nehta

High-Level System Architecture

PCEHR System

Version 1.35 — 11 November 2011

Final

This document is based on the
April 2011 release of the PCEHR System Concept of Operations (ConOps).

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 Amendments

This document was written to provide input to the National Infrastructure Partner tender. An update of the document, reflecting detailed design decisions by the National Infrastructure Partner, will be made available in future.

Document Control

The current electronic revision of this document is held and controlled by NEHTA. The printed form of the document is considered uncontrolled. It is the responsibility of the user to verify that this copy is latest revision of the document.

Document information

Purpose

This document provides a high-level description of the architecture of the PCEHR System. It is based on the April 2011 PCEHR System Concept of Operations and was written to provide input to the National Infrastructure Partner tender. It will be updated to reflect the PCEHR design developed by the National Infrastructure Partner.

The document provides the next level of detail below the PCEHR System Concept of Operations [PCEHR_CON_OPS], and includes a description of the solution, with a focus on key concepts, system functionality, dependencies and interfaces. This design provides conceptual and logical views of the system and it is expected that significant further implementation specific elaboration will be required.

As different components of the PCEHR System may be designed and implemented by different parties, the high level PCEHR System architecture is intended to provide the high level definitions required to ensure consistency between each of the sub-component specifications and implementations.

Note that this draft high-level system architecture portrays a possible design. Alternative designs are possible where they deliver the same key concepts, system functionality, dependencies and interfaces.

The high level design outlined in the PCEHR System architecture covers:

- PCEHR System channels, currently limited to the consumer portal, provider portal, B2B gateway and report portal
- PCEHR core services, including: Participation and Authorisation Service, Index Service, View Service, Audit Service, Report Service
- National Repositories Service and interfaces to Conformant Repositories.

The coverage of high level design for each of these elements will vary in level of detail based on their progress within the design program and the priority of components.

The design must support a range of information types including clinical documents (such as Shared Health Summaries), data sourced from Medicare Australia, and consumer-entered information.

This document is aligned with the NEHTA eHealth Framework (NEHF) implemented by NEHTA. The NEHF is itself closely aligned with HL7 SAIF and the Australian Government Architecture Reference Model. In line with the NEHF, this document provides a conceptual and logical view of the PCEHR System architecture from an enterprise, computational and informational viewpoint.

This document will be periodically updated as the PCEHR Program progresses. An update of the document will be made available in future to reflect detailed design decisions by the National Infrastructure Partner, updates as a result of the public consultation process around the Draft PCEHR System Concept of Operations, and the lessons learned from lead implementations.

Intended Audience

This document is primarily aimed at a technical audience, including:

- Enterprise and solution architects
- Business analysts and business architects
- Health informaticians
- National Infrastructure Partner technical staff
- Technical staff working for vendors and implementers
- System implementers seeking to integrate with the PCEHR System.

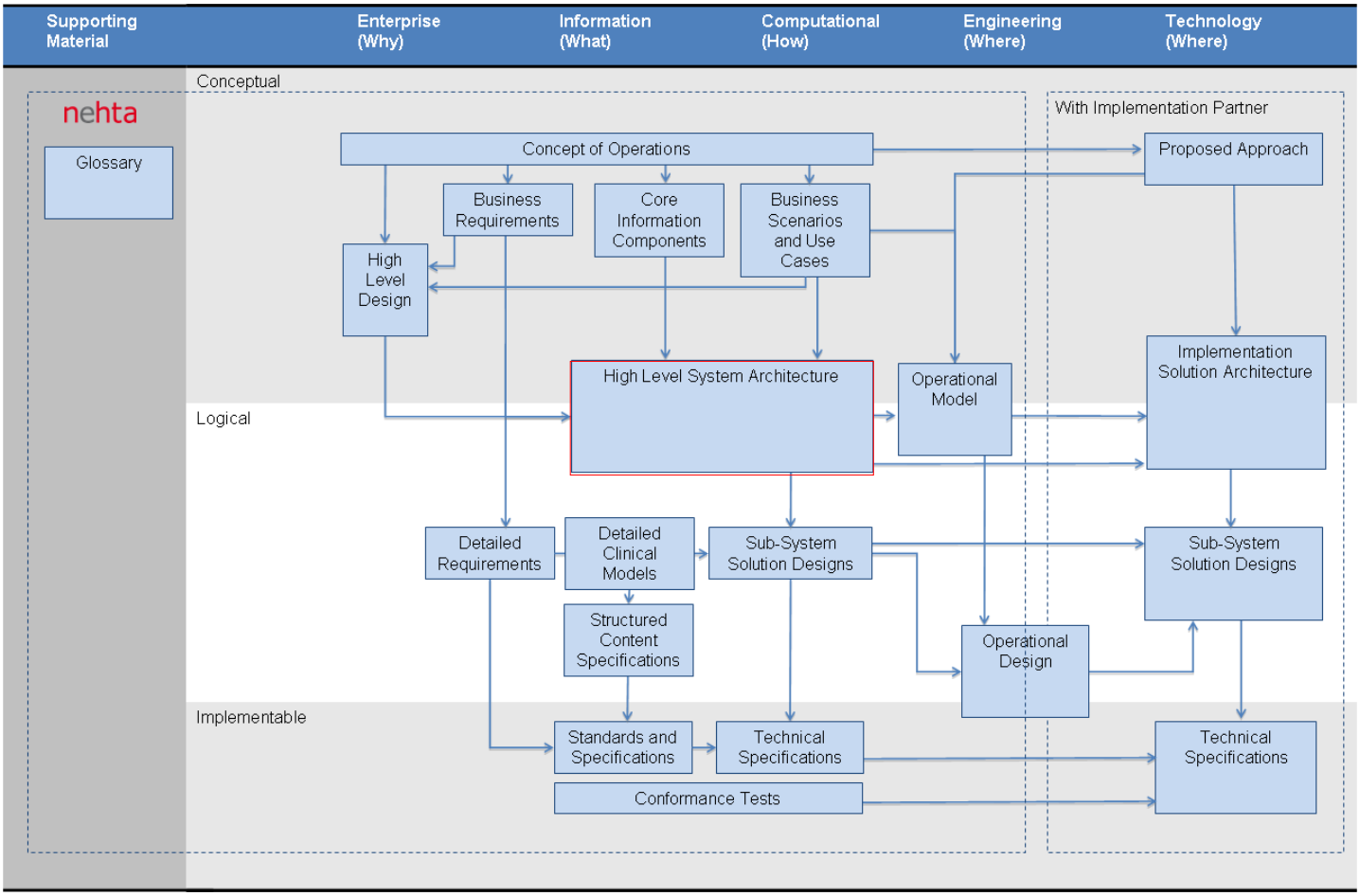
This document assumes the reader has read the April 2011 version of the PCEHR System Concept of Operations.

Document status

Name	PCEHR System - High-Level System Architecture	
Date	11 November 2011	Status: Final This document is based on the April 2011 release of the Draft Concept of Operations (ConOps). It will be updated in future to reflect the latest version of the ConOps and to reflect changes to the PCEHR design developed by the National Infrastructure Partner.
Owner	NEHTA Head of PCEHR	

Document Map

The PCEHR High-level System Architecture is one of a number of design documents being produced as part of the PCEHR System Standards Foundation and Architecture work stream. The following diagram outlines this document's relationship to other documents.



How to Read this Document

Readers may prefer to focus on different sections of the document:

- A reader seeking a high level conceptual overview of the architecture should read section 2.
- An implementer should read the logical overview of the PCEHR System architecture in section 3.

The modelling notation used throughout this document is based on the Unified Modelling Language (UML). This document assumes that readers of the logical system view and later sections are familiar with UML.

PCEHR Glossary

Please refer to the PCEHR System Glossary for definitions of key terms and abbreviations.

This page is intentionally left blank

Table of Contents

1 Architectural approach

1.1 Introduction

The architecture is a critical deliverable for the PCEHR Standards, Foundation and Architecture work stream as it will describe the fundamental organisation of the PCEHR System, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution[1]. An effective architecture for the PCEHR System will provide a vehicle for communicating how the system will work to a range of stakeholders and a basis for analysis of the system as a whole[2].

This section outlines the framework used to document the PCEHR System architecture, how the different architectural documents fit together and the role of this specific document.

1.2 National E-Health Framework

The PCEHR System has been architected using NEHTA's National eHealth Framework (NEHF). The NEHF is based on a combination of the Australian Government Architecture (AGA)[3] and HL7's Service Aware Interoperability Framework (SAIF)[4][5].

The NEHF is used by the PCEHR System to help deliver consistent and cohesive eHealth specifications. The NEHF 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.

The NEHF has a number of layers of abstraction (Figure 1), with the top layer focussing on defining the system in a stakeholder-centric fashion at the conceptual level, the addition of detail and refinement of the system definition at the logical level and then finally mapping that logical specification onto a number of technology-specific implementable specifications.

[1] Definition adapted from ANSI/IEEE Std 1471-2000, Recommended Practice for Architectural Description of Software-Intensive Systems

[2] Definition adapted from CMU/SEI-2001-TN-010 - Documenting Software Architectures: Organization of Documentation Package

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

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

[5] The NEHF differs from other popular frameworks such as TOGAF. TOGAF is more of a process-oriented framework for creating and managing architectural artefacts. NEHF is a specification framework used to describe system architectures. NEHF. 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 NEHF are more similar to the categories that underpin the Zachman framework. However, RM-ODP also provides a specification language that is compatible with UML.

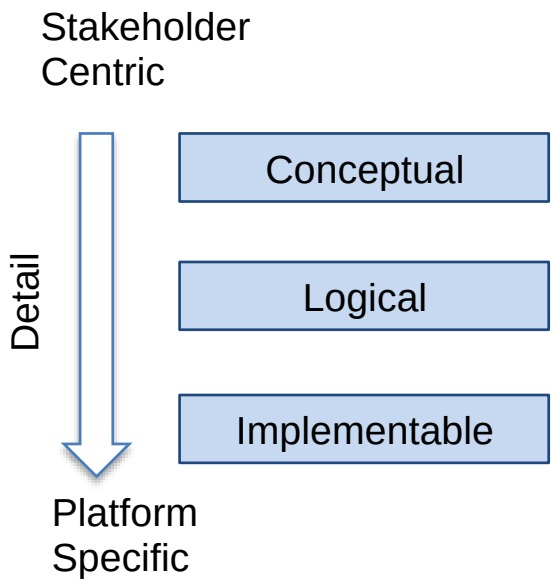


Figure 1: Layers of abstraction in the architecture

Separating conceptual from logical, and logical from implementable, allows the PCEHR System 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.

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.

Within the NEHF, there are a number of "viewpoints", shown in Figure 2. These include:

- 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/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.

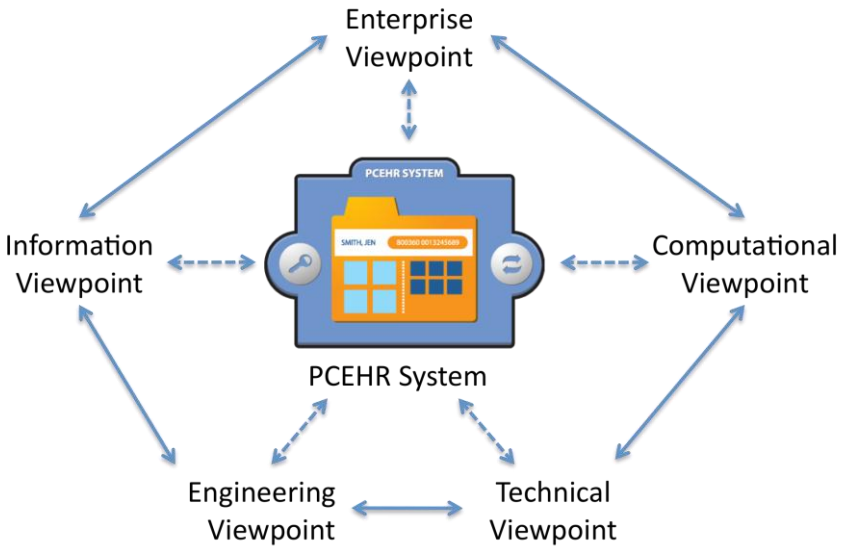


Figure 2: Architecture viewpoints

This document focuses on the enterprise, information and computational viewpoints of the PCEHR System and each of these areas are represented as distinct sections within the document.

The overlay between the viewpoints in Figure 2 and the layers of abstraction in Figure 1 creates a matrix of views. These views may be addressed by multiple documents.

A representation of this matrix is shown in the below table, indicating the kinds of artefacts expressed in each level of abstraction and viewpoint. This document covers those items highlighted in **bold**. The items in *italics* will be covered in other documents.

	Enterprise	**Information**	**Computation**	**Engineering**	**Technology**
Conceptual	**Purpose** **Scope** **Constraints** **Principles** **Policies** *Business Requirements* *Business Scenarios*	**Conceptual Information Model** *Core Information Component Models*	**Functional Components**	NA	NA
Logical	*Business Use Cases*	**Logical Information Architecture** *Detailed Clinical Models* *Structured templates*	**Logical Components** **Logical Interfaces** **Logical Level Interactions**	*Deployment model*	NA
Implementable	NA	*Standards Profiles* *XML Schemas* *Reference Sets*	*Standards Profiles* *Web Service Specifications*	*Standards Profiles*	*Implementation Guides*

1.3 Architecture Documents

NEHTA's role is to work with its stakeholders and deliver a range of documents, as detailed below.

Conceptual Level

- Concept of Operations, which provides an overview of what the PCEHR System is and how it is proposed to work.
- Business requirements, which provides a set of high level requirements about the PCEHR System.
- Core information components, which outline the kind of information required to be stored within the PCEHR System.
- Business scenarios and use cases, outlining common usage scenarios and the steps or actions undertaken by users of the PCEHR System.

Logical Level

- High Level Solution Architecture, which provides an overview of the architecture of the PCEHR System from the conceptual and logical level and defines the enterprise, information and computation viewpoints. As much of the conceptual level of the architecture has already been described in other documents, such as the Concept of Operations, this document will only summarise the conceptual level and provide more detail around the logical level.
- Detailed requirements, which provide a detailed list of conformance points required of the final solution. These conformance points will form the basis of system acceptance and will help drive the production of conformance tests.
- Detailed clinical models, which define a set of reusable information models and are used to ensure a point of consistency between different clinical document specifications
- Structured content specifications, which provide detailed information about the structure of clinical documents.
- Interface specifications, which provide a detailed logical view of each interface to be supported by the PCEHR System.

Implementable

- Standards and other specifications, which provide an implementable set of specifications that suppliers of systems will be expected to implement.
- Conformance tests, which define the conformance test procedures to be used in the conformance assessment of the PCEHR System and systems connecting to the PCEHR System.

NEHTA will work with a range of implementation partners, including the national infrastructure partner, to deliver an implementation of the PCEHR System and its connecting systems. These partners will deliver a range of documents, as detailed below.

Conceptual

- Proposed approach describing how their product set meets the Concept of Operations, and other related documents, such as the business requirements, core information components and the business scenarios and use cases.

Logical

- An implementation architecture and sub-system design documents, describing how their product meets the high level solution architecture, structured content specifications and interface specifications.

