approved by their Authorised Representative.

2.2 Nominated Representative

A Nominated Representative has no authority under law, but is afforded access to an individual's record by the individual themselves.

The Individual defines what permissions the Nominated Representative has in relation to their PCEHR.

2.3 Authorised User

An Authorised User, is an employee of a healthcare organisation who is authorised by that organisation to access information held by the PCEHR system.

All Authorised Users must be identified to the PCEHR System Operator by Name.

Only Authorised Users who are acting on behalf of Healthcare Provider Organisations may post information to an Individual's PCEHR.

2.4 Individual

An Individual is a person who is, or could be, seeking care in Australia. Individual is sometimes referred to as a patient, client or consumer. For the purposes of the PCEHR System, an Individual must have been assigned an Individual Healthcare Identifier (IHI) by the Healthcare Identifier Service.

2.5 Healthcare Provider

A healthcare provider is an individual who:

- has provided, provides, or is to provide, healthcare; or
- is registered by a registration authority as a member of a particular health profession.

For the purposes of the PCEHR, a Healthcare Provider that has chosen to participate must be an Authorised User acting on behalf of a Healthcare Organisation.

2.6 Identified Healthcare Provider

An Identified Healthcare Provider is a healthcare provider who has been assigned a Healthcare Identifier (HPI-I) by the Healthcare Identifier Service.

2.7 Healthcare Organisation

A Healthcare Organisation is an organisation that provides healthcare services.

2.8 Identified Healthcare Organisation

An Identified Healthcare Organisation is a healthcare organisation which has been assigned a Healthcare Identifier (HPI-O) by the Healthcare Identifier Service.

3 Key Participation and Authorisation Concepts

This section lists the key Participation and Authorisation concepts that have influenced the design and capability of the P&A Framework. The concepts are presented in this section as an overview. For a more comprehensive view, refer to the PCEHR Concept of Operations [PCEHR_CON_OPS].

3.1 Provider Participation

Access to the PCEHR System is restricted to Identified Healthcare Provider Organisations who have registered their participation in the PCEHR System and consented to the PCEHR Terms and Conditions of Use.

Individual healthcare providers are not required to register their participation in the PCEHR System, but their participation is authorised by a participating healthcare provider organisation (See 2.3 Authorised User on Page 11).

3.2 Provider Authorisation

A provider must not access information in an Individual's PCEHR without their consent.

There are two models available to an Individual which they may select through their PCEHR Access Controls which define how consent may be provided:

- Basic Settings
  "I consent to any provider engaged in my care to access my record."
- Advanced Settings
  "I consent to specific healthcare organisations accessing my record only when I provide them with my Provider Access Consent Code (PACC)."

Notes:

- Consent is considered to be granted at organisational level.
  If an Individual grants access to a specific provider, consent is considered to have been given to the provider's participating organisation.
- An Individual may withdraw their consent verbally on presentation.
  Despite having established Basic Settings or previously provided a PACC, an Individual may request a provider not to access their record.
- Access without explicit consent is permitted in an Emergency situation
  An Emergency is defined as being "a serious threat to life, health or public safety."
- A provider may always assume consent to post information to an Individual's record unless the Individual specifically requests them not to.

3.3 Access Control Settings

Individuals have two access control models available to them:

- Open Access
- Provider Access Code

3.3.1 Open Access

If the Individual elects to operate their PCEHR under an Open Access model, any healthcare organisation involved in the Individual's healthcare may access their PCEHR (unless the Individual specifically requests otherwise).

3.3.2 Provider Access Consent Code (PACC)

The PACC is an access code that the individual may elect to use for their PCEHR. The individual provides this access key at the point of care so that the healthcare organisation can access their PCEHR. If the Individual elects to set a PACC, healthcare organisations cannot access the Individual's PCEHR unless they are explicitly provided with that PACC by the Individual at the point of care.

3.4 Disclosure Indicator

The Disclosure Indicator allows the Individual to elect whether to disclose the existence of their PCEHR. It is initially set and maintained by the Individual at registration. The Individual can change it at any time in the same way that they can change other access controls.

