nehta

Logical Service Specification

PCEHR Record Access Service

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

Disclaimer

NEHTA 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. NEHTA 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. The current revision of this document is located on the NEHTA Web site and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

Document Information

Approver	PCEHR Design Authority
Owner	Head of PCEHR
Contact officer	PCEHR Design Team
Contributors	PCEHR Standard, Foundation and Architecture Team

Version History

Date	Version	Name	Comments
	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 define the logical service interfaces and associated conformance points for the PCEHR Record Access Service.

The Record Access Service enables implementers and systems to obtain a PCEHR personal disclosure indicator, search a PCEHR and gain access to a PCEHR.

This specification considers the computational and information viewpoints of the solution and provides logical considerations of these areas. It defines the set of system roles and associated responsibilities and provides context for technical service specifications that follow this specification.

Technical service specifications will provide a realisation of the interfaces for a given technical platform and will not repeat the logical role definitions or conformance points.

Intended Audience

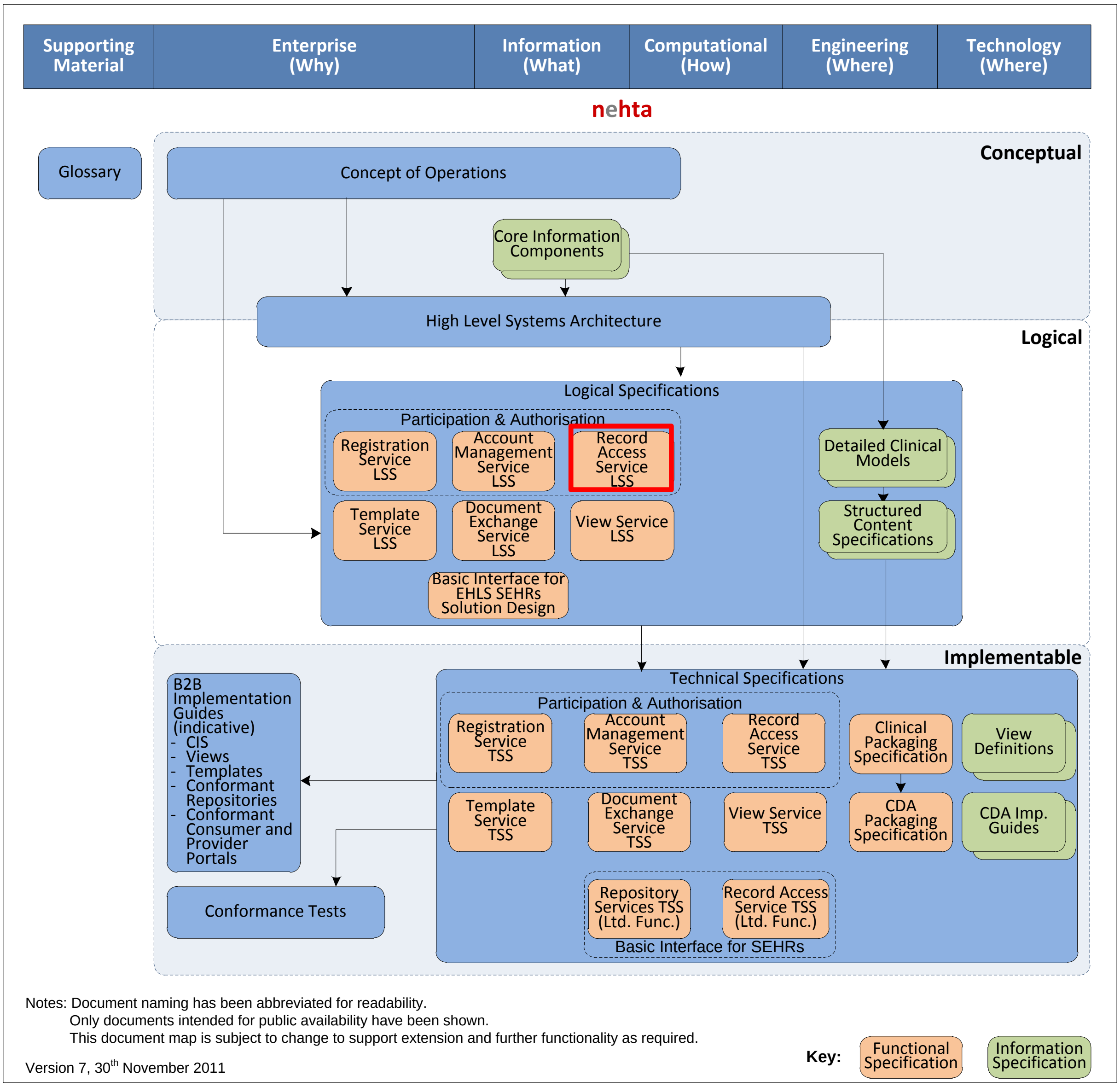
This document is intended for:

- Developers and implementers of the National PCEHR System, Clinical Information Systems seeking to interact with the PCEHR System and PCEHR Conformant Portals (normative).
- Organisations that produce software products which seek to interact with the PCEHR System (normative).
- Jurisdictional eHealth programs (informative).
- The Australian health informatics standards development community (informative).

This is a technical document which makes use of the UML2.3 standard [UML2010]. It is assumed that the audience is familiar with:

- UML and service-oriented architecture concepts and patterns
- The PCEHR Concept of Operations [PCEHR_CON_OPS], September 2011 release
- RM-ODP (Reference Model of Open Distributed Processing) reference model [RM-ODP].

Document Map


Supporting Material
Enterprise (Why)
Information (What)
Computational (How)
Engineering (Where)
Technology (Where)
nehta
Glossary
Concept of Operations
Conceptual
Core Information Components
High Level Systems Architecture
Logical
Logical Specifications
Participation & Authorisation
Registration Service LSS
Account Management Service LSS
Record Access Service LSS
Template Service LSS
Document Exchange Service LSS
View Service LSS
Basic Interface for EHLS SEHRs Solution Design
Detailed Clinical Models
Structured Content Specifications
Implementable
B2B Implementation Guides (indicative)
- CIS
- Views
- Templates
- Conformant Repositories
- Conformant Consumer and Provider Portals
Conformance Tests
Technical Specifications
Participation & Authorisation
Registration Service TSS
Account Management Service TSS
Record Access Service TSS
Template Service TSS
Document Exchange Service TSS
View Service TSS
Clinical Packaging Specification
CDA Packaging Specification
View Definitions
CDA Imp. Guides
Repository Services TSS (Ltd. Func.)
Record Access Service TSS (Ltd. Func.)
Basic Interface for SEHRs
Key:
Functional Specification
Information Specification

Notes: Document naming has been abbreviated for readability.
Only documents intended for public availability have been shown.
This document map is subject to change to support extension and further functionality as required.

Version 7, 30th November 2011

Figure 1 - Document Map

Acronyms and Terminology

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

1 Introduction

1.1 Context

This document describes the Record Access Service that forms part of the PCEHR Participation and Authorisation Service. Additional services that comprise the Participation and Authorisation Service are specified in separate documents. This document describes the functions available to check if a PCEHR exists, to search for a PCEHR and to gain access to a PCEHR.

The set of interfaces required to support Record Access forms a key part of the PCEHR interface set. However there is a wide range of additional functional areas.

The red highlighted areas in Figure 2 show how this logical service specification fits into the complete set of PCEHR functionality.