Implementable

- Technical specifications describing how their product supports the appropriate standards and related NEHTA specifications.

Note that the implementation partner is likely to use their own framework for defining each of these deliverables. As a result there might not be a direct correspondence in document naming conventions between NEHTA deliverables and the partner's deliverables.

2 Conceptual View of the System

The PCEHR System conceptual architecture is intended to define the high level PCEHR System architecture and it covers the following viewpoints:

- Enterprise viewpoint covering the system purpose, scope, constraints, principles and key policies.
- Information viewpoint, covering the Conceptual Information Model and Core Informational Elements.
- Computational viewpoint, covering major functional components of the system and outlining key interactions.

This section is non-technical and provides an architectural treatment of the material covered in the PCEHR Concept of Operations.

2.1 Enterprise Viewpoint

2.1.1 Background

eHealth is important to the future of health care in Australia. For individuals and healthcare providers alike, it will enhance the way healthcare is delivered.

eHealth is an integral part of the Australian Government's agenda for Health Reform, an agenda that aims to create a continuously improving healthcare system for the 21st century – a system that is accountable, affordable and sustainable, with safety and quality at its centre.

The Personally Controlled Electronic Health Record (PCEHR) System is the next step in using eHealth to enhance the healthcare system. The PCEHR System enables the secure sharing of health information between an individual's healthcare providers, while enabling the individual to control who can access their PCEHR.

The Government has invested $466.7 million in the first release of the PCEHR System. The first release delivers the core functionality required to establish a PCEHR System that can grow over time. The first release will ensure that all individuals seeking care in the Australian healthcare system will be able to register online for a PCEHR from July 2012, if they choose to do so.

The PCEHR System will build on the foundation laid by the introduction of the National Healthcare Identifiers for individuals, healthcare providers and healthcare organisations, as well as the National Authentication Service for Health, standard clinical terminologies and methods for communicating health information between healthcare providers such as discharge summaries and electronic referrals.

Beyond July 2012, the policy directions for eHealth are clear. The Government's complementary investment in telehealth, coupled with the rollout of the National Broadband Network, align with the National E-Health Strategy trajectory endorsed by the Australian Health Ministers' Conference in 2008. Additionally, the current two-year investment in the PCEHR Program, including in the lead eHealth sites, will inject significant momentum for PCEHR use in designated regions and consumer cohorts building towards a tipping point for broader adoption as the national infrastructure elements come on line. The work of the PCEHR Benefits Evaluation Partner will also be critical to demonstrating tangible benefits and improvements against baseline activity.

It is recognised that the PCEHR System will grow over time, and government investments, user expectations and market forces will simulate this growth. Government funding for the PCEHR System beyond July 2012 will be subject to consideration in the 2012-13 Budget context. Further consultation, including collaboration with the states and territories, will be required to consider a sustainable model for ongoing operations of the PCEHR System, ongoing change and adoption and further enhancements to the PCEHR System.

2.1.2 Project Vision and Concept

The national PCEHR System aims to place the individual at the centre of their own healthcare by enabling access to important pieces of health information when and where it is needed by individuals and their healthcare providers.

Individuals will be able to choose whether or not to have a PCEHR, and if they choose to participate, they will be able to set their own access controls. Using the PCEHR System, individuals will be able to access their own healthcare information and allow their healthcare providers to access and use this information to provide more coordinated and effective care for the individual.

Individuals will have greater involvement in their care through increased access to their information and other resources and will not be required to remember all the details of their previous healthcare.

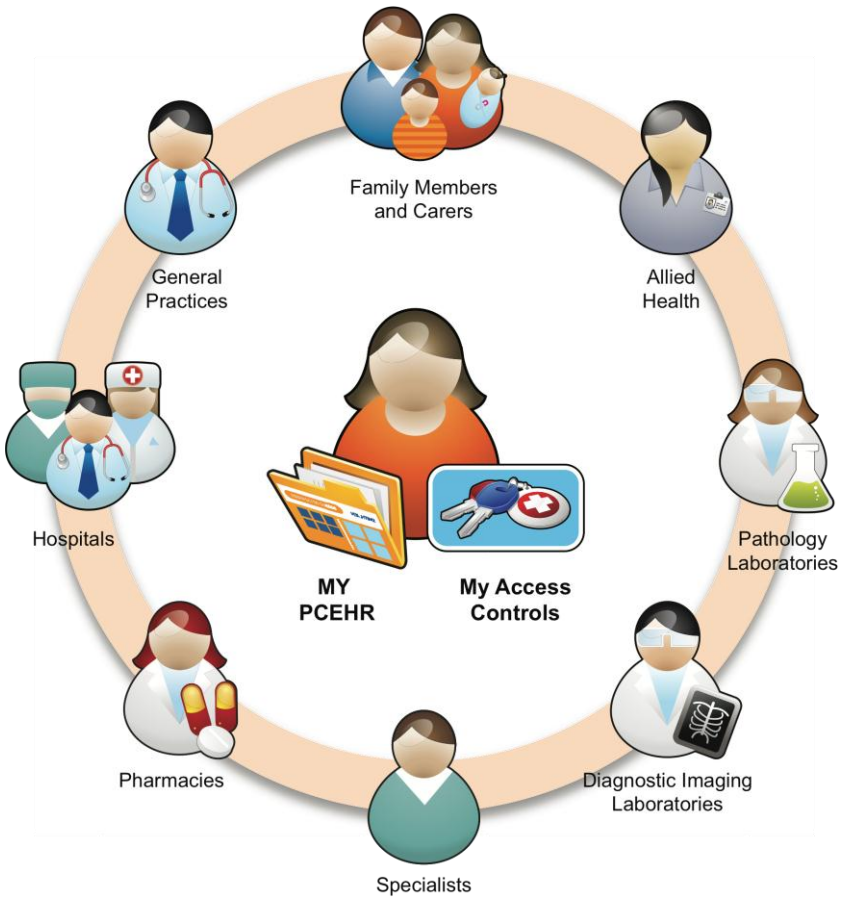


Figure 3: PCEHR System concept

In order to deliver this vision, the PCEHR System will provide:

- Secure access for individuals and their healthcare providers to their eHealth records via a range of access channels.
- A national set of services that will allow streamlined access to eHealth records, drawn from multiple repositories, such as:
  - A Shared Health Summary including allergies/adverse reactions, medicines, medical history and immunisations.
  - Clinical documents such as discharge summaries, event summaries and other documents over time (e.g. pathology result reports, specialist letters, etc.).
- Governance, legislation and oversight to ensure trust and confidence in the PCEHR System.
- The national standards, planning and core national infrastructure required to use the PCEHR System.

2.1.3 System Purpose

The purpose of the PCEHR System is to address information fragmentation across the current healthcare system by allowing an individual to more easily access their own health information, and to make their health information securely accessible to different healthcare providers involved in their care.

The PCEHR System will only collect personal information for the purpose of supporting an individual's healthcare. Information within the PCEHR System will also be reported against for operational and management purposes.

2.1.4 System Scope

The scope and focus of the PCEHR System funded by the Commonwealth includes the implementation of the core national infrastructure to support the operation of the PCEHR System, including key components such as:

- Access channels, such as a consumer portal, provider portal, report portal, B2B gateway and call centre.
- The core PCEHR services required to support major functional areas around participation and authorisation, indexing, views, audit and reporting.
- A National Repositories Service holding a minimum critical set of healthcare information about participating individuals within multiple nationally operated repositories.
- The capability to connect to conformant repositories and portals as they become available.
- Support for a range of systems accessing the B2B gateway, such as clinical systems and contracted service providers.
- A new foundation service for supporting templates.

The PCEHR System needs to support:

- Registration and managing the ongoing participation of individuals and healthcare providers.
- Access controls managed by the individual.
- The access controls will include a number of base features around access control. Options around more advanced features may also be included.
- The collection of health information from a range of points of care, including: Shared health summaries, event summaries, discharge summaries and consumer entered information.

- This information, subject to the individual's access controls, will provide the base information required to support sharing of important information around allergies/adverse reactions, medicines, medical history and immunisations. This information will facilitate improved continuity of care, medication management and consumer participation.
- In addition to this, a range of optional information sources will be considered in the first release. The options include: specialist letters, pathology result reports, diagnostic imaging reports, Medicare information (e.g. Medicare claims history, PBS data, ACIR and Organ Donor), referrals, prescriptions/dispense notifications and the location of the individual's advance care directives (if they have one).
- The consolidation and analysis of information collected in the PCEHR System via:
    - Views to enable easy access to consolidated information about an individual's allergies/adverse reactions, medicines, immunisations and medical history.
    - Reports to support the evaluation and operational requirements of the PCEHR System.

2.1.5 System Interfaces

As illustrated in Figure 4 on the following page, the PCEHR System is designed to interface with a number of existing and new systems. These interfaces include:

- Consumer oriented systems, including:
    - Browser-based access to a consumer portal
        - Use of conformant portals. Note that some lead eHealth sites may already be establishing conformant portals.
- Healthcare provider oriented systems, including:
    - Clinical systems. Note that some lead eHealth sites are working with a range of healthcare provider systems. Many of these systems are on a "multi-use" list.
    - Contracted service providers, which provide healthcare software as a service.
- Repositories, including:
    - Medicare repository(s), designed to support sharing of Medicare information, including:
        - Medicare Benefits Schedule (MBS) claiming history
        - Pharmaceutical Benefits Scheme (PBS) claiming history
        - Status from the Australian Organ Donor Registry (AODR)
        - Australian Childhood Immunisation Registry (ACIR).
    - Diagnostic service provider repository(s), designed to share pathology result reports and diagnostic imaging reports.
    - State, territory and regional repositories. Note that some lead eHealth sites may be establishing conformant repositories. These sites could include:
        - NT Department of Health and Families
        - NSW Department of Health
        - Wave 1 sites.

- Other repository providers, including lead eHealth sites funded under Wave 2, namely:
  - eRx Script Exchange Program (eRx).

- Foundation infrastructure:
  - HI Service, for healthcare identifiers.
  - NASH Service, for digital credentials
  - A CTI Service for clinical terminology reference sets
  - A Template Service, which provides definitions about the types of healthcare information that can be shared via the PCEHR System (and other systems). Note that this is a new service funded under the PCEHR Program.
  - A National Healthcare Provider Service Directory, which provides a "Yellow Pages" style search of healthcare providers and organisations and location of end point services for delivering electronic messages. Note that this is a new service which is funded by COAG separately from the PCEHR Program.

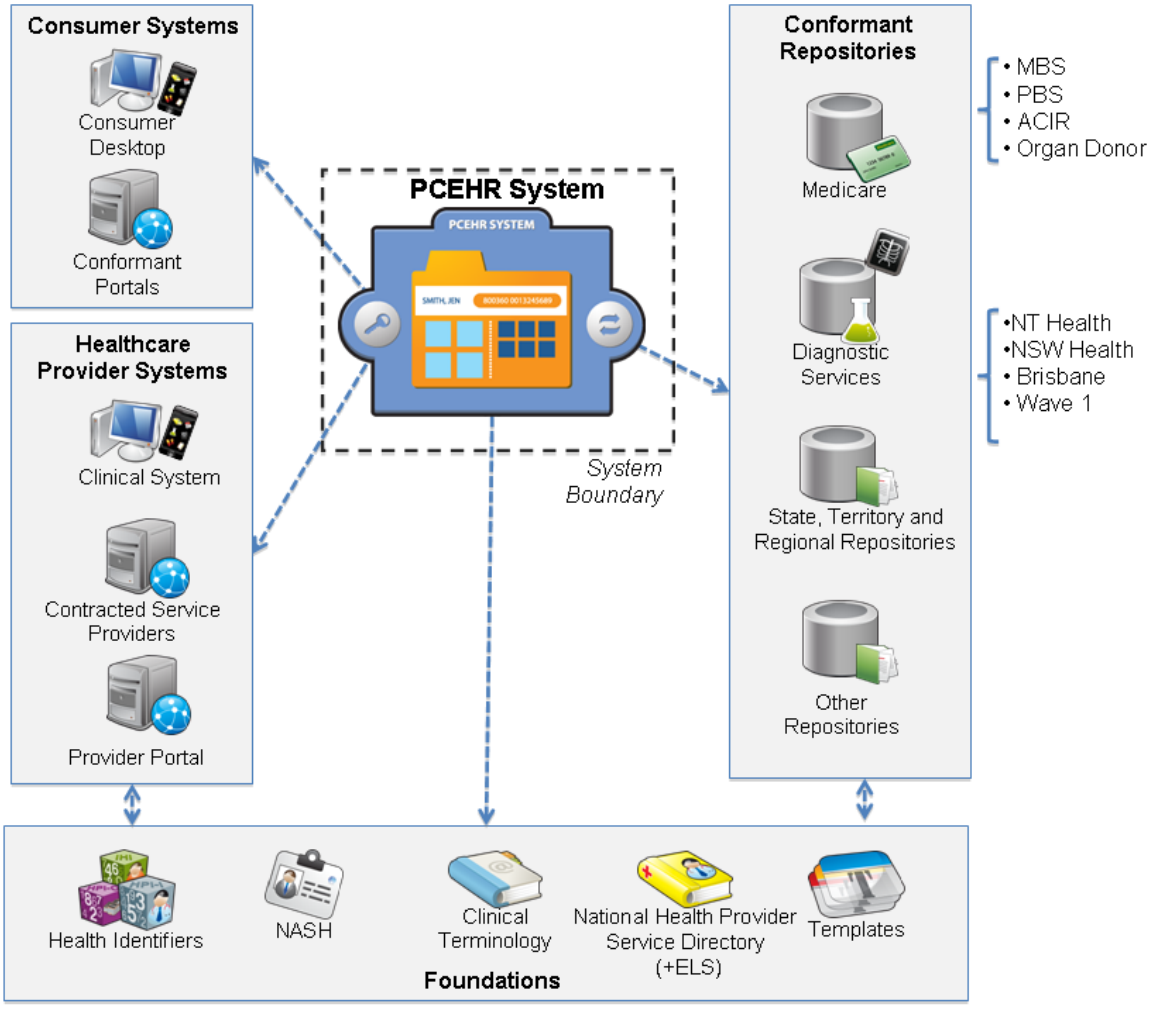


Figure 4: PCEHR System interfaces

2.1.6 System Constraints

2.1.6.1 Budget

Constraint	Architectural Implications
The government has committed $466.7 million to the first release of the PCEHR System. This commitment will be invested in procuring a PCEHR System, program management and governance, change and adoption, development of the standards foundation and architecture and the funding of lead eHealth sites. Note that the PCEHR System budget has not been disclosed for probity reasons.	• Sufficient budget has been provided with the expectation of procuring a nationally scalable system. • Procurement processes will demand a value for money solution.

2.1.6.2 Timeframe

Constraint	Architectural Implications
From July 2012, individuals will be able to register online for a PCEHR. As the PCEHR System is taken up by healthcare providers, registered individuals will be able to progressively reap the benefits of having a PCEHR.	• The registration elements of the system are some of the highest priority components.
The government budgetary process requires that all funding should be committed by 1 July 2012. The funding for the PCEHR System has already been committed and no additional funding will be allocated prior to July 2012.	• Given that time is of the essence, a new build of infrastructure is unlikely within the timeframe available. Customisation of an existing off-the-shelf solution will be preferred.