For example, if the individual elects to disclose the existence of their PCEHR an integrated system can elect to highlight this to its user to facilitate easy access to the PCEHR when it is available.

3.5 Provider Access List

An individual will have the ability to control which healthcare organisations can access their PCEHR using a series of access control settings.

When an organisation is authorised to access an Individual's PCEHR, they are added to the Individual's 'Provider Access List'.

The Provider Access List maintains a set of healthcare organisations that have accessed an individual's PCEHR and tracks:

- The 'Access Level' that the healthcare organisation has been given (discussed in more detail later in this section)
- The authorisation end date

An Individual may revoke a healthcare organisation's access or remove them from the Provider Access List at any time.

The 'Provider Access List will also maintain the 'Access Level' that a healthcare organisation has been given. For example, if an organisation is authorised to access the PCEHR by being provided a PACCX (see section 3.6.1 for PACCX), they are added to the 'Provider Access List' with an access level of 'Limited Access'.

Once an organisation is added to the Provider Access List, no further authorisation is required until the authorisation expires or the Individual specifically revokes the organisation's access.

Access to a PCEHR is controlled at the healthcare provider organisation (HPI-O) rather than individual healthcare provider (HPI-I) level. This ensures that access to a PCEHR reflects current healthcare organisations' consent frameworks.

3.6 Document Level Access Controls

Individuals also have the option of controlling access to specific clinical documents relating to their PCEHR.

3.6.1 Provider Access Consent Code – Extended (PACCX)

The PACCX option is an access code that authorises a healthcare organisation to access to documents marked as 'limited access'. Providing PACCX access to a healthcare organisation is one way in which an Individual can provide access to their 'limited access' documents. The other way, is for the individual to upgrade the healthcare organisation's access level via their Individual portal/call centre etc.

Of note, Individuals can set an access level for documents without setting a PACCX for their PCEHR.

The allowable access levels are as follows.

3.6.1.1 General Access

General Access – a document with this setting is accessible by all healthcare organisations on the Individual's Provider Access List

3.6.1.2 Limited Access

Limited Access – a document with this setting is only accessible by healthcare organisations that have been given specific access to these documents by the individual.

There are two options for authorising a healthcare organisation to access documents marked as 'Limited Access':

- The individual creates a special Provider Access Consent Code (PACCX) which is given to the healthcare organisation at the point of care instead of the PACC.
- The individual upgrades the healthcare organisation's access level via their Individual portal/call centre etc.

3.7 Document and Provider Access Level Interactions

An Individual may assign Access Levels to Documents within their PCEHR.

The Access Level determines whether the Document may be viewed by particular healthcare organisations.

The Access Level assigned to a Document may be:

- "General Access"
  The Document is accessible to any provider with access to the record.
- "Limited Access"
  The Document is accessible only to a limited set of providers.

Participating Healthcare Organisations may be granted three levels of access to read documents on an Individual's PCEHR. These are:

- "General Access"
  Providers in the organisation may view General Access Documents only.

- "Limited Access"
  Providers in the organisation may view both General and Limited Access Documents.
- "Revoked"
  Providers in the organisation may not view any Documents.

The View Access Level assigned to different provider organisations is maintained in the PCEHR's Provider Access List (PAL).

The PAL also allows an Individual to define what Document Access Level should be ascribed to any document posted by that organisation. This is referred to as their Post Access Level.

Table 1 - Access List (Example)

Organisation	View	Post
North Shore Hospital	General	General
Southern Medical Centre	Limited	General
Eastern Sexual Health Clinic	General	Limited
Western Psychology	Limited	Limited
Central Dental	Revoked	General

Table 2 - Document List (Example)

#	Document	Author Organisation	Access Level
1	Discharge Summary	North Shore Hospital	General
2	Event Summary	Southern Medical Centre	General
3	Prescription	Eastern Sexual Health Clinic	Limited
4	Specialist Letter	Western Psychology	Limited
5	Referral	Central Dental	General

Table 3 – Document Visibility (Example)

Organisation	Document				
	1	2	3	4	5
North Shore Hospital	Y	Y			Y
Southern Medical Centre	Y	Y	Y	Y	Y
Eastern Sexual Health Clinic	Y	Y	Y		Y
Western Psychology	Y	Y	Y	Y	Y
Central Dental					

In **Error! Reference source not found.**, the Access List illustrates how View and Post Access Levels may be assigned to different organisations. The Document List in **Error! Reference source not found.** illustrates how different Access Levels may be applied to different documents.