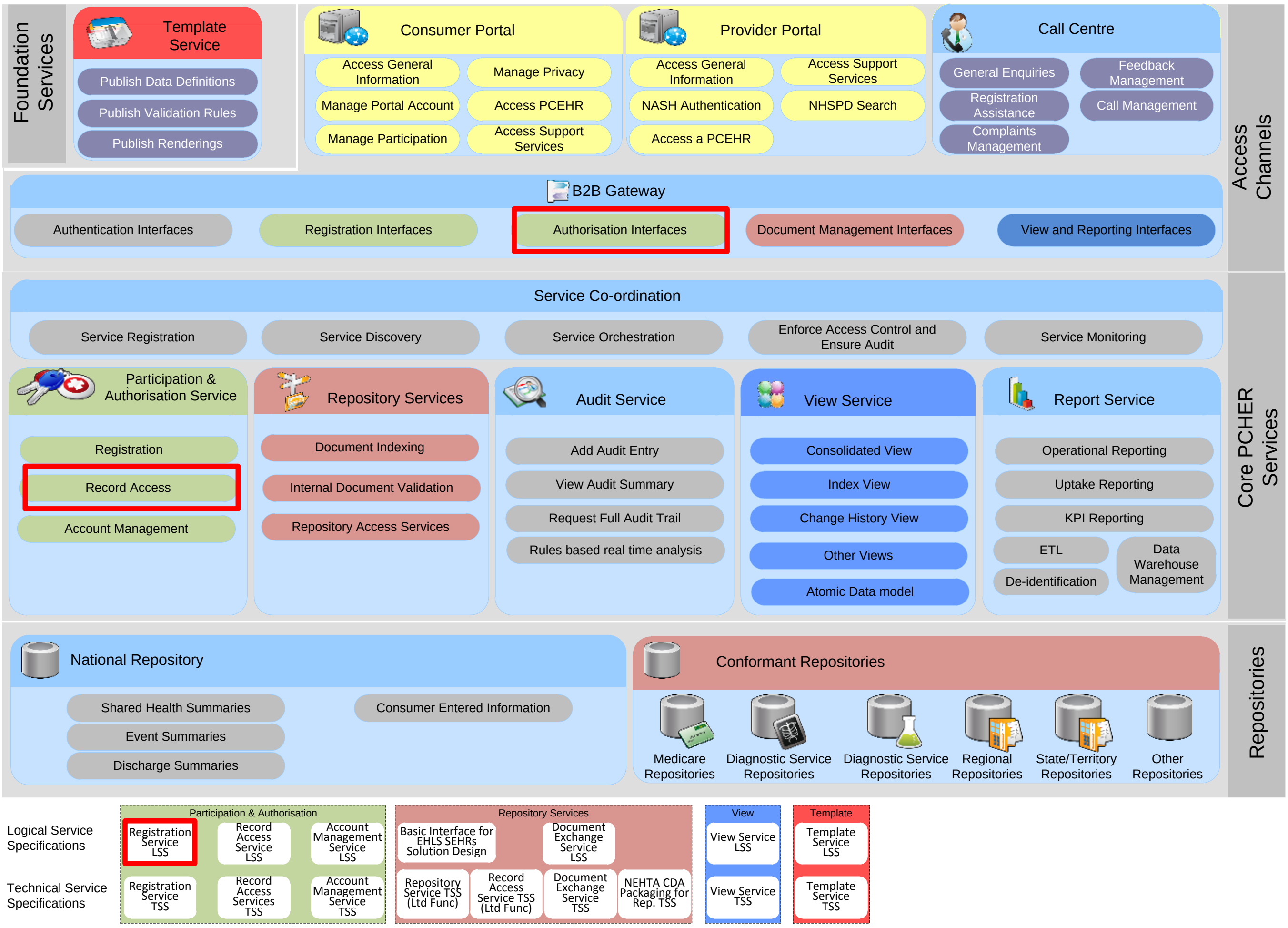


Figure 2 – PCEHR Functions Addressed

As illustrated in Figure 3 below, the Record Access Service is expected to be used by Clinical Information Systems (including Contracted Service Providers) and Conformant Provider Portals. This is further described in later sections of this document.

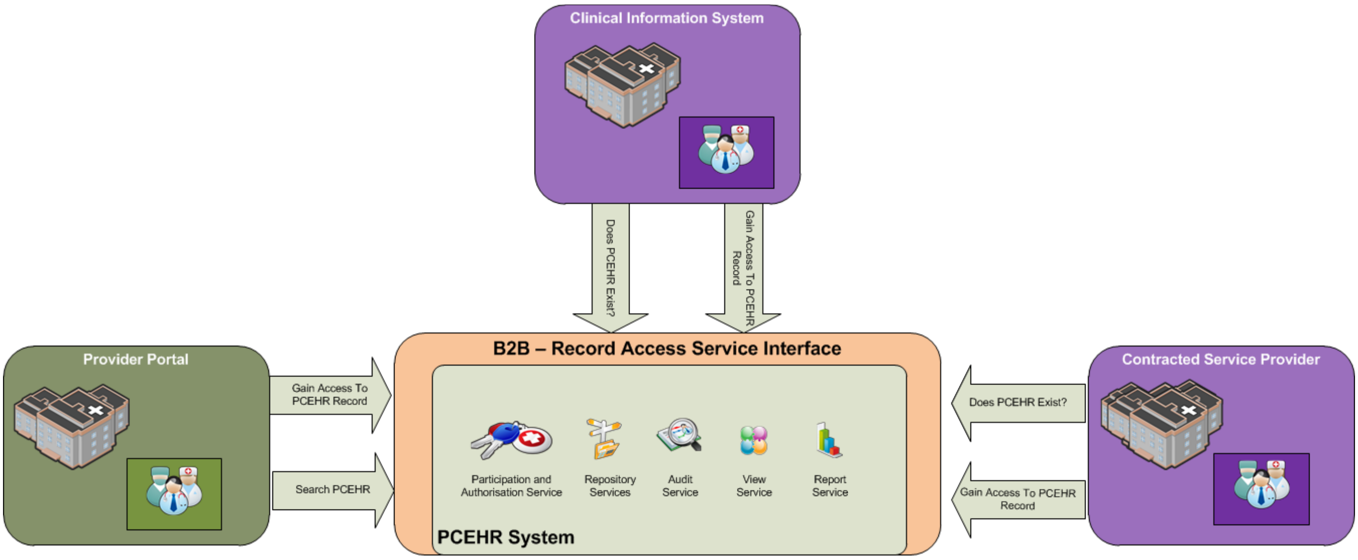

Clinical Information System
Does PCEHR Exist?
Gain Access To PCEHR Record
Provider Portal
Gain Access To PCEHR Record
Search PCEHR
B2B – Record Access Service Interface
Participation and Authorisation Service
Repository Services
Audit Service
View Service
Report Service
PCEHR System
Does PCEHR Exist?
Gain Access To PCEHR Record
Contracted Service Provider

Figure 3 – Record Access Service systems and interactions

1.2 Scope of Document

This document specifies the behaviour that is required of a set of interworking systems. This behaviour is specified in terms of a catalogue of related services that are provided and consumed by those systems. Services are specified in terms of interface contracts.

1.2.1 In Scope

The following items are in scope for this specification:

- A logical platform-agnostic specification for services offered to:
    - check the status of an individual's PCEHR
    - search for an individual's PCEHR
    - enable ongoing authorised access to an individual's PCEHR
- The specification of formal conformance points.

1.2.2 Out of Scope

The following items are explicitly out of scope for this specification:

- The specifications of how to implement the *Record Access Service* on a particular technology platforms (such as via specific types of Web service stacks, messages or electronic documents) – these aspects are addressed in technical service specifications.
- The specification of Conformant Portals or Clinical Information Systems.
- The internal design for national PCEHR components such as the Participation and Authorisation Service.
- Administrative and support related operations which are internal to the PCEHR System.
- Those services covered under other logical service specifications for the PCEHR as per Figure 1 and Figure 2.

1.3 Relationship to eHealth Interoperability Framework

This specification has been produced in accordance with the eHealth Interoperability Framework [EIF], which considers three layers of abstraction and five viewpoints (see summary in Appendix A). The viewpoints relevant to this logical service specification are each covered in a separate section.

1.4 Conformance Points

This specification contains conformance points that identify normative requirements that are to be complied with by systems fulfilling roles identified in this specification.

Conformance points include requirements on a party invoking the service (Service Invoker) and the party providing the service (Service Provider).

Any capability required to meet a conformance point SHALL be considered part of the requirements to be met under this specification.

Conformance points are identified within this document by the means of the following notation:

RCAS-L 0	This is an example only. Conformance points are numbered and prefixed with 'RCAS-L' to indicate that they apply to the Record Access Service logical service specification.

2 Computational Viewpoint

The computational viewpoint is concerned with describing the functional decomposition of the system as computational objects which interact at their interfaces. It includes descriptions of services that objects offer and other objects consume, i.e. service contracts in general terms. These objects describe the key functionality of the system to be built, assuming that necessary infrastructure support and services will be specified in the technical service specification.

This viewpoint is mainly relevant for solution architects and software developers, although a high-level computational description of the interaction between information technology systems and users may also be relevant. This can be a refinement of the interactions defined in the enterprise viewpoint and can involve subject matter experts and business analysts.

This section of the document contains conformance statements that specify the services in terms of the:

- messages exchanged
- processing required of the Service Invoker before invoking a service
- dependency between the response messages generated and the request message and the prior state of the Service Provider
- resulting effect (if any) on the state of the Service Provider
- required processing of response message by the Service Invoker.

2.1 Services Architecture

2.1.1 Overview

This section provides a summary of the system roles and interactions.

Figure 4 illustrates the key system roles and interactions within the scope of the PCEHR Record Access Service.