2.1.6.3 Risk

Constraint	Architectural Implications
The Australian Government's tolerance for risk within ICT projects is low.	• The final solution will need to be assembled (as much as possible) from proven components. • Key areas of risk will be around privacy and security and the architecture will need to ensure this has been adequately dealt with.

2.1.6.4 Approach

Constraint	Architectural Implications
The PCEHR System is not mandatory — participation by individuals will be voluntary.	• The PCEHR System will need to provide sufficient infrastructure to efficiently manage registration processes • The PCEHR System needs to have a compelling user experience, otherwise user uptake will be limited
The PCEHR System is not a comprehensive record of an Individual's healthcare — only key health information shared from participating source systems will be available via the PCEHR System, subject to access controls. This information will only be summaries of the episodes of care (e.g. a Discharge Summary or an Event Summary) and not the full record of care (e.g. the full hospital medical record).	• Management of data quality will be essential to ensure that the right information is available for the right individual at the right time.
The PCEHR System is not a replacement for local health records — the introduction of a PCEHR System will not reduce the requirement for healthcare providers and organisations to maintain their own health records. It will complement existing local health records by providing a way of securely sharing health information.	• The interface between local clinical systems and the PCEHR System needs to be clearly defined
The PCEHR System is not a replacement for existing clinical communications — existing provider-to-provider communications, such as Referrals, Discharge Summaries, pathology Requests and Result Reports, Prescriptions etc., will continue to flow using existing communication channels. The PCEHR System provides a new complementary communication channel.	• As much as possible, the PCEHR System should take copies of information shared in existing communication processes
The PCEHR System is not a single central national database — the information that makes up an individual's PCEHR will originate from multiple sources and be stored in multiple repositories.	• The national infrastructure needs to have a distributed architecture, with multiple services and repositories.
The PCEHR System is not a way of directly accessing healthcare provider records — participating healthcare providers will upload copies of clinical documents into the PCEHR System.	• The PCEHR System cannot "reach" into provider records. The provider system needs to supply copies of the records to be shared.

2.1.7 Principles

The PCEHR System Concept of Operations identified a number of principles for the PCEHR. These are listed below, with the architectural implications of each.

Principle	Architectural Implications
Personally Controlled: Individuals will be able to choose whether or not to have a PCEHR, and if they choose to participate, they will be able to set their own access controls.	• The architecture will need to ensure that individuals have control over a number of elements of their PCEHR.
Value: Deliver a PCEHR System that offers value to both individuals and their healthcare providers.	• The architecture will need to support components that are tailored for different user groups
National infrastructure: Deliver core elements of PCEHR System infrastructure once, rather than duplicating development costs and efforts and increasing the impact of rework.	• The architecture should facilitate reuse wherever possible. This may include the reuse of physical components (or sub-components), specifications, test tools or any other applicable artefacts. As such, all deliverables should be developed in a manner that readily supports reuse.
Stakeholder engagement: Actively engage key healthcare stakeholders in the design and delivery of the PCEHR System.	• Stakeholder involvement in the development of the architecture is required. • Key points of signoff will be within the NEHTA co-chairs, the NHCIOF and the Department of Health and Ageing. • Consultation with the ICT industry, jurisdictional implementers, lead eHealth sites and other implementers is required.
Incremental approach: Build the PCEHR System in an incremental and pragmatic manner, focusing initial investment in those areas that that deliver the greatest benefits.	• The architecture will need to support a range of extension points for future enhancements
Recognising different starting points: Balance active support for healthcare providers with less developed capability, while not constraining the ability for more advanced participants to progress.	• The architecture will need to provide multiple methods of accessing the system to accommodate new and legacy systems. • The architecture will need to support staged pathways to full adoption where applicable.
Leverage: More effectively leverage and scale existing and planned eHealth activities and standards in the delivery of the PCEHR System.	• The architecture must leverage the existing NEHTA foundations, including the HI Service, NASH, CTI Service and solution specifications for key transactions, such as Discharge Summaries, Referrals, ETP, etc. • The architecture will be required to leverage information assets within Medicare Australia, including MBS claiming history, PBS claiming history, and organ donor status and childhood immunisations. • Integration with lead eHealth sites will need to be considered.

Principle	Architectural Implications
Balancing alignment and independence: Drive alignment of PCEHR System implementation activities whilst not unnecessarily limiting the ability of participants and vendors to implement locally relevant solutions.	• Localisation of standards based information feeds may need to be considered to accommodate variance.
Trust and confidence: Deliver a PCEHR System that all users are able to trust that it is governed effectively; individuals trust that their privacy has been handled appropriately; and moreover, users are confident in the quality and safety of the health information provided by the PCEHR System.	• Key areas of risk will be around privacy and security and the architecture will need to ensure this has been adequately dealt with.
Relevant skills: Ensure sufficient numbers of skilled practitioners are available to support delivery of the PCEHR System	• The change and adoption partner to assess how the PCEHR System can be transitioned into operations.

2.2 Conceptual Computational View

The conceptual computational view provides a non-technical overview of the key computational features. Where the enterprise view focuses on providing the functional outline of the system and the enterprise it fits into, the computational view breaks this into logical functional sub-units which interact at their interfaces.

The PCEHR System allows clinical organisations to associate appropriately structured clinical documents with a specific individual. The PCEHR System gives the individual, or their nominated or authorised representative(s), complete control over access to their PCEHR. The system also provides the ability to monitor and track the operational progress of the overall system.

2.2.1 A PCEHR

A PCEHR is a logical construct; it is analogous to a folder of clinical records associated with an individual. The folder is logical as the actual records may be spread across numerous distinct systems. A PCEHR is related to a single individual.

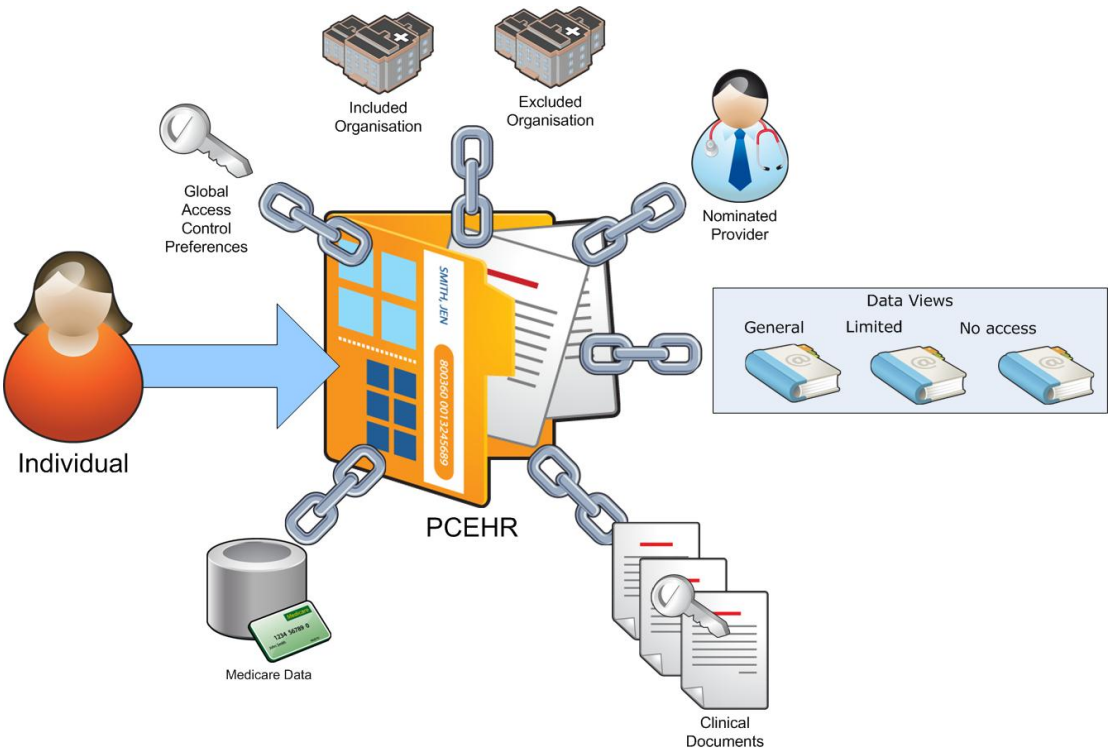


Figure 5: A PCEHR

A PCEHR encompasses:

- An individual
- Global access controls (i.e. General Access, No Access or Limited Access)
- Sets of included and excluded health organisations which control access to an individual's PCEHR
- A nominated provider
- Set of Medicare records (patient demographic, ACIR, MBS, PBS and AODR)
- Sets of PCEHR clinical documents where each of the documents may have document access controls.
- A consolidated view which can be created at the General Access, No Access or Limited Access level depending on the requester's access control permissions.

Key Principles

- The relationship between a provider and the PCEHR is mediated by a set of access controls.
- Individual documents may be marked as being for general access, limited access or no access (other than to the managing individual and the author).
- Views created from document or metadata must be sensitive to the access level of the requestor. This in effect leads to three logical versions of each view, a general access view, a limited access view and a no access view.
    - The general access view contains data from documents marked as being for general access
    - The limited access view contains data from documents marked as being for general or limited access.
    - The no access view contains data from documents marked as being for general, limited or no access. This is only visible to the PCEHR managing individual and to the document author.

2.2.2 PCEHR System Conceptual Component Model

Figure 6 shows a conceptual breakdown of the functional components proposed within [PCEHR_CON_OPS] into sub-functional areas. It is important to realise that this diagram provides functional groups and is not intended to provide technical or implementable definitions.

Each layer is dependent upon the layer below and all layers are dependent upon the foundation services on the left hand side of the diagram.

An A3 version of this diagram is available in Appendix C at the end of this document.

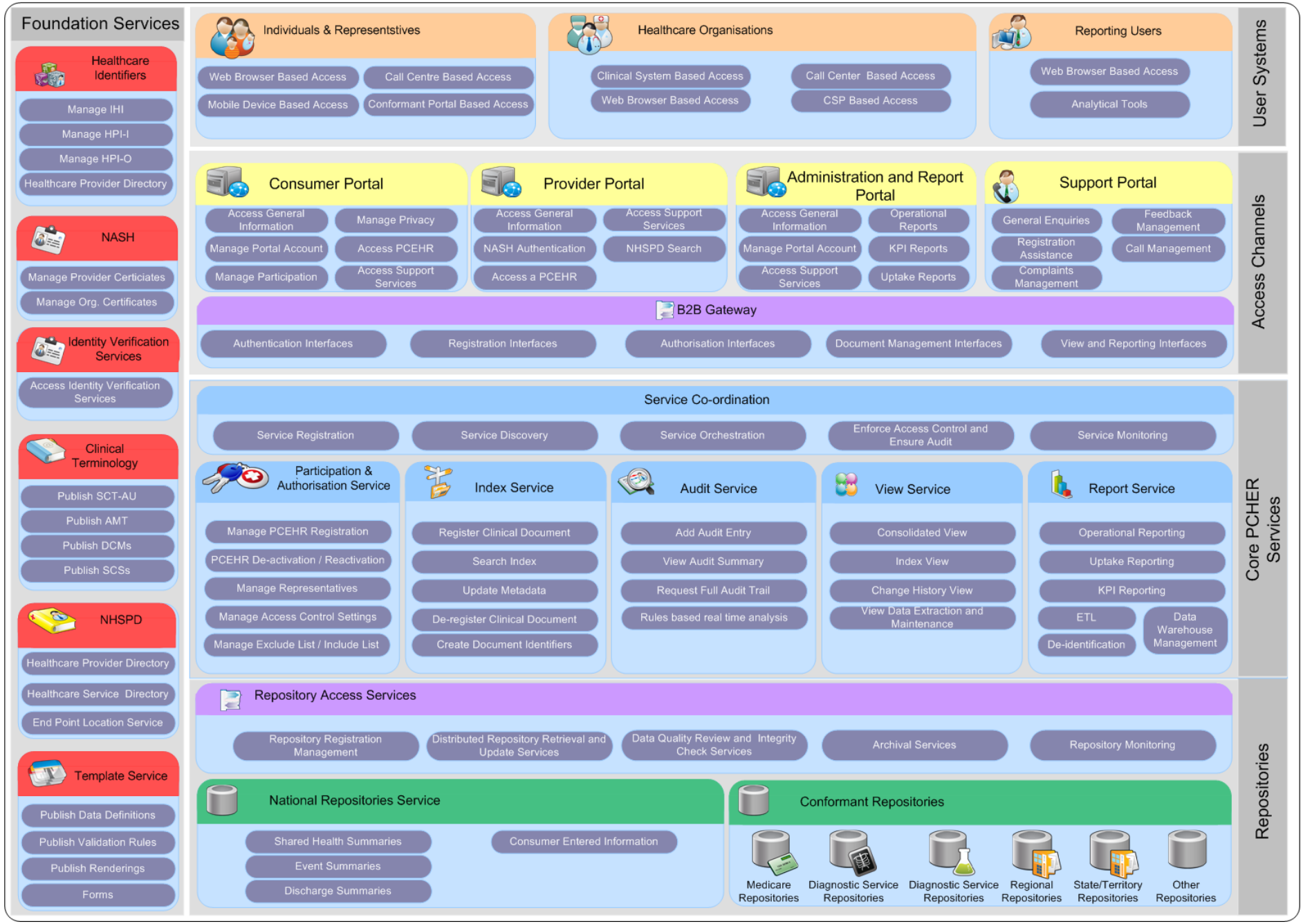


Figure 6: Conceptual computational view

2.2.3 PCEHR Conceptual Components

In order to support the tendering process, the PCEHR System has been split into bundles, which include the following:

- Consumer Portal
- Provider Portal
- Core PCEHR Infrastructure Services
- Template Service
- Reporting Service

The operations and call centre bundles are not elaborated within this document.

The following sections describe the separation of system functions across the functional bundles and conceptual system components.

2.2.3.1 Consumer Portal

The consumer portal provides a web browser based user interface for registering and administering an individual's PCEHR.

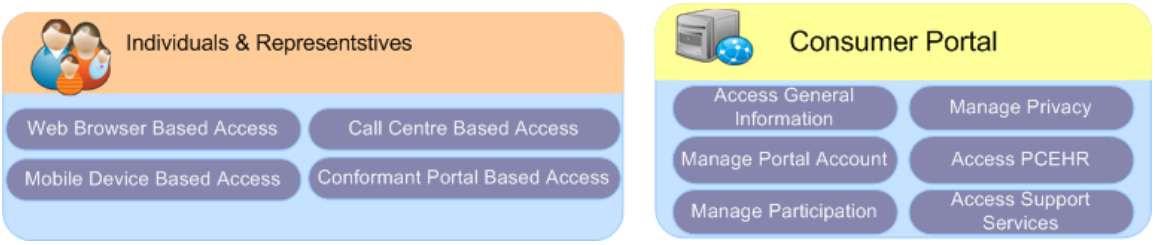


Figure 7: Conceptual Consumer Portal

The consumer portal is the encapsulation of the functionality required to:

- Locally validate a user's identity to a sufficiently strong degree.
- Associate the local account with an Individual Health Identifier (IHI) and a PCEHR.
- Allow the user to easily access healthcare information which has been sourced from various records within the PCEHR and assembled by the View Service.
- Allow the user to view audit logs.
- Allow the user to view clinical documents (according to minimum user software requirements)
- Provide a user interface for controlling organisations' access to the PCEHR, including the management of exclude lists, include lists and document level access controls (the actual operations are performed by the core infrastructure components).
- Provide a user interface for changing global PCEHR access rights (the actual operations are performed by the infrastructure component).
- Provide a user interface for managing user preferences and contact settings (the actual operations are performed by the infrastructure component).
- Provide a user interface for specifying the location of the Advanced Care Directive (the actual operations are performed by the infrastructure component).
- Provide a user interface for nominating a representative.