Based on the example, the "Document Visibility" in **Error! Reference source not found.** illustrates which documents from the Document List are visible to providers in the different organisations.

- North Shore Hospital may only View General Access Documents.

- Southern Medical Centre and Western Psychology have been granted Limited Access and may view both General and Limited Access Documents.
- Eastern Sexual Health Clinic has General Access and may view General Access Documents PLUS the Limited Access Document they posted.
- Access for Central dental has been revoked and they may not view any documents.

3.8 Emergency Access

A healthcare organisation may assert 'Emergency Access' if an Individual is in need of emergency care and is not capable of giving or communicating consent.

Emergency access:

- Bypasses all access control settings (including allowing access where the Individual has elected to set a PACC or the healthcare organisation's access to the PCEHR has been revoked by the Individual).
- Allows the healthcare organisation to access documents marked as 'Limited Access'.
- Expires 5 days after last access.

4 PCEHR B2B Services

This section puts the B2B services, as described in the logical services specifications, in the context of the Participation and Authorisation framework. The PCEHR B2B gateway is broken down into five functional areas:

1. Registration Services
2. Account Management Services
3. Record Access Services
4. Document Exchange Services
5. Views Services

The figure below illustrates these five groups in the context of P&A.

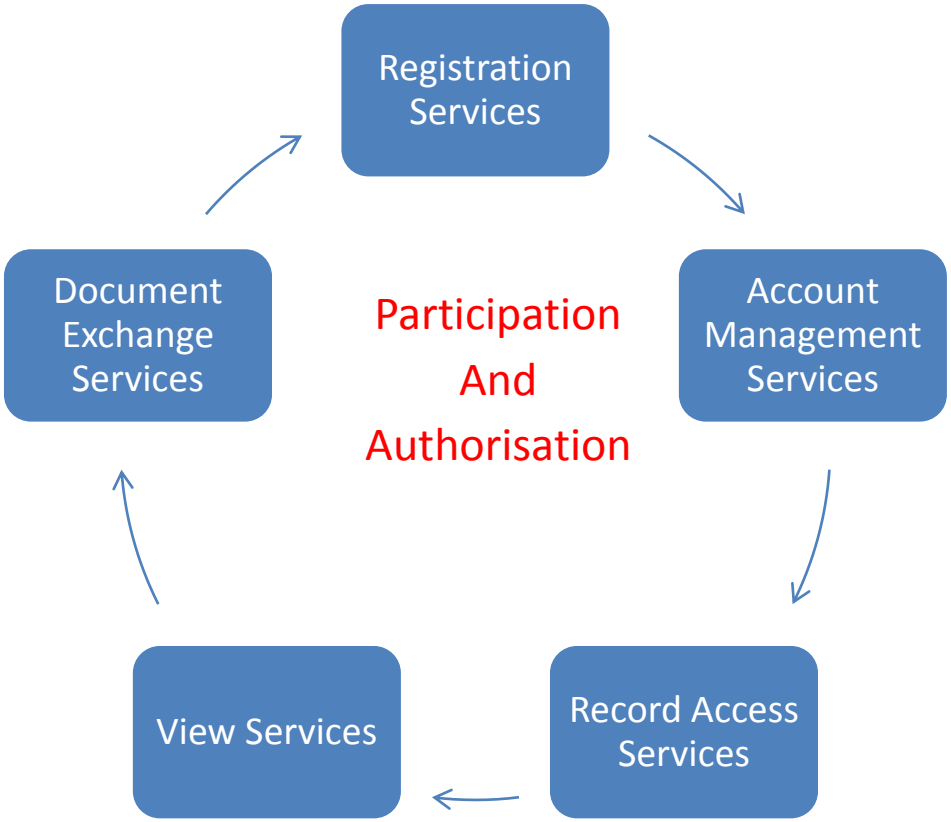

Figure 2 P&A relation to B2B Services

The remainder of this section describes these five services with respect to the Participation and Authorisation entities outlined in section 3.