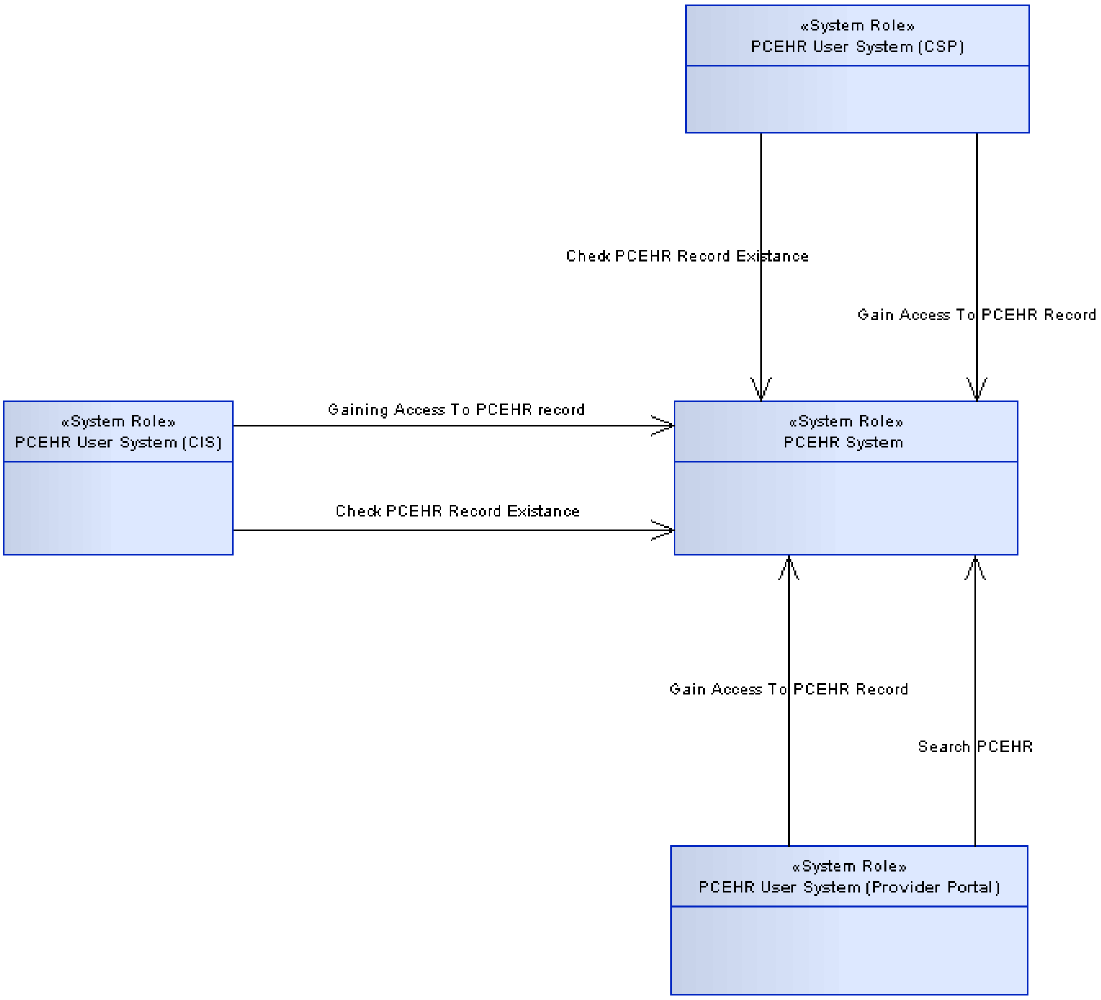

«System Role»
PCEHR User System (CSP)
Check PCEHR Record Existance
Gain Access To PCEHR Record
«System Role»
PCEHR User System (CIS)
Gaining Access To PCEHR record
Check PCEHR Record Existance
«System Role»
PCEHR System
Gain Access To PCEHR Record
Search PCEHR
«System Role»
PCEHR User System (Provider Portal)

Figure 4 - PCEHR Record Access Service Interactions

2.1.2 System Roles

Table 1 provides a summary of the roles in order to give context to the following sections. The full detail of each role is provided in the section shown in the right hand column.

Table 1 PCEHR Record Access Service systems and their community roles

System Role	Description and Rationale	Section
PCEHR System	The *PCEHR System* role is responsible for maintaining the set of documents (and associated metadata) linked to each PCEHR, enforcing access policies and providing interfaces to clinical systems and portals.	2.5
PCEHR User System (CIS)	*PCEHR User System (CIS)* is the client software that is used by healthcare providers to interact with the PCEHR System. It is associated with a Healthcare Organisation.	2.6
PCEHR User System (CSP)	*PCEHR User System (CSP)* is a hosted practice management solution that is used by healthcare providers to interact with the *PCEHR System*. It may be associated with multiple Healthcare Organisations (HPI-Os).	2.7
PCEHR User System (Provider Portal)	*PCEHR User System (Provider Portal*) is a Provider Portal that is used by healthcare providers to interact with the *PCEHR System*. It may be associated with multiple Healthcare Organisations (HPI-Os).	2.8

2.2 Services

Figure 5 illustrates how the interactions between the systems role defined above may be grouped into services. These services provide a logical grouping and are not intended to dictate the physical realisation of the solution

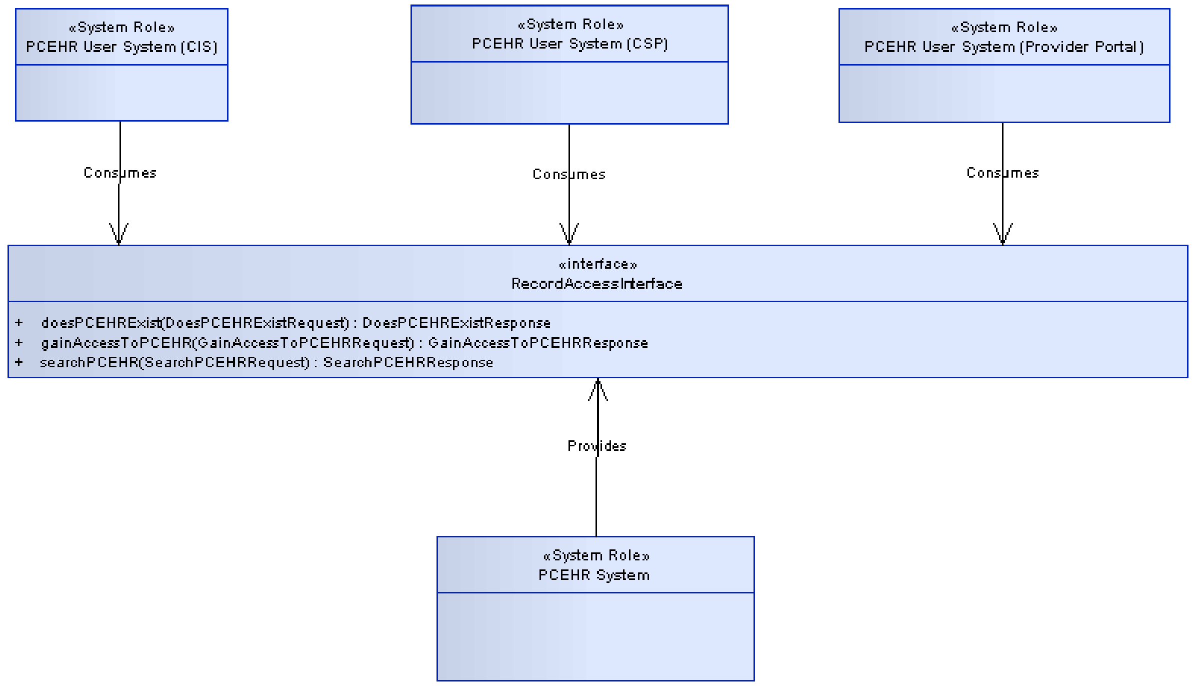

«System Role»
PCEHR User System (CIS)
«System Role»
PCEHR User System (CSP)
«System Role»
PCEHR User System (Provider Portal)
Consumes
Consumes
Consumes
«interface»
RecordAccessInterface
+ doesPCEHRExist(DoesPCEHRExistRequest) : DoesPCEHRExistResponse
+ gainAccessToPCEHR(GainAccessToPCEHRRequest) : GainAccessToPCEHRResponse
+ searchPCEHR(SearchPCEHRRequest) : SearchPCEHRResponse
Provides
«System Role»
PCEHR System

Figure 5 – Interfaces Mapping

2.3 PCEHR Record Access Service Contract

2.3.1 Service Interface - RecordAccessInterface

The RecordAccessInterface encapsulates the set of operations which support the access from the PCEHR system.

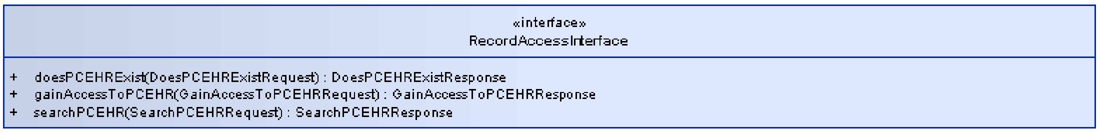

«interface»
RecordAccessInterface
+ doesPCEHRExist(DoesPCEHRExistRequest) : DoesPCEHRExistResponse
+ gainAccessToPCEHR(GainAccessToPCEHRRequest) : GainAccessToPCEHRResponse
+ searchPCEHR(SearchPCEHRRequest) : SearchPCEHRResponse

Figure 6 – RecordAccessInterface

This interface provides the following operations.

Table 2 - Service Interface RecordAccessInterface - Operations

Service Interface - Operations	Mandatory	Comment
doesPCEHRExist	Yes	This function is used to obtain a PCEHR record existence indicator and PCEHR record access preferences.
searchPCEHR	Yes	This function is used to locate a PCEHR.
gainAccessToPCEHR	Yes	This function is used to obtain access to a PCEHR.

The following sub-sections provide operation-specific considerations and conformance points for each of the operations defined in Table 2.