- Allow the user to link to and manage PCEHRs for which they are nominated.
- Support the future functionality required to allow users to add a document to their PCEHR.

A Conformant Portal represents a portal proven to be Conformant to the specification for a Consumer Portal. The national Consumer Portal is therefore an instance of a Conformant Portal. The detailed specification of the requirements for conformance are deferred to the Conformant Portal Solution Design. The provider portal is not related to a conformant portal.

2.2.3.2 Provider Portal

The Provider Portal provides a web browser based user interface for providers to view PCEHR data. It is expected that will be used where using a Clinical Information System to access the PCEHR is not possible or appropriate.

Figure 8: Conceptual Provider Portal

The Provider Portal is an encapsulation of the functionality required to:

- Locally validate a Provider's identity to a sufficiently strong degree as per the National E-Health Authentication Framework (NEAF).
- Associate the account with a Healthcare Provider Identifier-Organisation (HPI-O) and an Healthcare Provider Identifier-Individual (HPI-I) and the related credentials.
- Allow the user to easily access healthcare information which has been sourced from various records within the PCEHR and assembled by the View Service.
- Allow the user to view clinical documents (according to minimum user software requirements).
- Allow the user to perform individual search. Individual search result will be sensitive to the individual access control against the user (Provider)

Note that in the initial release of the system it is not expected that Providers will be able add or edit documents through the provider portal.

2.2.3.3 Core PCEHR Infrastructure

The PCEHR Infrastructure Services bundle provides the core realisation of PCEHR services.

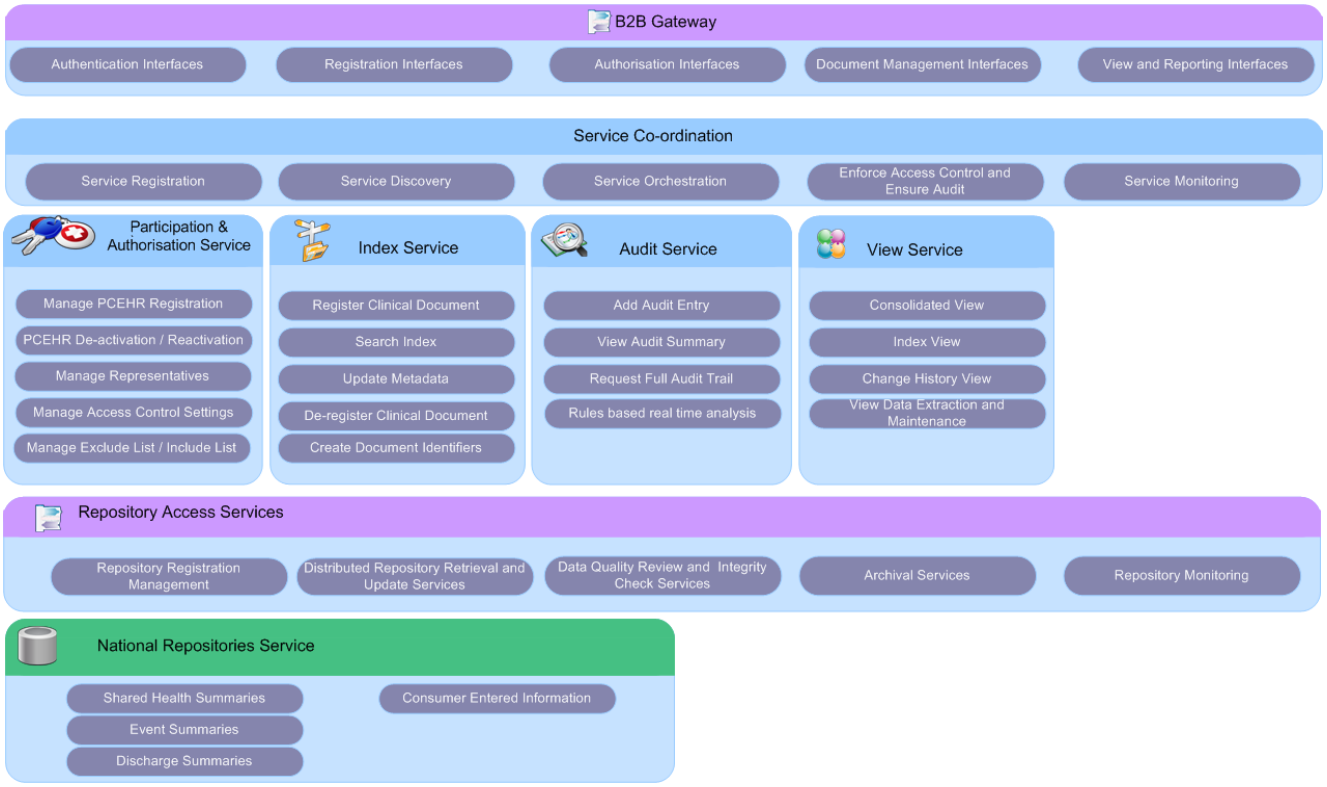


Figure 9: Conceptual core infrastructure services

This suite of components is required to support the following functionality.

User Management, Authentication and Authorisation

- Validate the identity of a conformant system.
- Associate providers with appropriate access control rights.
- Allow Individuals managing a PCEHR to:
  - Register for a PCEHR
  - Control who can access the PCEHR and the level of access that they have
  - Manage document level restrictions
  - Manage contact and system preferences
  - Appoint one or more Nominated Representatives
  - Suspend or deactivate a PCEHR.
- Manage emergency provider access.
- Manage personal information.
- Access an audit log of all key events.

Document Query and Management

- Allow conformant systems to:
  - Add documents to a PCEHR.
  - Search for documents within a PCEHR
  - Retrieve documents within a PCEHR.

- Provide populated views in an agreed format (display will likely be handled by the CIS or portal system).
- Provide a central instance of a conformant repository.
- Facilitate access into conformant repositories (both future and existing).

Reporting

- Log sufficient operational data to support the reporting service.
- Offer an externally accessible mechanism for the reporting service to extract the pre-determined operational data.

Auditing

- Audit all key points.

Templates

- Ensure all documents are compliant with a template specified within the Template Service.
- Control the actions which can be performed for clinical documents which are based on a specified template.
- Cache local copies of frequently used templates in line with the Template Service usage policies.

Interfacing

- Provide a mechanism for Clinical Information Systems and Conformant Portals to access the system's functions in a consistent and reliable way.

The PCEHR set of system interfaces will only be available to a closed group of user systems. All systems connecting to the Core infrastructure Services must demonstrate compliance with the relevant specifications and policies before they are allowed to use the service.

2.2.3.4 Reporting Service

The Reporting Service is responsible for providing reports on the operational parameters of the PCEHR System. The reporting service should replicate the required data from the PCEHR core infrastructure services component and store this data locally. Any individually identifiable data must be de-identified before leaving the PCEHR core system.

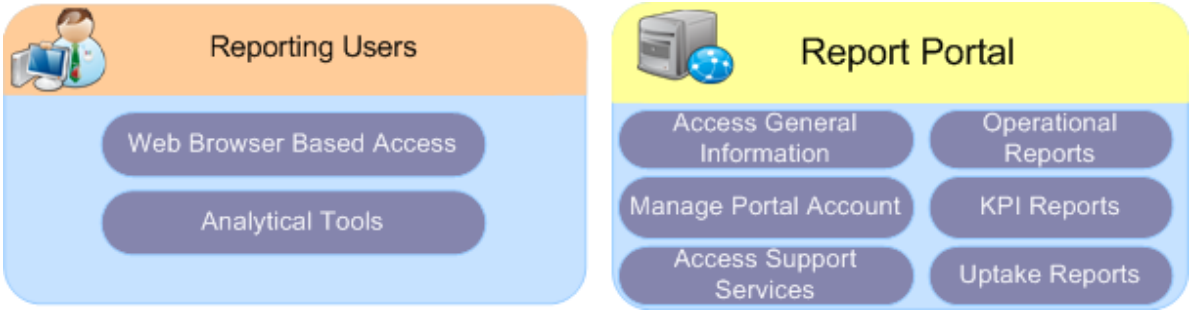


Figure 10: Conceptual Reporting Service

The reporting service will provide a set of tools and a number of pre-defined reports for interpreting the operational data.

2.2.3.5 Template Service

Within the scope of the PCEHR System, the Template Service is responsible for managing and storing the data representations associated with all of the data formats stored within a PCEHR.

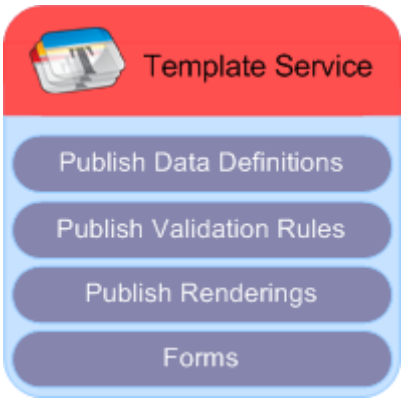


Figure 11: Conceptual Template Service

Each template describes the data format, how to validate against this format, the mechanisms for displaying or accessing all or parts of the data associated with a document matching the template.

Approved PCEHR templates cannot be modified. The addition of new PCEHR templates is expected to be infrequent and will be subject to a strict governance process. All template consumers are encouraged to limit their dependency on the Template Service and cache templates where appropriate.

2.2.4 Key System Usage Scenarios

This section shows how the functional bundles interact to complete key usage scenarios.

The diagrams within this section are intended to be intuitive and do not follow any formal notation. The labelled entities represent entities, components or actors, the labelled arrows represent steps (not necessarily control or data flows) and a circular arrow represents internal processing.

The Logical Computational Viewpoint (Section 3.1) outlines the key system interactions using a more complete "separation of concerns" and formal notation.

2.2.4.1 A Note on Error Handling

This section outlines some of the key error handling cases contained within the scenarios.

IHI Search

Where a provider searches for an IHI and is unable to find a match on the HI service, the HI Service will return an error to the requesting system. The HI Service does not currently provide a description of the reason for the failure.

Provider and Consumer Authentication

Where a provider or consumer cannot be suitably authenticated, they will not be granted access to the PCEHR System.

Provider Authorisation

If authentication fails, the requestor receives a generic error stating that the PCEHR could not be found or accessed.

2.2.4.2 Provider Opens a PCEHR

This section covers the steps associated with a provider opening a PCEHR.

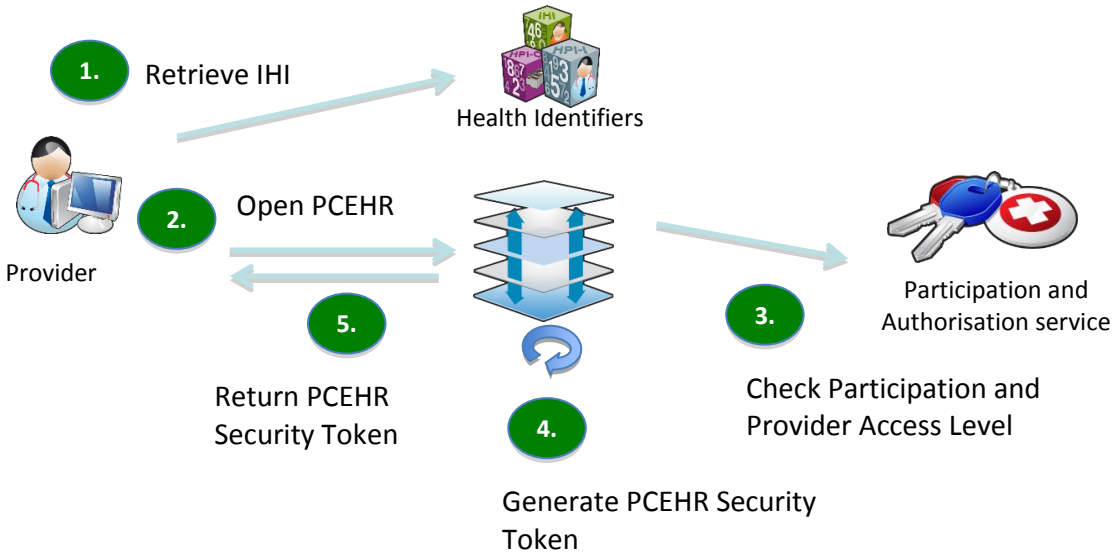


Figure 12: Conceptual view - provider opens a PCEHR

Performing an upfront open operation sets the context for future PCEHR operations and allows the calling system to avoid repeating expensive operations such as authorisation operations.

The process for opening a PCEHR is as follows:

- If the provider is accessing the PCEHR via a portal they must first query the HI service and retrieve the correct IHI (even if the IHI is known this validation must take place).
- Where a provider is accessing through a CIS system the system must query the HI service to retrieve the IHI on the first attempt. On subsequent attempts the CIS may locally store the IHI association between the CIS record and the IHI.
- When the IHI is identified an authenticated provider then requests that the PCEHR be opened.
- The provider supplies the IHI alone as the primary key for the PCEHR (as the demographic match is performed in preceding steps).
- If the IHI is found an authorisation check is performed.
- If the provider is authorised to open the PCEHR a PCEHR Security Access Token is created.
- The token is returned to the provider's system and may be used in subsequent calls.
- The Security Access Token is only valid for a limited time period and must not be accepted by the PCEHR System after it has expired.

2.2.4.3 *Provider Adds a Document*

This scenario covers the process where a clinical provider uploads a document to a PCEHR. There is no restriction placed on the type of provider.