4.1 Registration Services

At the time of writing this document, the Registration Logical Service specification has not yet been developed. This section will therefore not reference any material in the Registration Services LSS.

Registration Services deal with registrations of:

- Providers and Healthcare Organisations
- Individuals
- Conformant Repositories and Conformant Portals

- Conformance and Compliance accredited system.

4.1.1 Registration of Providers and Healthcare Organisations

For any Healthcare organisation to access a PCEHR, that organisation must be registered to use the PCEHR system. The registration of a Provider Organisation is based on the Provider Organisation's Identifier, the HPI-O.

When accessing the PCEHR, the HPI-O is validated against a directory of registered HPI-Os and access is granted if and only if the HPI-O appears in the directory of registered healthcare organisations.

For certain access channels individual providers need to be registered. Individual providers are registered based on a provider identifier, the HPI-I. HPI-Is are associated with HPI-Os. An association between e.g. a HPI-I *n* and a HPI-O *m* means that *n* can act on behalf of *m*. The cardinality of this association is many to many. When accessing via the provider portal the directory of registered HPI-Os and their associated HPI-Is is used to ensure a provider is associated with an organisation that has registered to use the PCEHR system.

4.1.2 Registration of Individuals

The PCEHR system is an opt-in system. For all individuals an explicit registration is required before a PCEHR record can exist for that individual. Any activity with respect to an individual in the context of the PCEHR system cannot be done until the individual has registered for a PCEHR record.

An individual can register via a number of channels. The PCEHR Concept of Operations defines those channels in further detail.

4.1.3 Conformant Repositories and Conformant Portals

Any system that wishes to act in the capacity of a Conformant Repository or a Conformant Portal, must be registered within the PCEHR system. If a system tries to access as, say, a conformant repository, the access will be denied by the PCEHR system.

The number of conformant repositories and portals will not be very large and registering each in the PCEHR system is therefore feasible.

4.1.4 Conformance and Compliance accredited system

For e.g. clinical information systems, a conformance and compliance accreditation process must to be passed for that system to access the PCEHR system.

When a system has passed compliance and conformance tests, the software name and version will be registered in the PCEHR system.

For example, a GP practice, to access the PCEHR via a clinical information system they need to:

- Have their HPI-O registered with the PCEHR System, and
- Use a CIS system that is registered with the PCEHR system.

Note that these two registrations are independent. If a practice changes to another accredited CIS system, they do not need to perform any additional registration actions in the PCEHR.

4.2 Account Management Services

At the time of writing this document, the Account Management Logical Service specification has not yet been developed. This section will therefore not reference any material in the Account Management Services LSS.

Account Management Services provide means for individuals with a registered PCEHR record to manage their personal controls.

There are a number of personal controls available to individuals to set. These were introduced in section 3.

The Account Management Service enables users to manage the following:

Table 4 Account Management Services

P&A Concept	Actions	Comment	Default
PACC	Create, Update, Delete	Relates to PCEHR Record access	None
PACCX	Create, Update, Delete	Relates to document access level	None
Provider Access List	Change access level, revoke access		
Disclosure Indicator	Update		Disclose
Nominated Representative	Create, Update, Delete		None
Default Write access level for PCEHR	Update	Default write document access level for new organisations	General
Read / Write access levels per provider organisation	Update	Read and write access levels for individual organisation	General
Document Access level	Update	For each document the access level can be set	General
Notification Preferences	Set, Update	Events where notifications shall be sent and the means by which notifications are sent can be set.	None

4.3 Record Access Service

The Record Access Service provides operations to access PCEHR records for healthcare organisations.