2.3.1.1 Service Operation - doesPCEHRExist

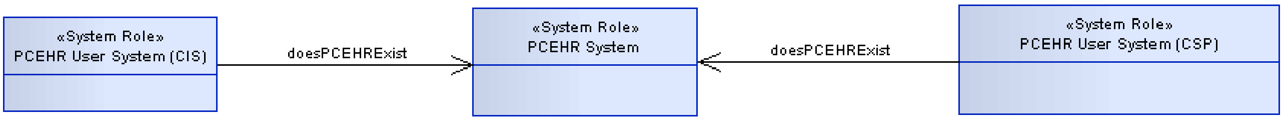


Figure 7 – doesPCEHRExist

Description

This operation provides the ability to check for the presence of an Individual's PCEHR within the *PCEHR System* and to notify the healthcare provider whether an access code is required to gain access to the PCEHR.

This operation will return an indicator which discloses the existence of a PCEHR if the PCEHR record holder chooses to advertise its existence. It provides the following information.

PCEHR Exists

An individual will have the ability to choose to advertise or not advertise the existence of their PCEHR to healthcare providers. When the individual chooses to advertise the existence of their PCEHR, this value will return true.

If the PCEHR does not exist, or if the individual has chosen to not advertise the existence of their PCEHR, it will return false.

Access code required

When PCEHRExists is true, the "*Access code required"* field provides information on how to open the PCEHR (i.e. with an access code, without an access code or access has been granted).

Precondition

Conformance Points

RCAS-L 1	The Service Invoker SHALL pass the Individual Health Identifier (IHI) of the Individual when performing this request.
RCAS-L 2	The Service Invoker SHALL pass the HPI-O of the healthcare organisation when performing this request.
RCAS-L 3	The Service Invoker SHALL pass the User Identifier of the healthcare provider when performing this request.

Post condition

Conformance Points

RCAS-L 4	The Service Provider SHALL return a response indicating that a PCEHR exists when the PCEHR record holder has chosen to disclose its existence.
RCAS-L 5	The Service Provider SHALL return a response indicating that a PCEHR exists when the healthcare provider is currently granted access to PCEHR.
RCAS-L 6	The Service Provider SHALL return a response indicating how to open the PCEHR when PCEHRExists is set is true.
RCAS-L 7	The Service Invoker SHALL be able to access a PCEHR without an access code when the PCEHR exists and an access code is not required.

RCAS-L 8 The Service Invoker SHALL NOT be able to access a PCEHR without an access code and not asserting emergency when the PCEHR exists, when the access code is required and the healthcare provider is not on the provider access list.

Input, Output and Fault

Table 3 – Input, Output and Fault

Operation data fields	Data structures
Input	DoesPCEHRExistRequest
Output	DoesPCEHRExistResponse
Fault	GenericServiceFault

Exception Conditions

Conformance Points

RCAS-L 9 If a technical or functional error occurs while processing the request, the PCEHR System SHALL construct a response message conformant with the generic fault definition in section 3.1.7

2.3.1.2 Service Operation – searchPCEHR

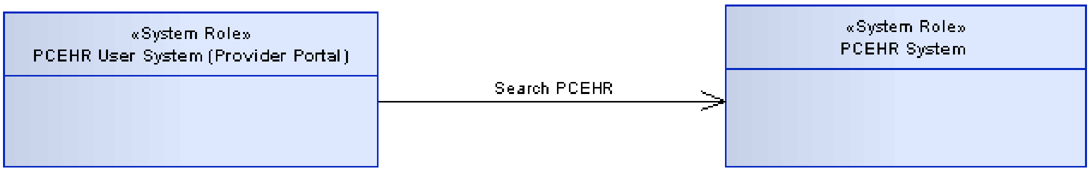


Figure 8 – searchPCEHR

Description

This operation provides the ability for the *PCEHR User System (Provider Portal)* to search for a PCEHR using Individual demographic details. It utilises the Healthcare Identifier (HI) Service searchIHI functionality to search for a PCEHR. The operation allows the Service Invoker to enter the individual demographic detail (please see the Healthcare Identifiers Implementation Guide [HIGUIDE] on the search parameters-set) to locate a PCEHR.

Precondition

Conformance Points

RCAS-L 10 The *PCEHR User System (Provider Portal)* SHALL pass the HPI-O of the healthcare organisation when performing this request.

RCAS-L 11 The Service Invoker SHALL pass the set of demographic parameters specified in section 3.1.3 of the Individual when performing the request.

RCAS-L 12 The *PCEHR User System (Provider Portal)* SHALL provide a healthcare provider individual identifier (HPI-I) when interacting with the *PCEHR System*.

Post condition

Conformance Points

RCAS-L 13 The Service Provider SHALL return a response indicating whether a PCEHR exists.

RCAS-L 14 The Service Provider SHALL return the PCEHR where the PCEHR record holder does not want to advertise its existence.

Input, Output and Fault

Table 4 – Input, Output and Fault

Operation data fields	**Data structures**
Input	SearchPCEHRRequest
Output	SearchPCEHRResponse
Fault	GenericServiceFault

Exception Conditions

Conformance Points

RCAS-L 15 If a technical or functional error occurs while processing the request, the PCEHR System SHALL construct a response message conformant with the generic fault definition contained within section 3.1.7.

2.3.1.3 Service Operation – gainAccessToPCEHR

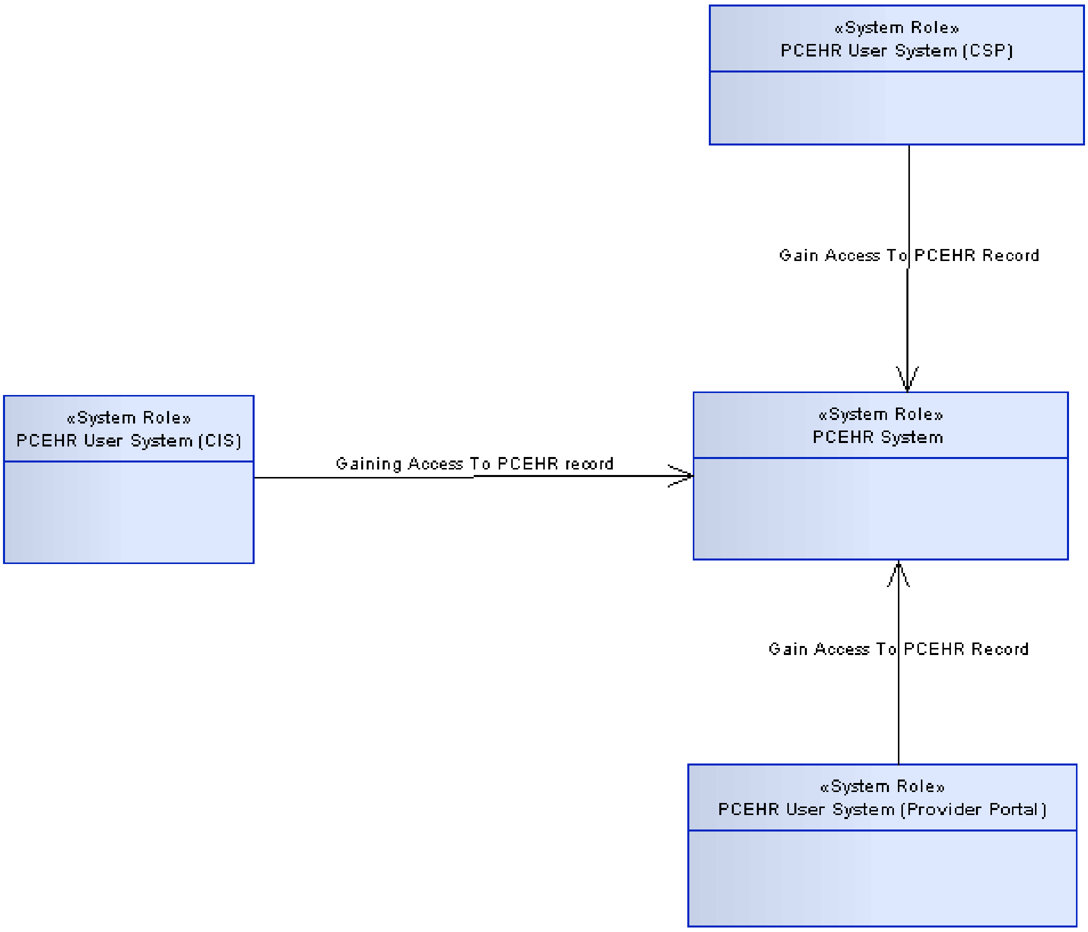

«System Role»
PCEHR User System (CSP)
Gain Access To PCEHR Record
«System Role»
PCEHR User System (CIS)
Gaining Access To PCEHR record
«System Role»
PCEHR System
Gain Access To PCEHR Record
«System Role»
PCEHR User System (Provider Portal)

Figure 9 – gainAccessToPCEHR

Description

This operation provides the ability for *PCEHR User Systems (Provider Portal, CSP and CIS)* to gain access to a PCEHR on behalf of a healthcare organisation using a specific access condition i.e. with Open Access, Access Code or Emergency Assertion.

This operation will request the PCEHR System to add the healthcare organisation to the Provider Access List, based on the specified access condition. Further details can be found in the PCEHR Concept of Operations [PCEHR_CON_OPS].

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

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.

Precondition

Conformance Points

RCAS-L 16 The *PCEHR User System (Provider Portal, CSP or CIS)* SHALL provide the HPI-O of the healthcare organisation when interacting with the PCEHR System.