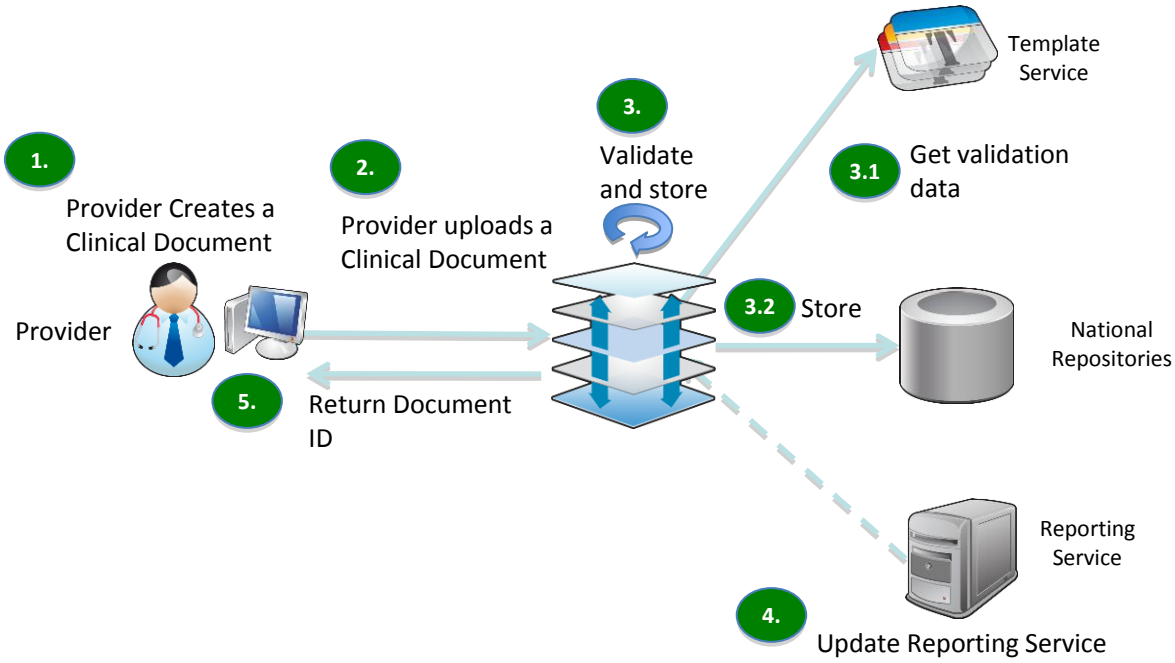


Figure 13: Conceptual view - provider adds a document

The clinician or clinical system creates a document which is attested to by the authorising clinician. According to the set of appropriate business rules, a copy may then be sent to the PCEHR System, which may use the validation definition provided by the Template Service to help validate the document. If the document is valid, it is added to the National Repositories and the reporting service is logically updated (in practice this may just mean that the event is recorded).

As any provider is allowed to upload a document regardless of their authorisation level, this process purposefully does not include the Open PCEHR operation or authentication and authorisation at the PCEHR level (although it must still occur at the connectivity level). An upload may follow the opening of the PCEHR by an authorised user but this is not mandatory.

2.2.4.4 Provider Retrieves a Consolidated View

This section outlines the process for a provider to access an Individual's consolidated view. The provider must have been authenticated and have opened the PCEHR prior to accessing the Consolidated View.

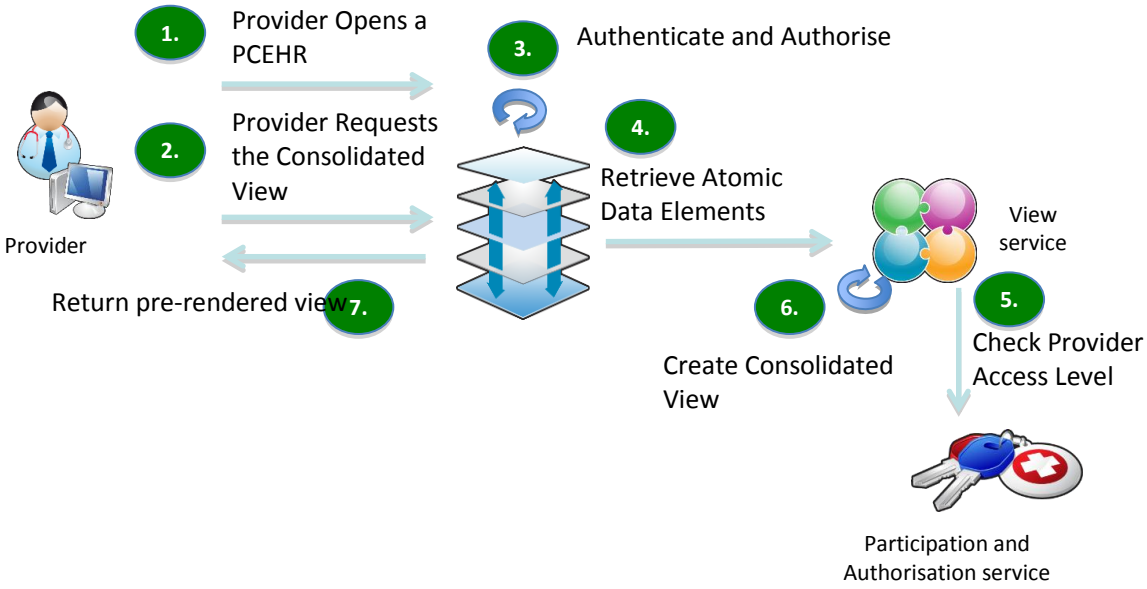


Figure 14: Conceptual view -provider retrieves a consolidated view

The provider will only be allowed access to the PCEHR if they are on the include list, the PCEHR is set to "General Access" mode or the usage is part of an emergency. The portal should not allow a user to access the screens relating to accessing the content within an Individual's PCEHR if they are not able to open the PCEHR.

The process for retrieving a consolidated view is as follows:

- A provider first opens the PCEHR (see 2.2.4.2).
- If the open request is successful, the provider then requests the Consolidated View from the PCEHR System.
- The provider's access level is determined.
- Only data taken from documents to which the provider has read access (including those the provider has authored) is used to create the view.
- Key stages are audited.
- The event is logically logged in the reporting service (this is logical as it may be stored as an audit row that can later be extracted as an offline process).

2.2.4.5 *Provider Retrieves a Document*

This scenario deals with the process for a provider accessing a document. It is likely that the provider has performed a search or accessed an index, change or consolidated view prior to this point in order to select the document.

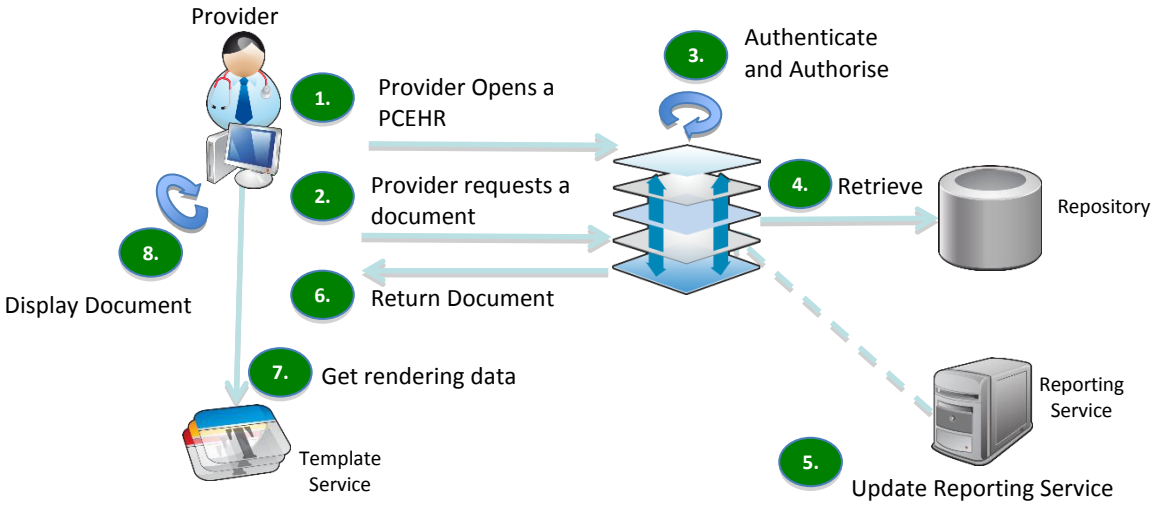


Figure 15: Conceptual view - provider retrieves a document

The provider will only be allowed access to the PCEHR if they are on the include list, the PCEHR is set to "General Access" mode or the usage is part of an emergency scenario. The portal should not allow a user to access document management screens for a specific PCEHR if they are not able to open the PCEHR.

Document search functions and views may be realised using PCEHR Views or directly within a CIS system. These functions must only include those documents matching the requestor's level of access.

Once the required document has been identified the process for retrieving a single document is as follows:

- A provider first opens the PCEHR (see 2.2.4.2).
- If the open request is successful, the provider then requests the document from the PCEHR.
- The PCEHR core services then determine whether the provider has sufficient access rights to view the document (this step is only necessary where PCEHR document IDs may be cached within client systems).
- If authorised, the document and accompanying envelope are retrieved and returned to the provider. The envelope will contain the document metadata, including the template used when submitting the document.
- Key stages are audited.
- The event is logically logged in the reporting service (this is logical as it may be stored as an audit row that can later be extracted as an offline process).

Providers who have previously had "Limited Access" rights may have locally stored document ids within a CIS system. Further requests for this document after access is revoked should be rejected (unless the provider is the author of the document).

The provider will only be allowed access to view the PCEHR if they are on the include list or the PCEHR is set to "General Access" mode. The portal should not allow a user to access document management screens if they are not able to open a PCEHR.

After retrieving the document the provider may obtain the document template in order to support the local validation and rendering process.

Although the above diagram shows a document being retrieved from the National Repositories the process is identical for documents retrieved from any conformant repository.

2.2.4.6 Individual Registers for a PCEHR

A consumer may register for a PCEHR through an online process using the Consumer Portal or via an assisted face-to-face registration process.

Key principles for PCEHR registration:

- The Individual's Identity must be validated and verified.
- The Individual must have an IHI number in order to be eligible to register for a PCEHR.

Registration via a Consumer Portal

A user may register for a PCEHR via a Consumer Portal. The user must first register with the portal and then associate the portal account with their PCEHR. A PCEHR may be associated with multiple portal accounts.

A portal account may be anonymous in nature and may not necessarily require upfront proof of identity. Before access to a PCEHR may be granted the individual must prove their identity.

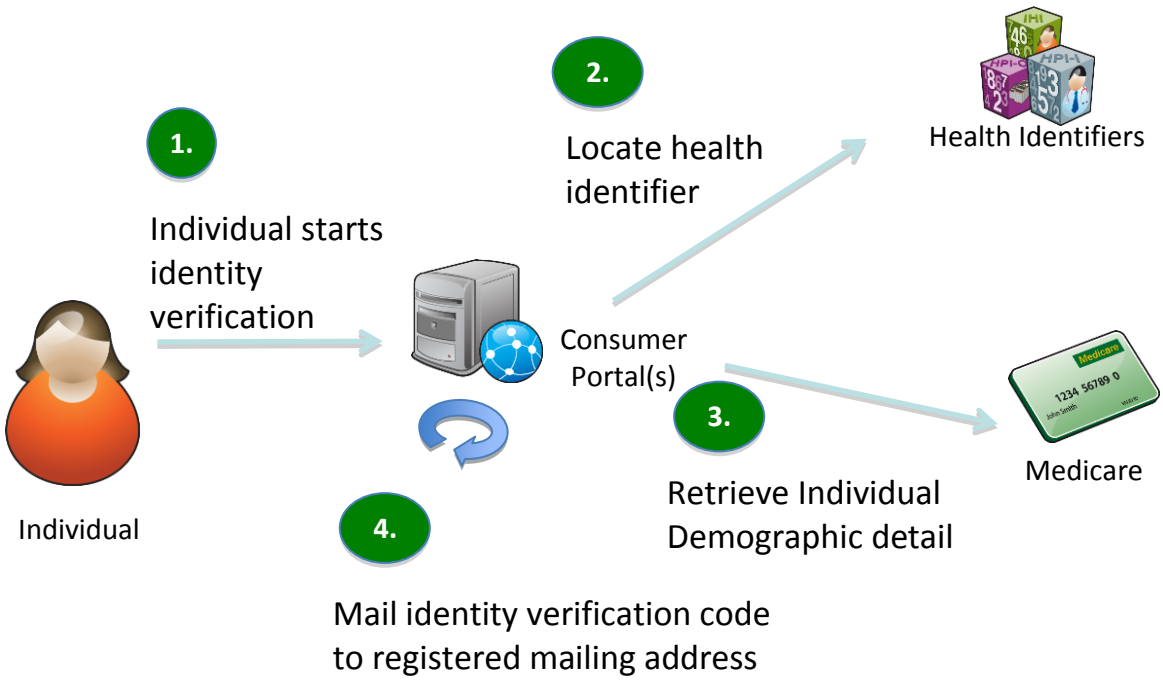


Figure 16: Identity verification - Step 1

The process for verifying identity is as follows:

- A portal user makes a request to associate the portal account with a PCEHR and provides a pre-defined set of demographic details.
- The portal locates the specified IHI.
- If the IHI and demographic details match those stored within the set of Medicare databases the Medicare system sends a verification code to the Individual's registered address.

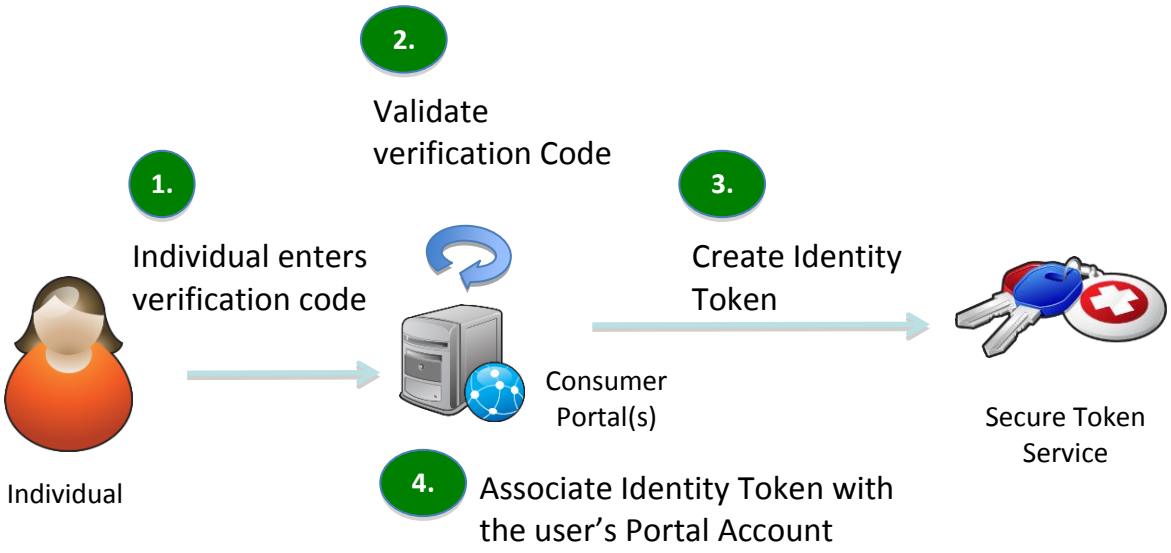


Figure 17: Identity verification - Step 2

The process for associating the verified identity with a portal account is as follows:

- The user logs into the portal and enters the postal verification code.
- The PCEHR System validates the verification code, IHI and demographic details.
- An identity token represents the association between a consumer portal identity and a PCEHR. Each distinct consumer portal account must use a different token.
- The identity token is stored by the consumer portal and used as the basis for credentialed identity in all future interactions with the PCEHR System.

Assisted Registration

In addition to registration through the consumer portal, a user may register through an assisted registration process by contacting a representative at a participating approved organisation. This is referred to as a "shop front".

When registering via a shop front, the user must provide formal proof of identity.

Registration at a shop front will not associate the PCEHR with a consumer portal account. If access via a consumer portal is required the individual must associate a portal account with their PCEHR (see Registration via a Consumer Portal on page 27).