The Record Access logical service specification defines three operations:

- doesPCEHRExist
- gainAccessToPCEHR
- searchPCEHR

4.3.1 Does PCEHR exist

This operation (doesPCEHRExist) is used to gain the required information on how to access a particular PCEHR. Consequentially, a PCEHR 'interfaced' system, has the option of invoking this operation when a local patient record is opened to put some visual indicator on the screen that there is a PCEHR for the patient that can be accessed. The doesPCEHRExist operation considers a range of PCEHR settings and responds according to the table below:

Table 5 Does PCEHR Exist behaviour

PCEHR Access Settings				Does PCEHR Exist Responses	
Open Access	**Advertised (*Disclosure Indicator*)**	**On PAL**	**Revoked**	**PCEHR Exists**	**Access Code Required**
T	T	F	F	T	WithoutCode
T	T	T	F	T	AccessGranted
T	T	T	T	F	NULL
F	T	F	F	T	WithCode
F	T	T	F	T	AccessGranted
F	T	T	T	F	NULL
T	F	F	F	F	NULL
T	F	T	F	T	AccessGranted
T	F	T	T	F	NULL
F	F	F	F	F	NULL
F	F	T	F	T	AccessGranted
F	F	T	T	F	NULL
Open Access with PACCX	Advertised (*Disclosure Indicator*)	On PAL	Revoked	PCEHR Exists	Access Code Required
T	T	F	F	T	WithoutCode
T	T	T	F	T	AccessGranted
T	T	T	T	F	NULL
T	F	F	F	F	NULL
T	F	T	F	T	AccessGranted
T	F	T	T	F	NULL

4.3.1 Gain access to PCEHR

This operation (gainAccessToPCEHR) is used to access a PCEHR. Once this operation is successfully executed, the participating healthcare organisation is added to the Provider Access List with their access privileges. The doesPCEHRexist

operation (See previous section) will return information guiding whether gainAccessToPCEHR is required to be invoked or not. In the general case, the gainAccessToPCEHR operation is only needed the first time an organisation accesses a PCEHR and when any changes have occurred on the PCEHR that require an organisation to regain access. Specifically, the gainAccessToPCEHR is required to be run as per the table below:

Table 6 gainAccessToPCEHR invocation

DoesPCEHRExist PCEHR Exist	DoesPCEHRExist Access Code Required	Invoke gainAccessToPCEHR
T	WithoutCode	Yes Access code is not required
T	F	Not Required
F	NULL	Yes, access code may be required
T	WithCode	Yes, access code required

4.4 View Services

The View Service exposes a series of views. The views present information that the healthcare organisation is entitled to access. To access any view the organisation must be on the provider access list with either general or limited access. The Record Access service (section 4.3) provides the means to gain access and thus be added to the provider access list of the PCEHR.

The owner of a PCEHR can access all views with all information that relates to his/her PCEHR. A provider can access all views but their read access level will determine what information is present in the view.

The View Services expose a series of operations:

- getConsolidatedView
- getChangeHistoryView
- getAuditView
- getDocumentList

4.4.1 Get Consolidated View

This operation (getConsolidatedView) retrieves the consolidated view for a particular PCEHR and returns it to the caller. The consolidated view is derived from a range of other documents in the system. The consolidated view is returned as a self-contained information unit. The returned consolidated view is compliant to the consolidated view specification.

Table 7: getConsolidatedView

P&A Concept	Positive case	Negative case
Provider Access List – General	Only documents with general access and documents authored by the healthcare organisation will be used to construct the consolidated view.	Any organisation not on the access list cannot execute this operation.
Provider Access List - Limited	If some documents are limited access and the accessing organisation has general access, any limited access documents will not be used to construct the consolidated view.	N/A
Provider Access List - Revoked	Cannot access any views.	N/A

4.4.2 Get Change History View

The operation (getChangeHistoryView) returns the list of previous versions of a document over a given time period.