RCAS-L 17 The *PCEHR User System (Provider Portal, CSP or CIS)* SHALL provide the Individual Health Identifier (IHI) of the Individual when performing this request.

RCAS-L 18 The *PCEHR User System (Provider Portal)* SHALL provide the HPI-I of the healthcare provider when interacting with the PCEHR System.

RCAS-L 19 The *PCEHR User System (Provider Portal, CSP or CIS)* SHALL provide the healthcare provider userid when interacting with the PCEHR System.

Post condition

Conformance Points

RCAS-L 20 The Service Provider SHALL return a response indicating whether the healthcare provider organisation has obtained access.

RCAS-L 21 The Service Invoker SHALL be able to access the PCEHR without an access code when the PCEHR exists and the access code is not required.

RCAS-L 22 Where a PCEHR exists, requires an access code and the healthcare provider is not on the provider access list, the Service Invoker SHALL NOT be able to access the PCEHR without an access code OR without asserting emergency access.

RCAS-L 23 The Service Provider SHALL return the PCEHR where the PCEHR record holder does not want to advertise its existence.

Input, Output and Fault

Table 5 – Input, Output and Fault

Operation data fields	**Data structures**
Input	GainAccessToPCEHRRequest
Output	GainAccessToPCEHRResponse
Fault	GenericServiceFault

Exception Conditions

Conformance Points

RCAS-L 24 If a technical or functional error occurs while processing the request, the PCEHR System SHALL construct a response message conformant with the generic fault definition contained within section 3.1.7.

2.4 Common Specifications

2.4.1 Security

Conformance Points

RCAS-L 25 Service Invoker and Service Provider SHALL establish a secure communication channel when interacting with each other.

2.4.1.2 Data Confidentiality

Conformance Point

RCAS-L 26 Service Invoker and Service Provider System SHALL use Transport Layer Security (TLS) encryption to ensure data confidentiality.

2.4.1.3 Audit

RCAS-L 27	Service Invoker and Service Provider System SHALL comply with audit requirements as per section 5.3 (Data Handling) in the National E-Health Security and Access Framework [NeSAF].

2.4.1.4 PKI

Conformance Points

RCAS-L 28	The Service Invoker SHALL use a gate keeper complaint X.509 certificate when interacting with *PCEHR System*.
RCAS-L 29	PCEHR System SHALL use NASH Public Key Infrastructure to verify validity of the NASH certificate.
RCAS-L 30	PCEHR System SHALL use other gate-keeper complaint Public Key Infrastructure to verify validity of the other gate-keeper complaint certificate.

2.5 System role – PCEHR System

This section ONLY covers the provider of the Record Access Service. Other services provided by the *PCEHR System* are addressed in separate logical service specifications (see Figure 1).

2.5.1 Role Considerations

The National *PCEHR System* is the only provider of the *PCEHR System*.

2.5.2 Identification

PCEHR System Identification is deferred to implementable detail within the Technical Service Specification.

2.5.3 Authentication and Authorisation

Conformance Points

RCAS-L 31	All inter-system communication shall occur over a mutually authenticated secure and encrypted communication channel.

2.5.4 Services Provided

The PCEHR System provides these following logical services.

Conformance Points

RCAS-L 32	The *PCEHR System* SHALL provide doesPCEHRExist operation.
RCAS-L 33	The *PCEHR System* SHALL provide searchPCEHR operation.
RCAS-L 34	The *PCEHR System* SHALL provide gainAccessToPCEHR operation.

2.5.5 Services Consumed

The *PCEHR System* does not consume other services in the context of the Record Access Service.

2.6 System role – PCEHR User System (CIS)

2.6.1 Role Considerations

PCEHR User System (CIS) may be fulfilled by a number of systems, including GP desktop Practice Management System, Public/Private Acute Care Patient Administration System, Emergency Department System and Community Care System.

2.6.1.1 Identification

The system role identification is derived from the information below.

Conformance Point

RCAS-L 35 *PCEHR User System (CIS)* Vendor, Product Name, Version Number and Platform SHALL be used when interacting with the *PCEHR System* for system identification.

2.6.1.2 Authentication and Authorisation

Conformance Point

RCAS-L 36 The *PCEHR User System (CIS)* SHALL use a NASH healthcare provider organisation (HPI-O) certificate for Transport Layer Security (TLS) when interacting with the *PCEHR System* for authentication.

RCAS-L 37 The *PCEHR System* SHALL use the HPI-O number from the NASH healthcare provider organisation (HPI-O) certificate for the *PCEHR User System (CIS)* authorisation.

2.6.1.3 PKI

Conformance Point

RCAS-L 38 The Service Invoker SHALL use a NASH healthcare provider organisation (HPI-O) certificate when interacting with the *PCEHR System*.

2.6.2 Services Provided

The *PCEHR User System (CIS)* does not provide any services.

2.6.3 Services Consumed

Conformance Points

RCAS-L 39 The *PCEHR User System (CIS)* SHALL consume Record Access Service.

RCAS-L 40 The *PCEHR User System (CIS)* SHALL use doesPCEHRExist operation to get the PCEHR record existence indicator.

RCAS-L 41 The *PCEHR User System (CIS)* SHALL use gainAccessToPCEHR operation to obtain access to the PCEHR.

2.7 System role – PCEHR User System (CSP)

2.7.1 Role Considerations

The *PCEHR User System (CSP)* may be fulfilled by a hosted practice management system.

2.7.1.1 Identification

The system role identification is derived from the following information.

Conformance Point

RCAS-L 42	The *PCEHR User System (CSP)* Vendor, Product Name, Version Number and Platform SHALL be used when interacting with the PCEHR System for system identification.
RCAS-L 43	The *PCEHR system* SHALL retrieve the *PCEHR User System (CSP)* identifier from the certificate used on the Transport Layer Security (TLS) by the *PCEHR User System (CSP)*.

2.7.1.2 Authentication and Authorisation

Conformance Point

RCAS-L 44	The *PCEHR User System (CSP)* SHALL use gate keeper complaint certificate for Transport Layer Security (TLS) when interacting with *PCEHR System* for authentication.
RCAS-L 45	The *PCEHR User System (CSP)* SHALL provide a HPI-O number that the user is currently represented for *PCEHR User System (CSP)* authorisation.
RCAS-L 46	The *PCEHR system* SHALL use a HPI-O number provided by the *PCEHR User System (CSP)* authorisation.
RCAS-L 47	The *PCEHR system* SHALL validate the relationship between the Healthcare Organisation (HPI-O) with the Contracted Service Provider (CSP).

2.7.2 Services Provided

The *PCEHR User System (CSP)* does not provide any services.

2.7.3 Services Consumed

Conformance Points

RCAS-L 48	*The PCEHR User System (CSP)* SHALL consume Record Access Service.
RCAS-L 49	*The PCEHR User System (CSP)* SHALL use doesPCEHRExist operation to get the PCEHR record existence indicator.
RCAS-L 50	*The PCEHR User System (CSP)* SHALL use gainAccessToPCEHR operation to obtain access to the PCEHR Record.

2.8 System role – PCEHR User System (Provider Portal)

2.8.1 Role Considerations

The *PCEHR User System (Provider Portal)* may be fulfilled by the National Provider Portal or Conformant Provider Portals.

2.8.1.1 Identification

System role identification is derived from the following information.

Conformance Point

RCAS-L 51	*The PCEHR User System (Provider Portal)* Vendor, Product Name, Version Number and Platform SHALL be used when interacting with the *PCEHR System* for system identification.

2.8.1.2 Authentication and Authorisation

Conformance Points

RCAS-L 52	The *PCEHR User System (Provider Portal)* SHALL use gate keeper complaint certificate for Transport Layer Security (TLS) if the PCEHR User System (Provider Portal) is a conformant Provider Portal when interacting with the *PCEHR System* for authentication.
RCAS-L 53	The *PCEHR system* SHALL use HPI-O number provider by the *PCEHR User System (Provider Portal)* for authorisation.
RCAS-L 54	The *PCEHR User System (Provider Portal)* SHALL authenticate Healthcare provider individual using the NASH Healthcare Provider Individual credential.

2.8.2 Services Provided

The *PCEHR User System (Provider Portal)* does not provide any services.

2.8.3 Services Consumed

Conformance Points

RCAS-L 55	The *PCEHR User System (Provider Portal)* SHALL consume Record Access Service.
RCAS-L 56	The *PCEHR User System (Provider Portal)* SHALL use searchPCEHR operation to locate a PCEHR.
RCAS-L 57	The *PCEHR User System (Provider Portal)* SHALL use gainAccessToPCEHR operation to obtain access to a PCEHR.

3 Information Viewpoint

The information viewpoint is concerned with the representation of information in the system. It is relevant for business (i.e. clinical and administrative) stakeholders and information modellers. The major contributions here is expected from subject matter experts (i.e. clinicians), health informatics experts, (i.e. clinical terminologists and informaticians) and information architects who document information components and the appropriate clinical terminology concepts according to their preferred style of expression.