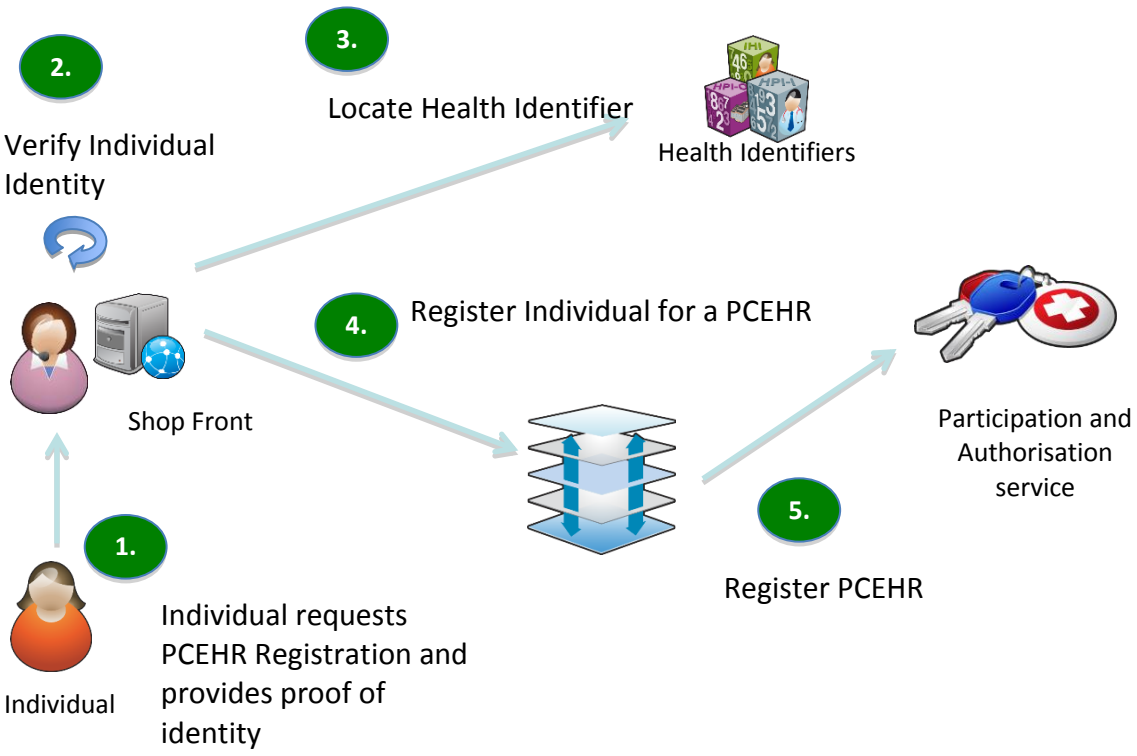


Figure 18: Assisted registration

The process for registering for a PCEHR via a shop front is as follows:

- The individual requests registration at an approved shop front and provides proof of identity.
- The individual's identity is verified
- The individual's IHI number is identified and verified.
- If the verification is successful the shop front system contacts the PCEHR System and creates a PCEHR for the Individual.

2.2.4.7 Individual Retrieves a Consolidated View

An individual or representative may view their Consolidated View via the Consumer Portal. The Individual's Consolidated View will contain the data from all relevant structured documents associated with the PCEHR.

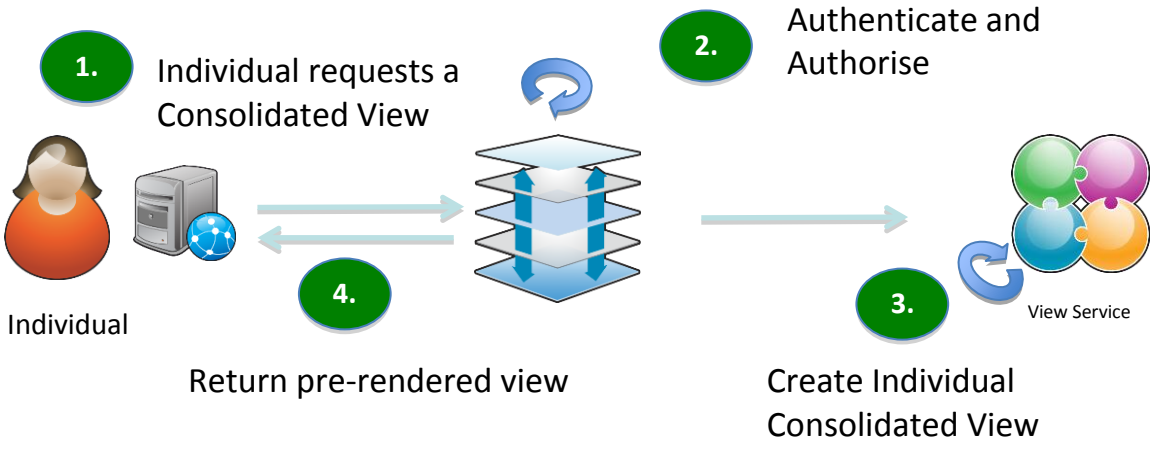


Figure 19: Consumer retrieves a consolidated view

2.3 Conceptual Informational View

The conceptual information view provides a high level view of the key information components used, managed and exchanged by the services described in the computational conceptual viewpoint.

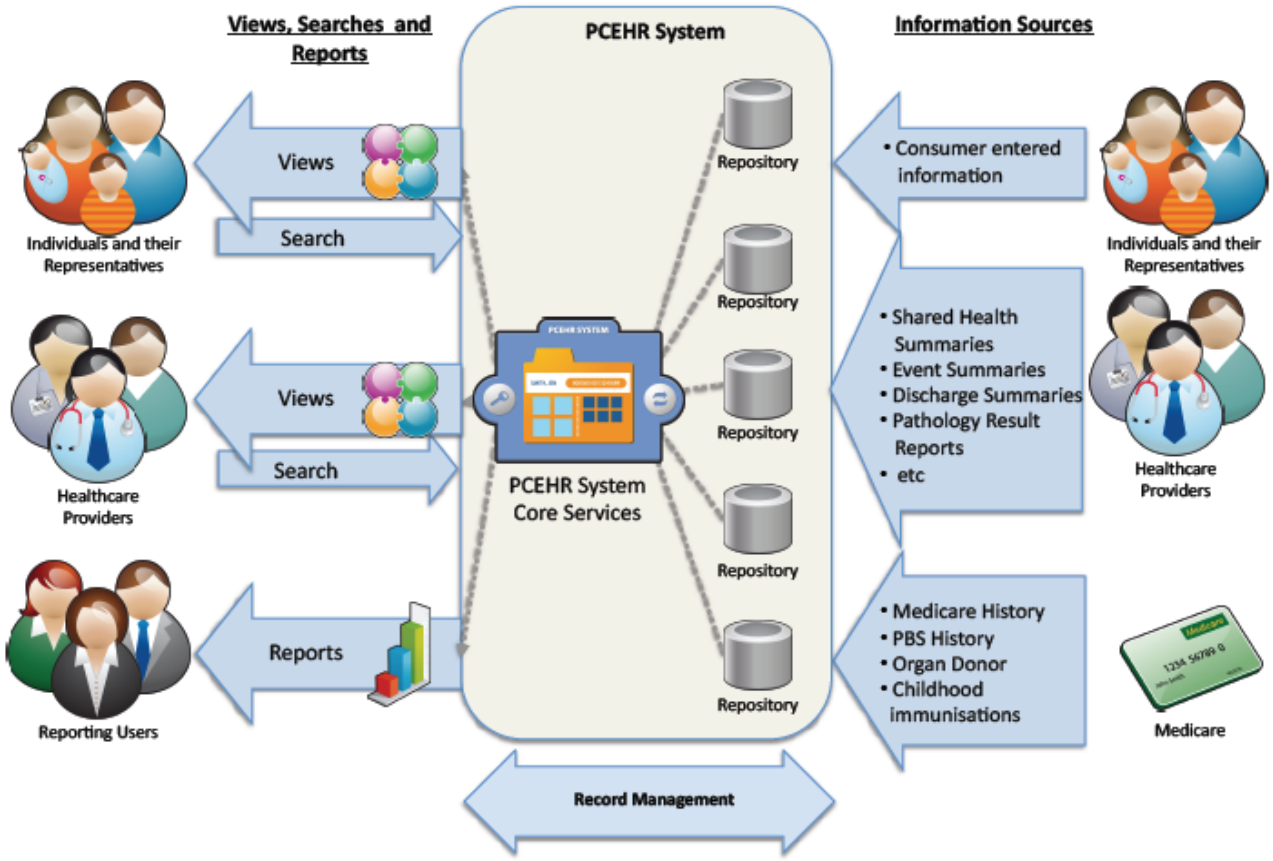


Figure 20: A conceptual view of the information flow

Figure 20 provides a simple view of the flow of information within the PCEHR System highlighting the data produced and consumed by participants. This concept is further elaborated in Figure 21, which provides an overview of the conceptual information view and covers:

- Users systems, including conformant portals, clinical systems and contracted service providers.
- Access channel components, such as the call centre, provider portal, consumer portal, report portal and the B2B gateway.
- Core services, such as the participation and authorization service, index service, view service, audit service and report service.
- The national repositories service and conformant repositories.
- Template service.

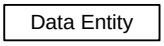
In order to better illustrate the responsibilities of the PCEHR System, the conceptual information view also elaborates the kind of information held by the HI Service, NASH, national healthcare provider service directory and the National Clinical Terminology and Information Service.

2.3.1 Conceptual Information Entities

Figure 21 provides an overview of the key conceptual informational entities, and associated relationships, within the PCEHR System. (An A3 version of this diagram is available in Appendix C at the end of this document.) Some simplifications have been made to help convey ideas and this model is not intended to represent a formal information model. Note that, in order to make the diagram less crowded by having numerous additional associations, some common information components have been repeated in multiple places (boxes with double lines indicate a repeated information component).

While purposely non-formal, the diagram is loosely based on UML class diagram notation.

Some key notation points are given below.



Items within rectangular boxes are data entities.

An orange coloured entity indicates a service.

Inheritance: The entity at source of the line (A) inherits properties from the entity at the target end of the line (B). If Item B contains an attribute item A also contains this attribute. In technical terms this is referred to as sub-typing or specialisation.

Association: The entity at source of the line (A) is associated with the entity at the target end of the line (B). Within Figure 21 the nature and type of association is not specified.

Dependency: The entity at source of the line (A) is dependent upon the entity at the target end of the line (B). This a specialised form of association.

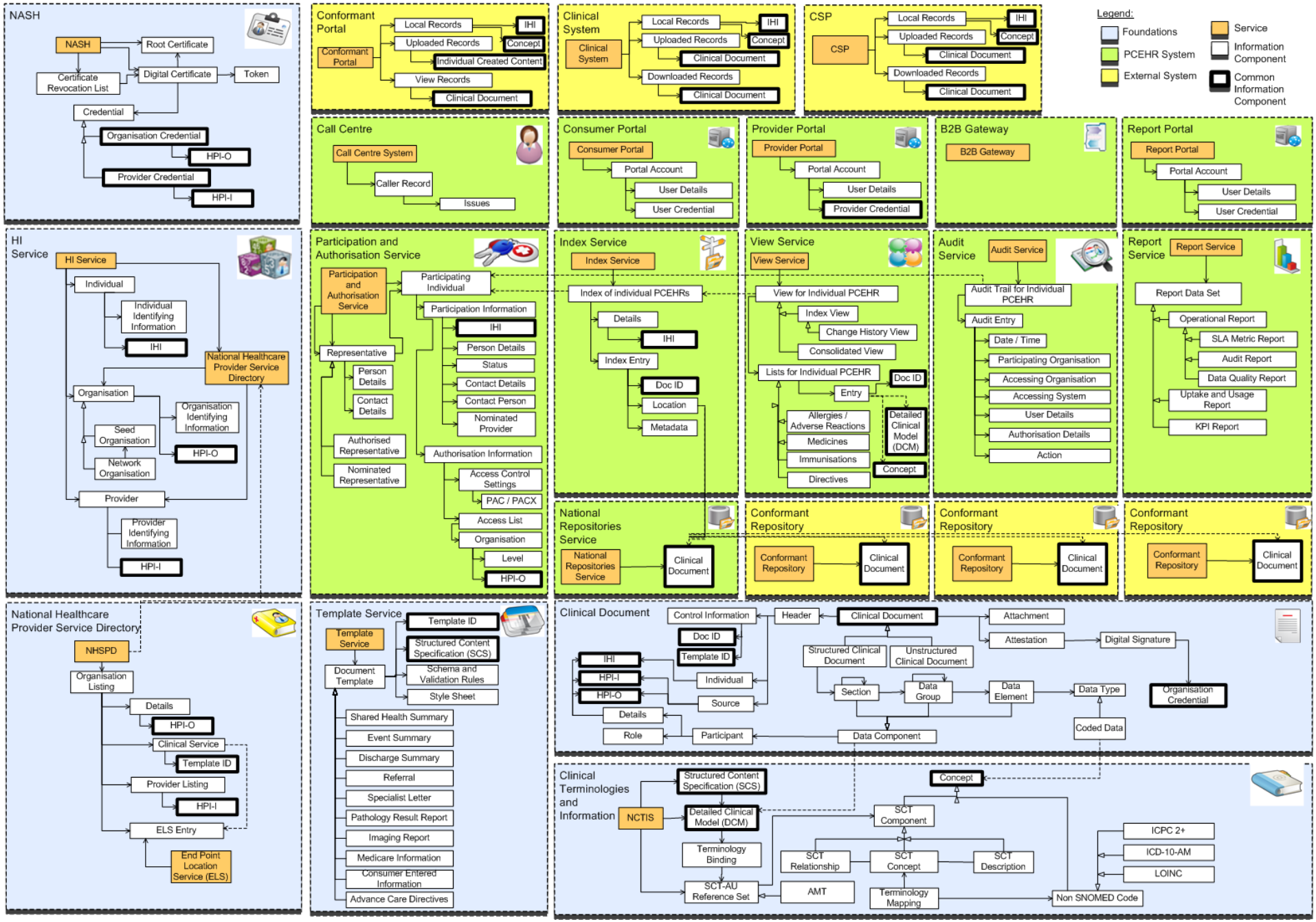


Figure 21: Conceptual information entities

2.3.2 Clinical Documents

Each PCEHR is basically a collection of clinical documents for an individual from a number of different sources. As the concept of a clinical document is used throughout the architecture, this section explains the underlying information structure of clinical documents.

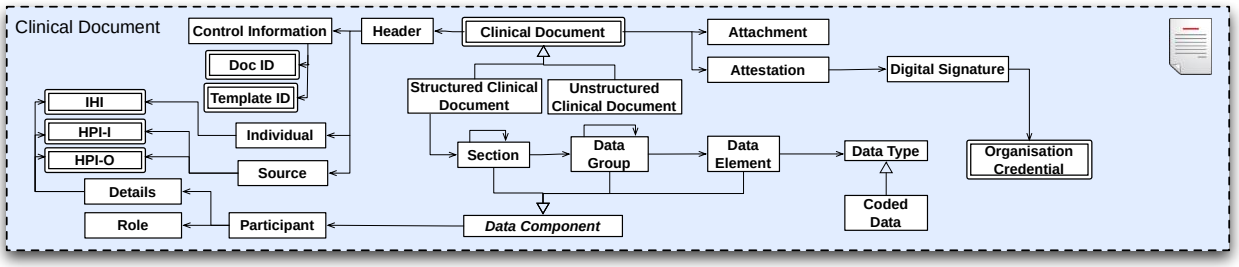


Figure 22: Clinical document

A *clinical document* is used to document information about one or more healthcare events. Clinical documents may either be:

- A structured document, which contains a mix of atomized fielded data and unstructured data.
- An unstructured clinical document, which contains unstructured data.