Table 8 getChangeHistoryView

P&A Concept	Positive case	Negative case
Provider Access List – General	Only documents with general access will be available to get the history view over.	Any organisation not on the access list cannot execute this operation.
Provider Access List - Limited	Both documents with general and limited access will be available to get the history view over.	N/A
Provider Access List - Revoked	Cannot access any views.	N/A

4.4.3 Get Audit View

This operation (getAuditView) returns a list of actions that have been taken / performed on a PCEHR. The getAuditView operation always returns a list of actions that relates to the invoker. For example, if a healthcare organisation invokes this operation, they can see actions that relate to their own activity. Similarly, if an Individual (or their authorised representative) invokes the operation, it returns actions that have been performed on his / her PCEHR.

Table 9 getAuditView

P&A Concept	Positive case	Negative case
Provider Access List – General	Healthcare organisations can see their own activity. Their access level on the Provider Access List does not affect the view	Any organisation not on the access list cannot execute this operation.
Provider Access List - Limited	Healthcare Organisations can see their own activity. Their access level on the Provider Access List does not affect the view	Any organisation not on the access list cannot execute this operation.
Provider Access List - Revoked	Cannot access any views. However, their previous access is still in the log and will be visible if access is granted to that organisation again.	N/A

4.4.4 Get Document List

The operation (getDocumentList) is used to retrieve a list of available documents for a PCEHR.

The operation does not return the actual documents only identifying meta data associated with the documents:

- Date/ time that the document was created and signed
- Document type information (e.g. Discharge Summary, Event Summary, etc.)
- Name of authoring organisation
- Organisation role (e.g. General Practice, Hospital, etc.)
- Healthcare role of authoring individual (e.g. Endocrinologist)
- Name of authoring individual
- Link to original document.

Table 10 getDocumentList

P&A Concept	Positive case	Negative case
Provider Access List – General	Only meta data for documents with general access and documents authored by the organisation are returned	If the organisation is not on the access list the operation cannot be invoked.
Provider Access List - Limited	Meta data for all documents are returned.	N/A
Provider Access List - Revoked	Cannot access any views	N/A

4.5 Document Exchange Services

The Document Exchange Services provides the means to manage documents in the PCEHR system. Documents can be inserted, removed and retrieved. An individual has full control over their documents and can see them all. Healthcare Organisation access to documents is dependent on their access level.

The operations provided by this service are:

- submitDocument
- retrieveDocument

4.5.1 Submit a document

This operation (submitDocument**)** is used to upload a document to the PCEHR system. This can only be done from CIS / CSP systems, Individual portals or conformant repositories[1]. The submission of a document cannot be done from a provider portal.

Table 11 submitDocument

P&A Concept	Positive case	Negative case
Provider Access List – General	The document will be assigned access level according to the default 'Write Access Level" for that organisation. The default access level setting can be general or limited access.	A provider organisation that is not on the Provider Access List can upload documents. The overall Default Write Access Level for the PCEHR will define if the document will be stored as limited or general access.
Provider Access List - Limited	See above.	See above
Provider Access List - Revoked	A provider with revoked access can upload new or amended documents. If the organisation has been revoked they would be treated as though they are not on the provider access list and would therefore use the overall Default Write Access Level.	N/A

[1] The envisaged common behaviour is for a conformant repository to update the index. There is however no reason why a conformant repository should not be allowed to inject a document.

4.5.2 Retrieve a document

The operation (retrieveDocument) is used to retrieve a document stored in the PCEHR.

Table 12 retrieveDocument

P&A Concept	Positive case	Negative case
Provider Access List – General	Only documents marked as general access and documents authored by the organisation can be retrieved.	A provider organisation not on the provider access list cannot retrieve documents.
Provider Access List - Limited	Both limited and general access documents can be retrieved.	N/A
Provider Access List - Revoked	No document can be retrieved	N/A

4.5.3 Find a document

This operation (findDocuments) searches for one or more documents within a PCEHR based on some search criteria. This operation is related to the getDocumentList (View services) in that it returns meta data for a set of docs. The difference is that this operation has search capabilities and can therefore be used to retrieve a subset of the documents that the getDocumentList returns.

Table 13 findDocuments

P&A Concept	Positive case	Negative case
Provider Access List – General	Only meta data for documents with general access and documents authored by the organisation are returned	If the organisation is not on the access list the operation cannot be invoked.
Provider Access List - Limited	Meta data for all documents are returned.	N/A
Provider Access List - Revoked	No information can be retrieved.	N/A

4.5.4 Remove a document

The removeDocument operation logically removes a document. Documents can only be removed by the author and by the Individual.