3.1 Service Operation Data Types

3.1.1 DoesPCEHRExistRequest

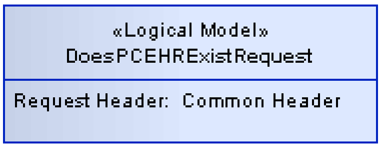


Figure 10 – DoesPCEHRExistRequest

Table 6 - DoesPCEHRExistRequest

DoesPCEHRExistRequest			
Field	**Data Type**	**Description**	**Cardinality**
Request Header	Common Header	Common request header	1

3.1.2 DoesPCEHRExistResponse

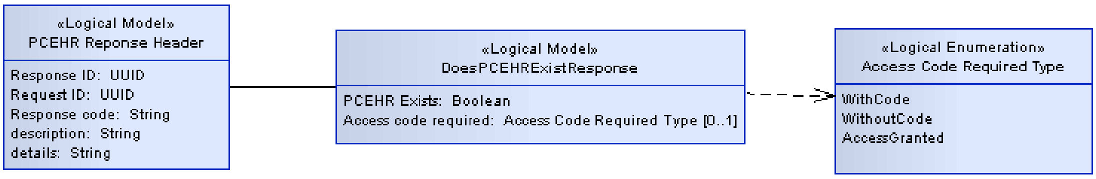


Figure 11 – DoesPCEHRExistResponse

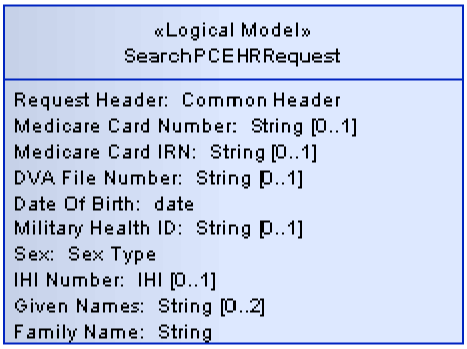
Table 7 - DoesPCEHRExistResponse

DoesPCEHRExistResponse			
Field	**Data Type**	**Description**	**Cardinality**
PCEHR Exists	Boolean	A flag indicating whether the PCEHR exists	1
Access code required	Access Code Required Type	An enumeration indicating whether the provider organisation must supply a code to access the PCEHR. When PCEHR Exists is False, this value must be set to NULL	0..1

Table 8 – Access Code Required Type

Field	Description
WithCode	Access can be obtained by invoking gainAccessToPCEHR with an Access Code.
WithoutCode	Access can be obtained by invoking gainAccessToPCEHR without an Access Code
AccessGranted	Access is already granted and can be obtained without invoking gainAccessToPCEHR

3.1.3 SearchPCEHRRequest



«Logical Model»
SearchPCEHRRequest

Request Header: Common Header
Medicare Card Number: String [0..1]
Medicare Card IRN: String [0..1]
DVA File Number: String [0..1]
Date Of Birth: date
Military Health ID: String [0..1]
Sex: Sex Type
IHI Number: IHI [0..1]
Given Names: String [0..2]
Family Name: String

Figure 12 – SearchPCEHRRequest

Table 9 - SearchPCEHRRequest

SearchPCEHRRequest			
Field	**Data Type**	**Description**	**Cardinality**
Request Header	Common Header	Common request header	1
Medicare Card Number	String	Medicare Card Number	0..1
Medicare Card IRN	String	Medicare Card IRN	0..1
DVA File Number	String	PCEHR Individual DVA File number	0..1
Military Health Identifier	String	Individual Military Health Identifier	0..1
Date Of Birth	Date	PCEHR Individual date of birth	1
Sex	Enumeration	Sex enumeration (i.e. Male, Female, etc.)	1
IHI Number	IHI	PCEHR Individual IHI number	0…1
Given Names	String	PCEHR individual first name and middle name	0..2
Family Name	String	PCEHR individual family name	1

3.1.4 SearchPCEHRResponse

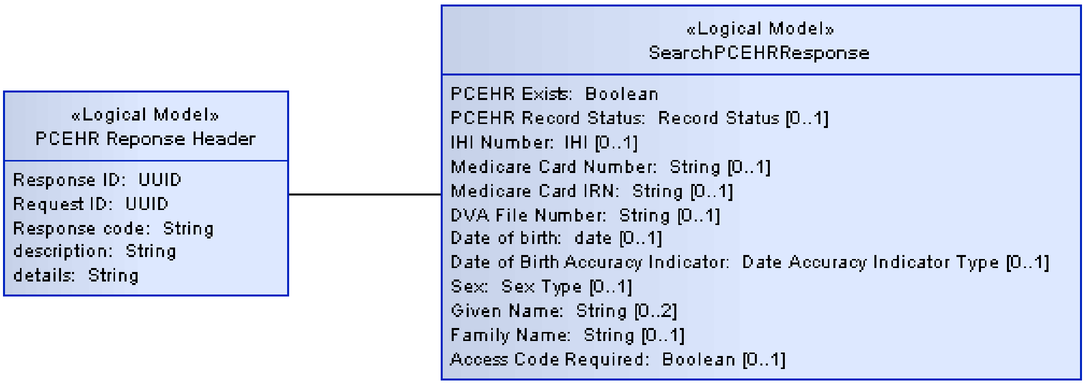

«Logical Model»
PCEHR Reponse Header
Response ID: UUID
Request ID: UUID
Response code: String
description: String
details: String
«Logical Model»
SearchPCEHRResponse
PCEHR Exists: Boolean
PCEHR Record Status: Record Status [0..1]
IHI Number: IHI [0..1]
Medicare Card Number: String [0..1]
Medicare Card IRN: String [0..1]
DVA File Number: String [0..1]
Date of birth: date [0..1]
Date of Birth Accuracy Indicator: Date Accuracy Indicator Type [0..1]
Sex: Sex Type [0..1]
Given Name: String [0..2]
Family Name: String [0..1]
Access Code Required: Boolean [0..1]

Figure 13 – SearchPCEHRResponse

Table 10 - SearchPCEHRResponse

SearchPCEHRResponse			
Field	**Data Type**	**Description**	**Cardinality**
PCEHR Exists	Boolean	A flag to indicate whether the PCEHR exists	1
PCEHR Record Status	Record Status Type	Indicates the status of the PCEHR: • Active • Inactive	0..1
IHI Number	IHI	PCEHR Individual Identifier (IHI)	0..1
Medicare Card Number	String	PCEHR Individual Medicare Card Number	0..1
Medicare Card IRN	String	PCEHR Individual Medicare Card IRN	0..1
DVA File Number	String	PCEHR Individual DVA File Number	0..1
Date Of Birth	Date	PCEHR Individual date of birth	0..1
Date Of Birth Accuracy Indicator	Date Accuracy Indicator Type	Date Accuracy Indicator (i.e. UEA,UUE,etc)	0..1
Sex	Enumeration	Sex enumeration (i.e. Male, Female, etc.	0..1
Given Names	String	PCEHR individual first name and middle name	0..2
Family Name	String	PCEHR individual family name	0..1
Access code required	Boolean flag	A flag indicating whether the Provider organisation must supply a code to access the PCEHR.	0..1

3.1.5 GainAccessToPCEHRRequest

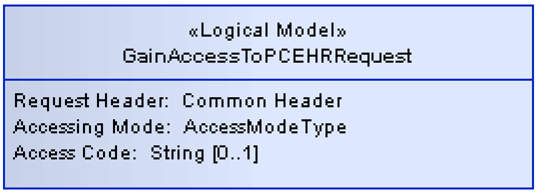

«Logical Model»
GainAccessToPCEHRRequest
Request Header: Common Header
Accessing Mode: AccessModeType
Access Code: String [0..1]

Figure 14 – GainAccessToPCEHRRequest

Table 11 - GainAccessToPCEHRRequest

GainAccessToPCEHRRequest			
Field	**Data Type**	**Description**	**Cardinality**
Request Header	Common Header	Common request header	1
Accessing Mode	Enumeration	The accessing mode such as Emergency, Access Code or Without Code.	1
Access Code	String	Access code that is given by the PCEHR record holder to the healthcare provider at the point of care.	0..1

3.1.6 GainAccessToPCEHRResponse

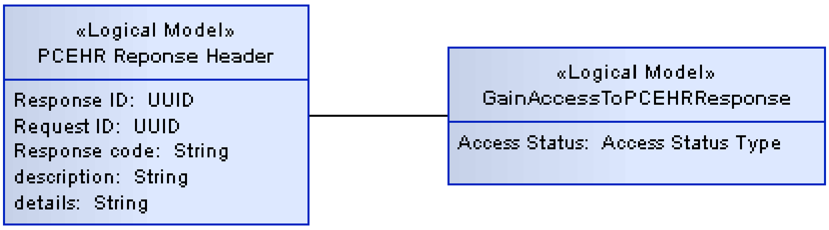


Figure 15 – GainAccessToPCEHRResponse

Table 12 - GainAccessToPCEHRResponse

GainAccessToPCEHRRequest			
Field	**Data Type**	**Description**	**Cardinality**
Access Status	Access Status Type	Access Status information i.e. granted or revoked	0..1

3.1.7 GenericServiceResponse

The GenericServiceResponse is the default response returned by most operations.