Every clinical document, including both structured and unstructured documents, has a common header. This header includes:

- Document control information, including:
  - A globally unique document identifier
  - A version number
  - A relationship to previous versions of the document
  - Document type information (e.g. Discharge Summary, Event Summary, etc.)
  - A reference to document template
  - A structured/unstructured clinical document flag
  - The date/time the document was attested
- The individual's details, which may include:
  - Name and title
  - IHI
  - Date of birth
  - Gender
  - Addresses
  - Communication details
  - Indigenous status
- The document *source*, including:
  - The name of the author
  - The author's HPI-I
  - The author's healthcare role
  - The submitting organisation details
  - The submitting organisation's HPI-O

- The submitting organisation role (e.g. general practice, hospital, etc.)
- The submitting organisation address and communication details.

Clinical documents may have an attachment, such as another clinical document.

Every clinical document must have clear provenance and be attested by the source of the information digitally signing the clinical document using the source's organisation credential.

Structured clinical documents may also contain a range of document *sections*, and each section may contain one or more sections or data groups. A *data group* is a cluster of related *data elements* and is used to explain a single concept, such as an observation, evaluation or instruction. Data groups also may include one or more other *participants* that are not already identified in the document header information. Data groups are related to their parent definition or detailed clinical model, defined in the NCTIS. Each data element also has a data type and some elements may have coded data, using codes drawn from the NCTIS or other terminology.

2.3.3 Foundations

The following sections outline the key informational pieces associated with the national foundation services. This section is not intended to describe the computational process associated with using this information.

2.3.3.1 HI Service

The HI Service manages information about individuals, providers and organisations. Individuals, providers and organisations are respectively identified by an IHI, HPI-I and HPI-O and have a record of identifying information (e.g. name, date of birth, address, etc.).

Organisations can be a seed organisation (the legal entity) and may have a number of network organisations representing locations and functional areas within the organisation. Both providers and organisations have the option of publishing a subset of their information within the Health Identifier Service Provider Directory (HISPD).

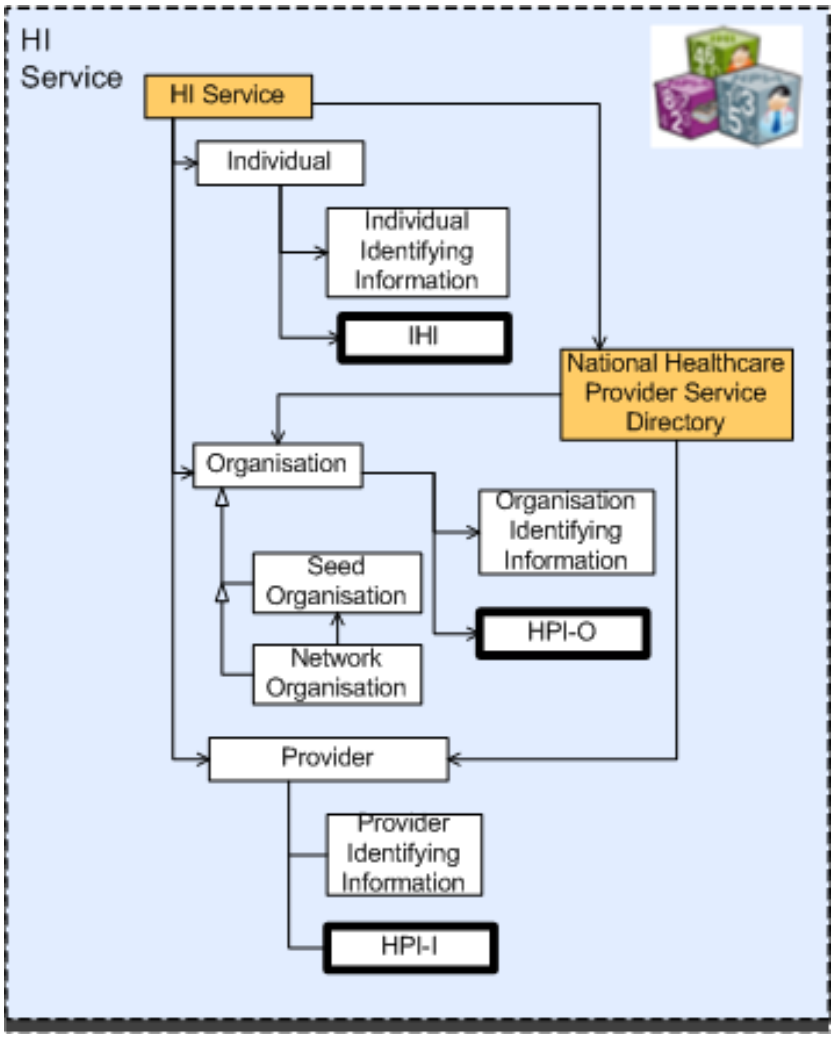


Figure 23: Information held by the HI Service

The Healthcare Identifier Service provides the mechanism for managing national identifiers associated with individuals, healthcare organisations and healthcare individuals.

The Individual Healthcare Identifier (IHI) provides the key mechanism for uniquely referencing a specific individual and, where a PCEHR exists, there will be a one-to-one map between the IHI and a PCEHR.

Healthcare providers interact with the PCEHR System at the organisation level. The HPI-O (Healthcare Provider Identifier for Organisations) is the key item used to control, audit and view provider access. An HPI-I may be linked to more than one HPI-O and the HI Service is the master source for the linkage between HPI-Is and HPI-Os.

2.3.3.2 NASH

The NASH is responsible for issuing a series of digital *credentials* and their corresponding *digital certificates,* which can be used to authenticate individual and organisation providers. These certificates can be made available as either a soft certificate or using a *token* such as a smart card.

The digital credential can either be a provider credential containing an HPI-I, or an organisation credential containing an HPI-O.

Each digital certificate is signed by a trusted *root certificate.* A digital certificate may also be revoked, in which case it will be added to the NASH Certificate Revocation List *(CRL)*.

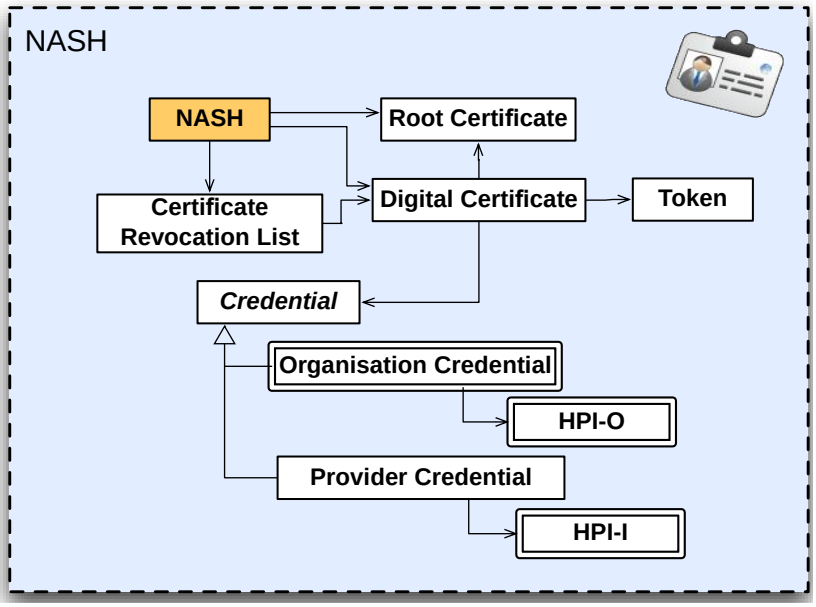


Figure 24: Information held by NASH

The PCEHR System only allows provider access to be controlled at the organisation level, therefore the identity credential submitted to the PCEHR System must be that of the organisation that the healthcare provider represents.

If the healthcare provider only possesses credentials relating to their HPI-I, a CIS or Conformant Portal must provide the mechanism for the healthcare provider to view the organisations they are related with within the HI Service and select the organisation they are working on behalf of. The credentials relating to the selected organisation must then be used for authentication and authorisation within the PCEHR System. Healthcare providers must not be able to select HPI-Os that their HPI-I is not explicitly related to within the HI Service.

NASH provides the master source for all HPI-O and HPI-I certificate data (and any associated certificate revocations).

NASH does not provide a mechanism for authenticating an individual's assertion of an IHI-based identity.

2.3.3.3 National Healthcare Service Provider Directory

The National Healthcare Service Provider Directory (NHSPD) provides "Yellow Pages" style directory and endpoint location services for healthcare organisations. For each organisation that opts to be listed on the directory, the *organisation* listing includes the details of the organisation, its HPI-O, a list of clinical services offered by the organisation and a list of providers available at the organisation to be referred to. Each clinical service supplied by the organisation has a list of templates supported by the organisation and also a link to an end point location, where secure messages should be sent.

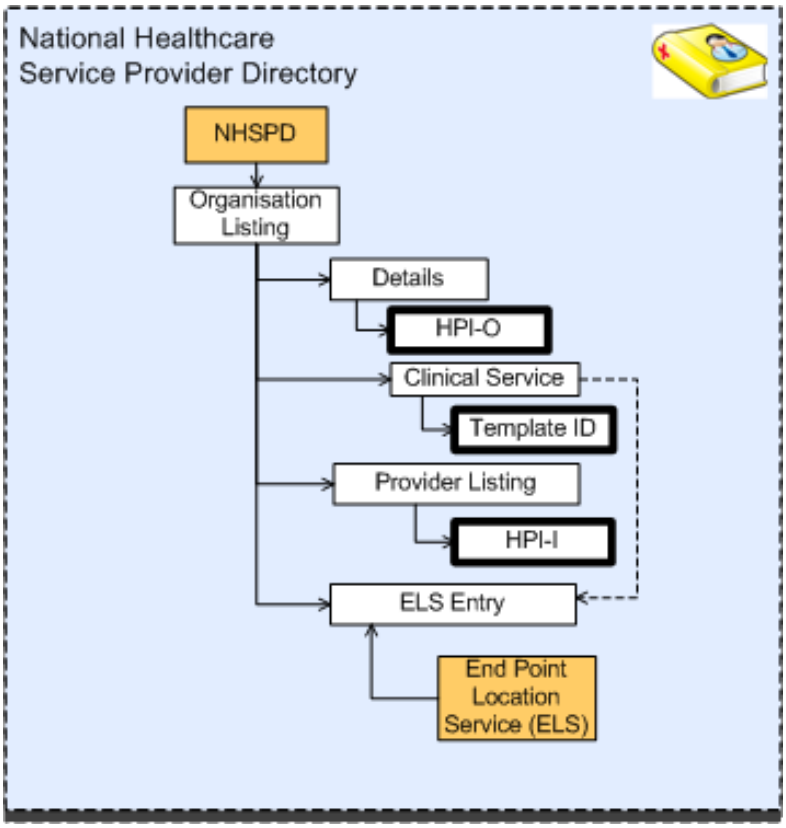


Figure 25: Information held by the NHSPD

The PCEHR System is not dependent on the presence of an NHSPD system or the data associated with this system.

In future, the NHSPD system may be used to allow consumers to look up provider organisations. This may then support such processes as allowing the consumer to directly add providers to the include or exclude lists via the Consumer Portal.

2.3.3.4 National Clinical Terminology and Information Service

The National Clinical Terminology and Information Service (NCTIS) is used to manage a series of structured content specifications (SCS), detailed clinical models (DCM) and SCT-AU Reference Sets. The NCTIS focuses on defining the semantics of clinical documents. It is partnered by the Template Service which provides a series of implementable syntactic specifications for interoperability.

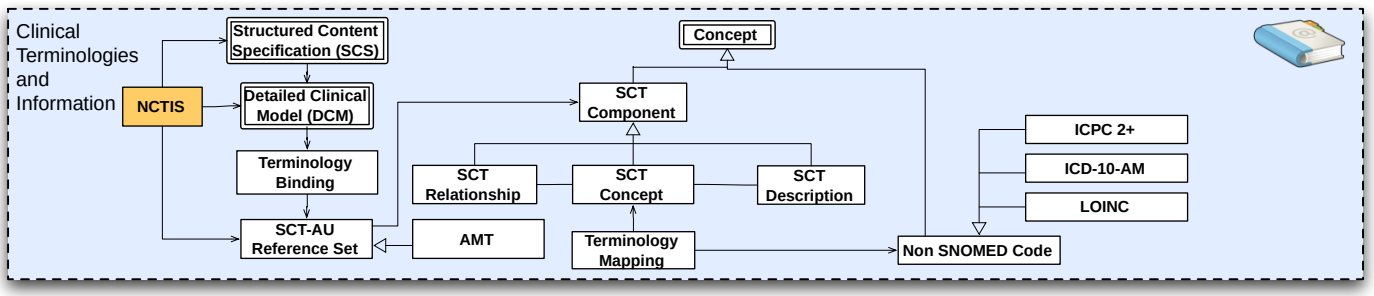


Figure 26: Information held by the NCTIS

An SCS is used to provide a logical definition for a clinical document. It is defined in terms of a series of usage guide and constraints on one or more DCMs.

A DCM provides a logical definition of a data group and is intended to be reused across a number of SCSs. Each DCM also has a binding to a range of SCT-AU reference sets. The binding defines which codes are acceptable in what fields.

Clinical terminologies are defined through use of concepts from SNOMED-CT (SCT) or other terminologies.

SCT Components of SNOMED-CT include concepts, their descriptions and relationships. A SCT description can either be a fully specified term, a synonym or a preferred term. A series of SCT-AU reference sets will be developed for use in the Australian context and will define the approach SCT components. One major reference set is the Australian Medicines Terminology (AMT).

SCT components will be mapped to other terminologies in use such as ICD-10 AM, ICPC 2+, LOINC, etc.

The NCTIS operates mainly as a publication-based service. Systems which make use of clinical terminologies, such as clinical systems or the view service, will need to be able to maintain their own local copy of the clinical terminology.

2.3.3.5 Template Service

The NCTIS provides the basic semantic definitions for a number of the clinical documents and their underlying clinical models and terminologies.

The Template Service is intended to provide a range of implementable syntactic definitions for the major types or classes of clinical documents, including shared health summaries, event summaries, discharge summaries, etc.

For each clinical document type or class, a template has a common template ID, a link to the SCS, an XML schema and related Validation Rules (such as schematron assertions) and style sheets for rendering a clinical document.