Table 14 removeDocument

P&A Concept	Positive case	Negative case
Provider Access List – General	N/A Authoring organisation can always see own documents regardless of access level.	If the organisation is not on the access list the operation cannot be invoked.
Provider Access List - Limited	N/A Authoring organisation can always see own documents regardless of access level.	N/A
Provider Access List - Revoked	N/A	N/A

4.5.5 Register a document

The registerDocument operation is primarily intended to be used by conformant repositories. The operation is used to index a document in the PCEHR system however, the document remains within the conformant repository, as such, will not be stored in the PCEHR system (only the index entry will).

This operation should therefore not be used by say, a CIS system that is not acting as a conformant repository.

Table 15 registerDocument

P&A Concept	Positive case	Negative case
Provider Access List – General	The document will be assigned access level according to the default 'Write Access Level" for that organisation. The default access level setting can be general or limited access.	A provider organisation that is not on the Provider Access List can index documents. The overall Default Write Access Level for the PCEHR will define if the document will be stored as limited or general access.
Provider Access List - Limited	The document will be indexed according to the default upload setting for that organisation. The default upload setting can be general or limited access.	N/A
Provider Access List - Revoked	A provider with revoked access can index new documents. If the organisation has been revoked they would be treated as though they are not on the provider access list and would therefore use the overall Default Write Access Level.	N/A

4.5.6 De-Register a document

An indexed (registered) document can be removed from the index using the deregisterDocument operation by the Individual and authoring organisation.

Table 16 De-registerDocument

P&A Concept	Positive case	Negative case
Provider Access List – General	N/A Authoring organisation can always see own documents regardless of access level.	If the organisation is not on the access list the operation cannot be invoked.
Provider Access List - Limited	N/A Authoring organisation can always see own documents regardless of access level.	N/A
Provider Access List - Revoked	N/A Authoring organisation can always see own documents regardless of access level.	N/A

Appendix A Acronyms and Terminology

The core set of terms used within the PCEHR are specified in the PCEHR System - Glossary [PCEHR-SYSTEM-GLOSSARY].

A.1 Acronyms

Acronym	Explanation
CIS	Clinical Information System
CSP	Contracted Service Provider
HPI-I	Healthcare Provider Identifier Individual
HPI-O	Healthcare Provider Identifier Organisation
IHI	Individual Healthcare Identifier
LSS	Logical Service Specification
TLS	Transport Layer Security
TSS	Technical Service Specification
UML	Unified Modeling Language

VIEW-L 0

A.2 Specialised Terminology

Term	Explanation
Clinical Information System	An Information System used to help support clinical activity.
Conformant Repository	A repository that conforms to the appropriate PCEHR standards and specifications required to ensure interoperability, privacy, integrity and long term availability of the healthcare information it holds.
Consumer Portal	A consumer portal is a nationally operated portal to allow individuals to access their own PCEHR.
Provider Portal	A provider portal complements existing local health record systems by providing an alternative form of access to the PCEHR for healthcare providers.
Service	A Service encapsulates the collaboration which occurs between two or more parties to achieve a goal. Each participant in the service may offer multiple Service Interfaces.
Service Interface	A Service Interface is a logical grouping of operations which be offered by a participant within the context of a Service.
Service Operation	A Service Operation is a specific function which supports communication between two participants.

Appendix B References

Tag	Name	Version Release Date
[PCEHR_CON_OPS]	PCEHR Concept of Operations: relating to a Personally Controlled Electronic Health Record System http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/pcehr-document	0.13.6 September 2011
[PCEHR-SYSTEM-GLOSSARY]	PCEHR System - Glossary	1.08 12/08/2011
[PCEHR_RAS_LSS]	Record Access Service Logical Service Specification	1.0
[PCEHR_VS_LSS]	View Service Logical Service Specification	1.0
[PCEHR_DE_LSS]	Document Exchange Logical Service Specification	1.0