Table 13 - GenericServiceResponse

GenericServiceResponse			
Field	**Data Type**	**Description**	**Cardinality**
Common Response Header	CommonServiceResponseHeader	An instance of the PCEHR common service header.	1

3.1.8 GenericServiceFault

Table 14 - GenericServiceFault

GenericServiceFault			
Field	Data Type	Description	Cardinality
Common Response Header	CommonServiceResponseHeader	An instance of the PCEHR Common Service Header.	1

3.1.9 PCEHR Response Header

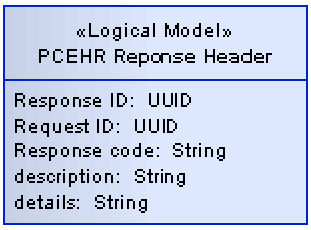


Figure 16 – PCEHR Response Header

Table 15 – PCEHR Response Header

PCEHR Response Header			
Field	**Data Type**	**Description**	**Cardinality**
Response ID	Identifier	A unique identifier for this response.	1
Request ID	Identifier	The identifier of the original request.	1
Response code	String	A code indicating the processing status of the request.	1
Description	String	String describing the processing status of the request.	0..1
Details	Strings	A string providing extended details of the response.	0..1

3.2 Common Header

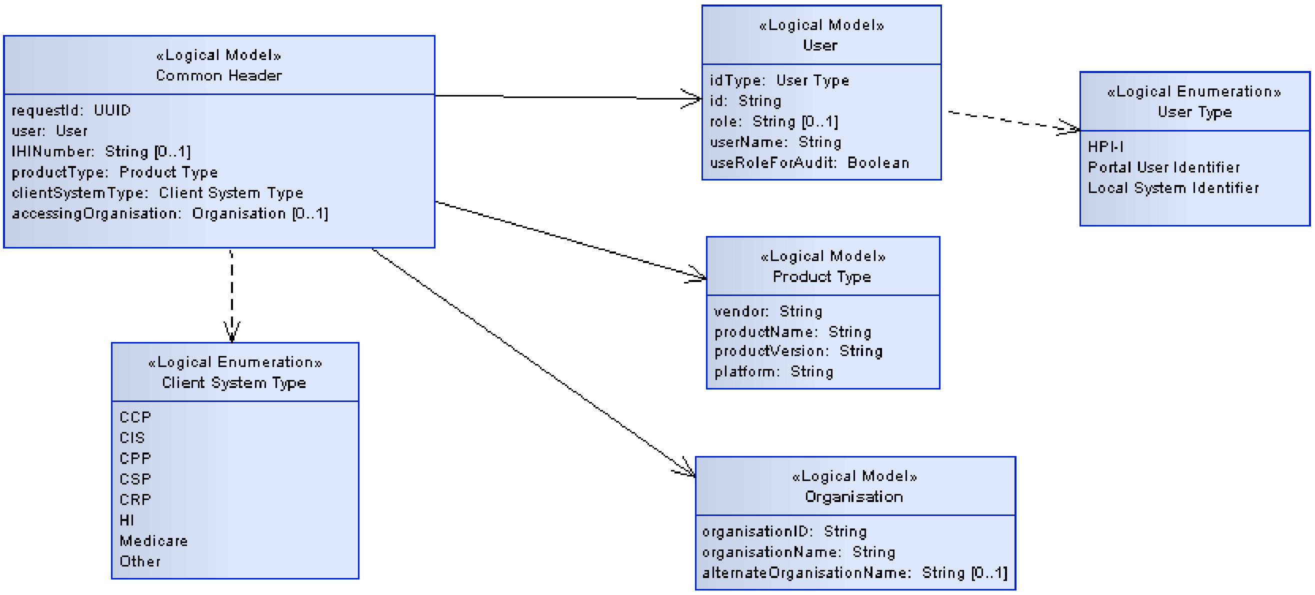


Figure 17 – Common Header

Table 16 – Common Header

Common Header			
Field	**Data Type**	**Description**	**Cardinality**
Request Id	UUID	Unique identification of the request	1
User	User	Identification details of the user originating the request	1
IHI Number	String	Individual IHI number	0..1
Product Type	Product Type	Identification of the system originating the request	1
Client System Type	Enumeration	The type of client system. • Conformant Consumer Portal (CCP) • Clinical Information System (CIS) • Conformant Provider Portal (CPP) • Contracted Service Provider System (CSP) • Conformant Repository Provider System (CRP) • HI Service (HI) • Medicare • Other	1
Accessing Organisation	Organisation	The healthcare organisation on behalf of which the request is being made	0..1

Conformance Points

RCAS-L 58 The `Request Id` SHALL be a different value for every request made. It SHALL be created in a way which ensures that the value is unique across all service requests from any system.

RCAS-L 59 The `IHI Number` SHALL be supplied for doesPCEHRExist and gainAccessToPCEHR requests.

RCAS-L 60 If the `IHI Number` is supplied it SHALL contain a string representation using only numeric digits of a valid Individual Healthcare Identifier issued by the HI Service.

3.2.1 User

The User entity encompasses the identity information relating to the end user of the system originating a request.

Table 17 - User

User			
Field	**Data Type**	**Description**	**Cardinality**
Id Type	Enumeration	The type of user ID supplied: • HPI-I • Portal User Identifier • Local System Identifier	1
Id	String	User identifier	1
Role	String	Optional field for to enter the role of the user for use in audit logging if User Name is not appropriate	0..1
User Name	String	The name of the user	1
Use role for audit	Boolean	If true indicates that the role is to be used for audit display purposes rather than the User name	1

Conformance Points

RCAS-L 61 The `Id` SHALL NOT contain leading or trailing spaces. It SHALL NOT be a null or zero length string.

RCAS-L 62 If the `Id Type` value of `HPI-I` is supplied, the `Id` SHALL contain a string representation using only numeric digits of a valid Healthcare Provider Identifier - Individual issued by the HI Service.

RCAS-L 63 If the `Id Type` value of `Portal User Identifier` is supplied, the `Id` SHALL contain a value issued by a trusted identity provider which relates a conformant portal user to a PCEHR identity.

RCAS-L 64 If the `Id Type` value of `Local System Identifier` is supplied, the `Id` SHALL contain a representation of the access credential utilised to access the system originating the request.

RCAS-L 65 If the `Id Type` value of `Local System Identifier` is supplied, the `Id` SHALL NOT contain leading or trailing spaces. It SHALL NOT be a null or zero length string.

RCAS-L 66 If the `Use role for audit` flag is set to True, the `Role` SHALL be supplied.

RCAS-L 67 If the `Role` is supplied it SHALL NOT contain leading or trailing spaces. It SHALL NOT be a null or zero length string.

RCAS-L 68 The `User Name` SHALL NOT contain leading or trailing spaces. It SHALL NOT be a null or zero length string.

3.2.2 Product Type

The Product type entity encompasses the information identifying the system originating the request.

Table 18 – Product Type

Product Type			
Field	**Data Type**	**Description**	**Cardinality**
Vendor	String	The name of the vendor that produced the system	1
Product Name	String	A name used to identify the system	1
Product Version	String	System version number	1
Platform	String	The system platform being used	1

Conformance Points

RCAS-L 69 The `Vendor` SHALL NOT contain leading or trailing spaces. It SHALL NOT be a null or zero length string.

RCAS-L 70 The `Product Name` SHALL NOT contain leading or trailing spaces. It SHALL NOT be a null or zero length string.

RCAS-L 71 The `Product Version` SHALL NOT contain leading or trailing spaces. It SHALL NOT be a null or zero length string.

RCAS-L 72 The `Platform` SHALL NOT contain leading or trailing spaces. It SHALL NOT be a null or zero length string.

3.2.3 Organisation

The Organisation entity encompasses the organisation identity information.

Table 19 - Organisation

Organisation			
Field	**Data Type**	**Description**	**Cardinality**
Organisation ID	String	An HPI-O identifier for the healthcare organisation	1
Organisation Name	String	The name of the Healthcare organisation	1
Alternate Organisation Name	String	An alternative display name for the healthcare organisation	0..1

RCAS-L 73 The `Organisation ID` SHALL contain a string representation using only numeric digits of a valid Healthcare Provider Identifier - Organisation issued by the HI Service.

RCAS-L 74 The `Organisation Name` SHALL NOT contain leading or trailing spaces. It SHALL NOT be a null or zero length string.

RCAS-L 75 The `Organisation Name` SHALL correspond to the name of the organisation asserted by the Healthcare Provider Identifier – Organisation contained in the `Organisation ID` field.

RCAS-L 76 If the `Alternate Organisation Name` is supplied, it SHALL NOT contain leading or trailing spaces. It SHALL NOT be a null or zero length string.

3.2.4 Client System Type

An enumeration of Client System Types which are supported by the PCEHR System, and as such, are allowable values for the common header when interacting with the PCEHR.

Table 20 – Client System Type

Field	Description
Conformant Consumer Portal	Conformant Consumer Portal
Clinical Information System	A Clinical Information System such as a PAS, RIS, PMS, ED System, etc.
Conformant Provider Portal	Conformant Provider Portal
Contracted Service Provider	Contracted Service Provider
Conformant Repository	A Conformant Repository
HI Service	The national Health Care Identifier Service
Medicare	DHS Medicare systems
Other	Any other system type

3.2.5 User Type

An enumeration of Source system user identifiers which are supported by the PCEHR System, and as such, are allowable values for the common header when interacting with the PCEHR System.

Table 21 – User Type

Field	Description
HPI-I	A Health Care Provider Individual identifier issued by the HI Service
Portal User Identifier	An identity which is managed and verified by the PCEHR system and identifies a user of a conformant portal
Local System Identifier	A local user id not managed by the PCEHR system

3.3 Other Data Types

3.3.1 Access Status Type

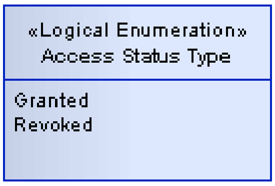


Figure 18 – Record Status Type

Table 22 – Access Status Type

Field	Description
Granted	Access Granted
Revoked	Access Revoked

3.3.2 Record Status Type

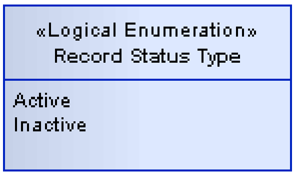


Figure 19 – Record Status Type

Table 23 – Record Status Type

Field	Description
Active	PCEHR Record Status is active
Inactive	PCEHR Record Status is inactive

3.3.3 Date Accuracy Indicator Type

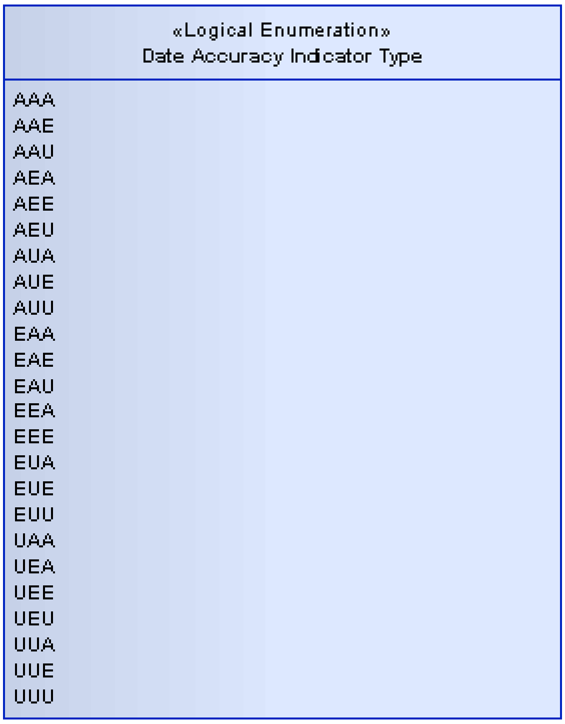


Figure 20 – Date Accuracy Indicator Type

Table 24 – Date Accuracy Indicator Type

Field	Description
AAA	Accurate day, accurate month, accurate year
AAE	Accurate day, accurate month, estimated year
AAU	Accurate day, accurate month, unknown year
AEA	Accurate day, estimated month, accurate year
AEE	Accurate day, estimated month, estimated year
AEU	Accurate day, estimated month, unknown year
AUA	Accurate day, unknown month, accurate year
AUE	Accurate day, unknown month, estimated year
AUU	Accurate day, unknown month, unknown year
EAA	Estimated day, accurate month, accurate year
EAE	Estimated day, accurate month, estimated year
EAU	Estimated day, accurate month, unknown year
EEA	Estimated day, estimated month, accurate year
EEE	Estimated day, estimated month, estimated year
EEU	Estimated day, estimated month, unknown year
EUA	Estimated day, unknown month, accurate year
EUE	Estimated day, unknown month, estimated year
EUU	Estimated day, unknown month, unknown year
UAA	Unknown day, accurate month, accurate year
UAE	Unknown day, accurate month, estimated year
UAU	Unknown day, accurate month, unknown year
UEA	Unknown day, estimated month, accurate year
UEE	Unknown day, estimated month, estimated year
UEU	Unknown day, estimated month, unknown year
UUA	Unknown day, unknown month, accurate year
UUE	Unknown day, unknown month, estimated year
UUU	Unknown day, unknown month, unknown year

3.3.4 Sex Type

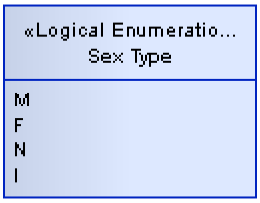


Figure 21 – Sex Type

Table 25 – Sex Type

Field	Description
M	Male
F	Female
N	Not Known
I	Intersex or indeterminate

3.3.5 Access Mode Type

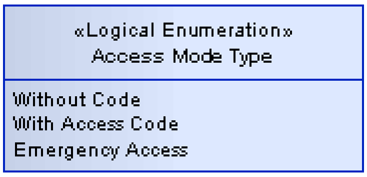


Figure 22 – Access Mode Type

Table 26 – Access Mode Type

Field	Description
Without Code	Access without an access code
With Access Code	Access with an access code
Emergency Access	Access with emergency mode

Appendix A eHealth Interoperability Framework

This document has been produced in accordance with the eHealth Interoperability Framework [EIF]. The eHealth Interoperability Framework is based on a combination of the Australian Government Architecture (AGA)[1], RM-ODP and HL7's Service Aware Interoperability Framework (SAIF)[2,3].

The eHealth Interoperability Framework is used across NEHTA products to help deliver consistent and cohesive eHealth specifications. It provides a common specification language for teams involved in working in eHealth, supports the identification of secure and interoperable services and assists in analysing eHealth solutions to ensure that they will deliver the intended outcome.

A.1 Three Layers of Abstraction

The framework has three layers of abstraction. The top layer focuses on defining the system in a stakeholder centric fashion at the conceptual level. The detail and refinement of the system definition is covered at the logical level and the implementable level maps the logical specification onto a number of technology-specific implementable specifications.

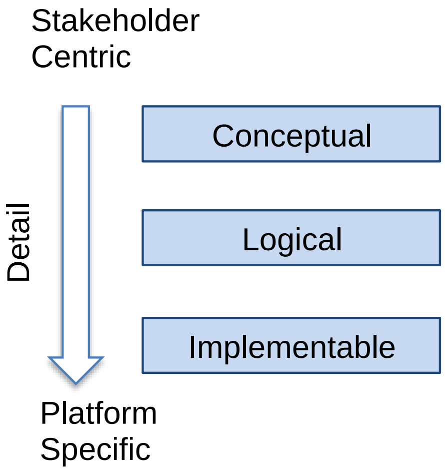


Figure 23 - Layers of abstraction

Separating the conceptual from the logical and the logical from the implementable allows service or other system components to be defined independently of technology choices. It also ensures that different stakeholder groups can play to their strengths at the different layers of abstraction.

In particular, the conceptual level is aimed at consumers, healthcare providers and government stakeholders. The logical level is aimed at more technical stakeholders, including health informaticians, implementers and the ICT industry. The implementable level is aimed at developers and testers.

[1] http://www.finance.gov.au/e-government/strategy-and-governance/aga-rm/AGA-RM.html

[2] http://gforge.hl7.org/gf/project/saeaf/docman/?subdir=320

[3] The EIF differs from other popular frameworks such as TOGAF. TOGAF is a process-oriented framework for creating and managing architectural artefacts. EIF is a specification framework used to describe system architectures. EIF, and the SAIF framework it is based on, are strongly influenced by ISO 10746, which is an international standard reference model for open distributed processing (RM ODP). The viewpoints and levels of abstraction in the EIF are more similar to the categories that underpin the Zachman framework. However, RM-ODP also provides a specification language that is compatible with UML.

A.2 Five Viewpoints

The framework has five "viewpoints":

- The *enterprise viewpoint*, which focuses on the purpose, scope, policies and business requirements for the system.
- The *information viewpoint*, which focuses on the semantics of the information and the information processing performed. It describes the information managed by the system and the structure and content type of the supporting data.
- The *computational viewpoint*, which describes the functionality provided by the system and its functional decomposition into objects and interfaces.
- The *engineering viewpoint*, which focuses on describing how the different elements described in the information and computational viewpoints will be deployed or distributed and how the system will meet the operational requirements.
- The *technology viewpoint*, which focuses on the choice of technology of the system and includes both the software and hardware platforms.

This document focuses on the information and computational viewpoints and each viewpoint is covered in a separate section.

In addition to the viewpoints, the framework also prescribes three abstraction layers, namely the Conceptual Layer, the Logical Layer and the Implementable Layer.

The interaction between the viewpoints and the layers of abstraction can be represented as a matrix of views, as shown below. This document covers the cells shown.

Table 27 –Matrix of views

	Enterprise	**Information**	**Computational**	**Engineering**	**Technology**
Conceptual					
Logical		**This Document**	**This Document**		
Implementable					

Appendix B Acronyms and Terminology

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

B.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

B.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 C References

Tag	Name	Version Release Date
[EIF]	eHealth Interoperability Framework Nehta managed publication http://www.nehta.gov.au/connecting-australia/ehealth-architecture	V1.0 02/12/2011
[HIGUIDE]	Healthcare Identifiers Implementation Guide	V1.1 6 June 2011
[NeSAF]	National E-Health Security and Access Framework	1.1 28/04/2011
[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	1.0 6/05/2011
[RM-ODP]	Reference Model of Open Distributed Processing ISO/IEC 10746-3:2009	2009
[UML2010]	UML Version 2.3 http://www.omg.org/spec/UML/2.3/	Version 2.3 May 2010