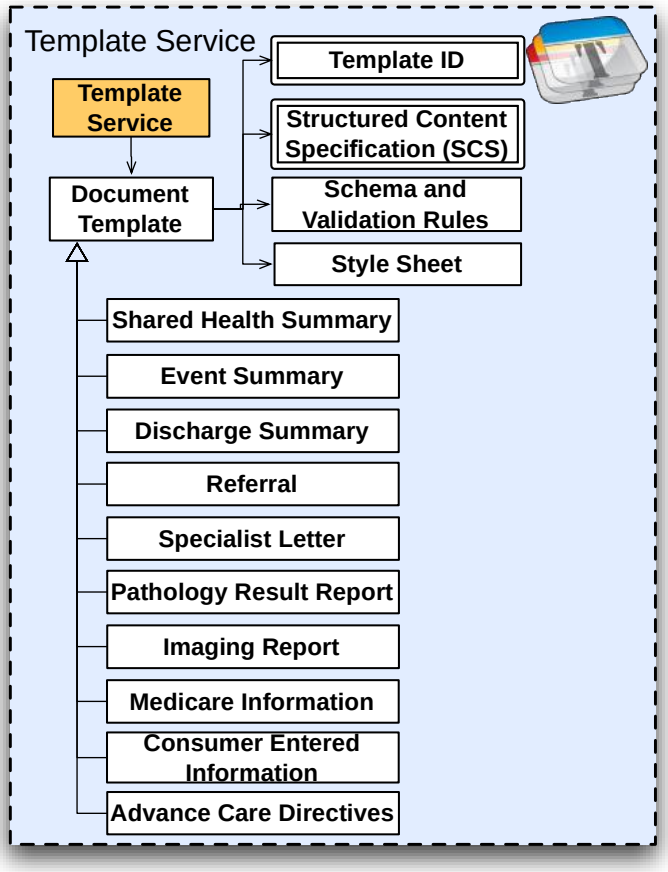


Figure 27: Information held by the Template Service

2.3.4 User Systems

As indicated in the conceptual computational architecture, there are a range of user systems, including conformant portals, clinical systems and contracted service providers.

User systems must attach an IHI to each of clinical documents added to the PCEHR. The user system will manage the master version of any clinical document *uploaded* to the PCEHR and copies *downloaded* from the PCEHR. If the system is to supply structured clinical documents, it must also support the SCT-AU and AMT concepts and reference sets.

How downloaded copies of clinical documents are incorporated into local records (e.g. update of current medication lists from a downloaded clinical document), or when a new clinical document should be uploaded into the PCEHR System based on changes in local records, is defined by the supplier of that system in accordance with the relevant standards set out by NEHTA. Conformance to these standards will be subject to CCA conformance testing.

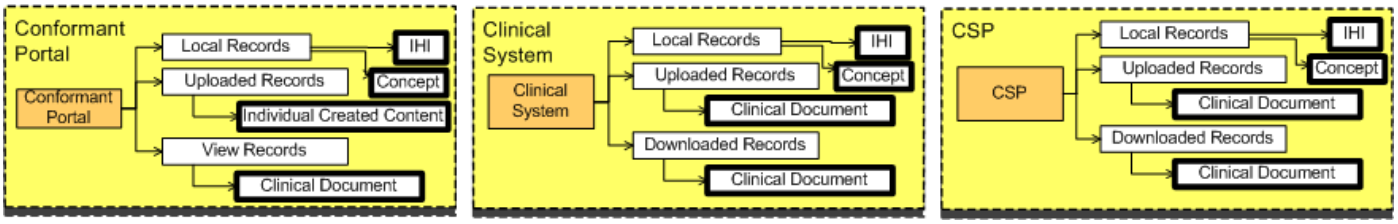


Figure 28: Information held by user systems

Consumers may use a conformant portal to add individual created content and to view clinical documents. It should be noted that, due to the nature of most web browsers, in practice there may be little difference between viewing and downloading a document.

A Conformant Portal represents a portal proven to be conformant to the specification for a *Consumer* Portal. The national Consumer Portal is therefore an instance of a Conformant Portal. The detailed specification of the requirements for conformance are deferred to the Conformant Portal Solution Design. The provider portal is not related to a conformant portal.

2.3.5 Access Channels

The PCEHR System provides a range of access channels, including a Call Centre, Consumer Portal, Provider Portal, B2B Gateway and Report Portal. From an information viewpoint, the access channel components focus mainly on managing user information and the core services manage the information within a PCEHR.

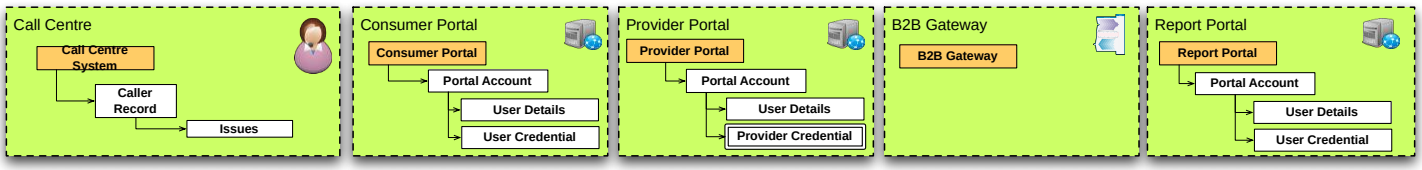


Figure 29: Information held in the access channels

The Call Centre is used to handle PCEHR related administrative queries from individuals and providers. The PCEHR Call Centre is a separate entity from any call centres which may be associated with conformant portals. The Call Centre is deemed to be outside of the scope of this document and as such the related informational entities are not covered further here.

The Consumer Portal manages portal accounts, for individuals and their representatives. For each of these users, the portal must maintain the user's details (such as name, contact details, etc.) and their portal user credentials. The Consumer Portal must also securely store the STS provided token which links a portal account to an IHI (and therefore a PCEHR).

Where an individual has been nominated or authorised to manage another individual's PCEHR account, a single Consumer Portal account may be used to manage multiple PCEHRs.

The Provider Portal manages portal accounts for healthcare providers. For each of these users, it maintains their details (name, contact details) and their respective NASH provider HPI-I specific credential. The HI Service provides the mechanism to map the HPI-I onto a HPI-O.

The B2B Gateway does not maintain any information.

The Report Portal manages a series of portal accounts for reporting users. For each of these users, it maintains their details (name, contact details) and their user credentials (password and secret questions).

2.3.6 PCEHR Core Infrastructure Services

2.3.6.1 Participation and Authorisation Service

The Participation and Authorisation Service manages the participation process for individuals and their representatives and supports the capture of their access control settings.

For each participating individual, the Participation and Authorisation Service will record the following information.

- *Participation information*, such as:
  - IHI
  - Details (name, date of birth and sex).
  - PCEHR status (active, de-activated).
  - Contact details (phone number, mailing address, email address).
  - Date(s) of sign up and exit.
  - Emergency contact details (name and contact details).
  - A nominated provider (name, contact details and HPI-I / HPI-O).
- *Authorisation information*, including:
  - *Access control settings*, including:
    - Can the PCEHR be found via an IHI Search on the PCEHR System (Y/N)?
    - Is a PAC required to be added to the include list (Y/N)?
    - The *PAC* and or *PACX* (PIN/passphrase)
    - Can access without a PAC be undertaken if individual forgets PAC (Y/N)?
    - Is notification required when access without PAC undertaken (Y/N)?
    - Is notification required when new organisations are added to the include list (Y/N)?
  - Document Access Control settings (this may be either General, Limited or No Access).
- Notification details (email address or other form)

- An access list, listing organisations and their HPI-O and the level of access (i.e. included with access to 'general access', included with access to 'general access' and 'limited access' or excluded)

The participation and authorisation service also captures information about a *representative*, their *details* (name, date of birth, sex), their *contact details* and their *relationship* with an individual (authorised or nominated).

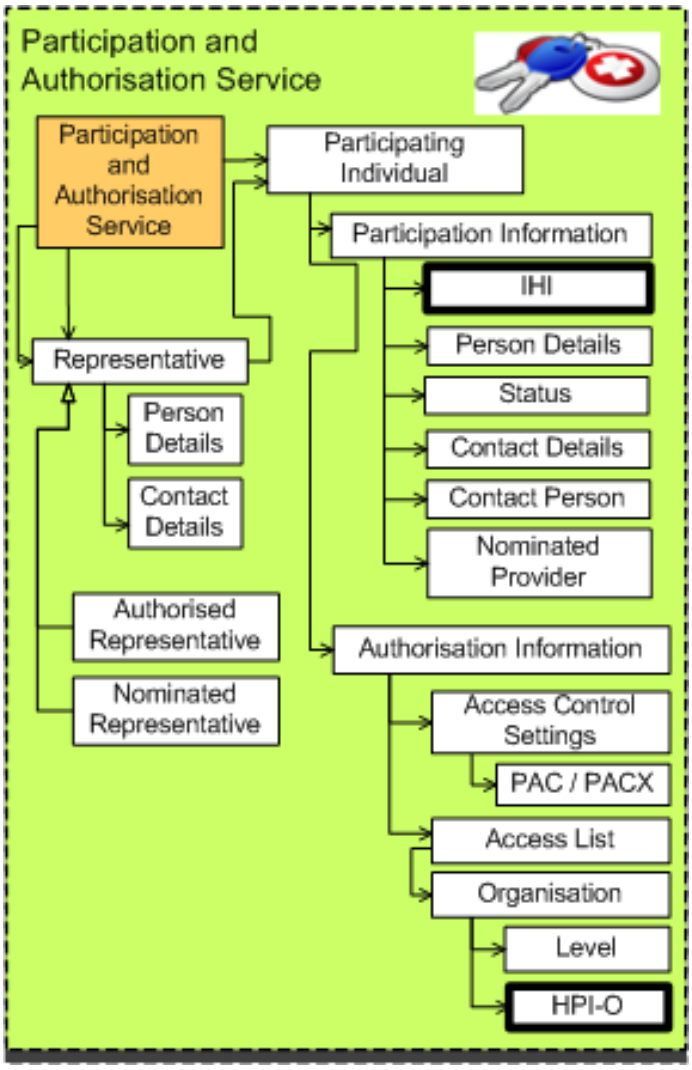


Figure 30: Information held by the Participation and Authorisation Service

2.3.6.2 Index Service

The index stores metadata (i.e. data that serves to provide contextual information about other data) about each clinical document; the actual content of the records is stored within the PCEHR-conformant repository.

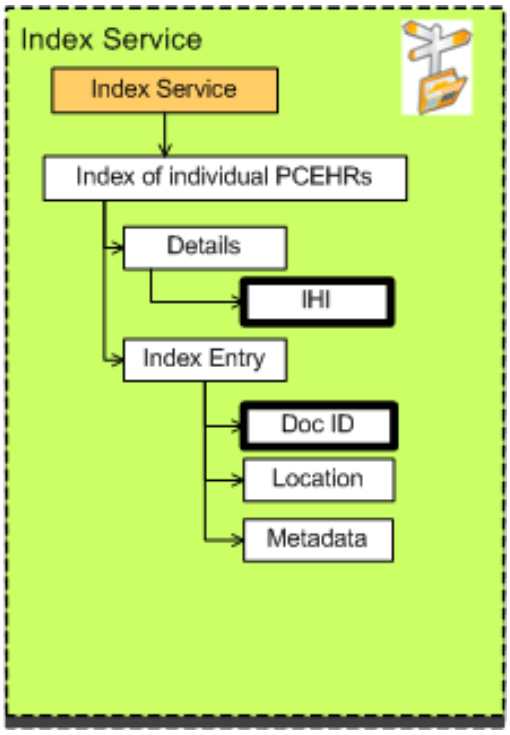


Figure 31: Information held by the Index Service

For each registered clinical document, the index service stores:

- The individual's details, including the individual's IHI, name, sex and date of birth.
- An entry for each clinical document, including:
  - The clinical document ID (an OID unique identifying the clinical document).
  - A reference to the document (repository specific identifier). This may include the address of the repository containing the document and the repository's document identifier.
  - Other metadata, including:
    - The template ID (an OID identifying the template).
    - The type of clinical document (e.g. Discharge Summary, Event Summary).
    - A keyword list for search function.
    - The date and time at which when the clinical document was created.
    - The name, role and HPI-I of the healthcare provider that created the Clinical document.
    - The name and HPI-O of the healthcare organisation where the clinical document was created.
    - The name and HPI-O of the participating healthcare organisation that created the record.
  - Versioning information about the clinical document.

- Management information about the integrity of the document reference (e.g. last time the reference was checked, flag to indicate potential duplicate, etc.).
- A label indicating if the information is 'general access', 'limited access' or 'no access'.
- A flag indicating the clinical document had to be 'effectively removed' because it was posted into the wrong PCEHR. A document which has been "effectively removed' is logically no longer linked to the PCEHR and is not visible to the Individual.

2.3.6.3 View Service

The purpose of the View Service is to allow authorised users, individuals and their representatives to access a series of 'views' of an individual's PCEHR.

The view service supports a range of views of an individual's PCEHR, including:

- Index view, which lists the clinical document available in an individual's PCEHR
- Change history view, which is similar to the index view, except it allows users to quickly find any clinical documents that may have been amended.
- The consolidated view, which allows individuals to see a summary of an individual's PCEHR

The views are built out of a number of reusable component lists. A list assembles a common subset of data from multiple clinical documents. Examples include a list of an individual's allergies and adverse reactions assembled from an individual's shared health summary, discharge summaries, event summaries, etc. In order to ensure that users of a list within a view can trace back to the clinical document where it was sourced, each entry in the list will be linked to the document identifier for the clinical document. Also to ensure consistency, entries within lists will be based in a common detailed clinical model (DCM). The DCM in turn is bound to a common terminology in order to ensure that elements of the list are comparable and can be sorted or grouped.

The view service may need to maintain a local copy of SCT-AU and AMT to support list construction.

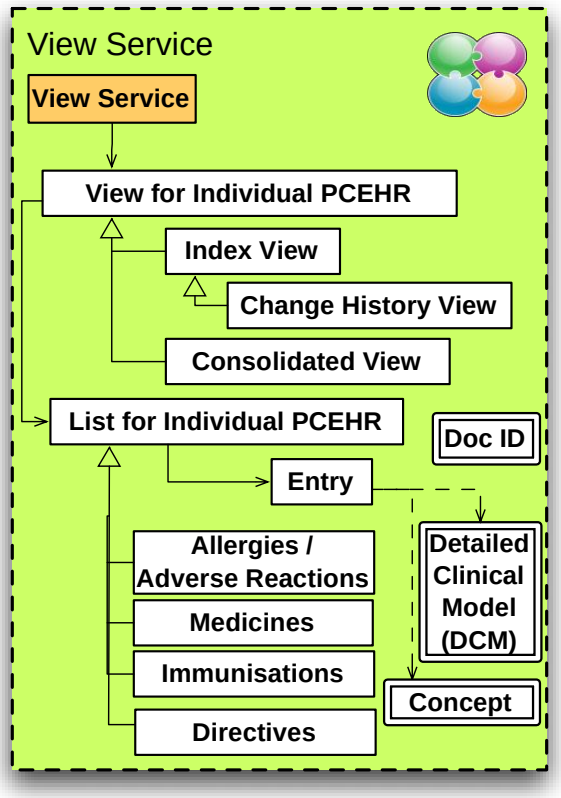


Figure 32: Information held by View Service

2.3.6.4 Audit Service

The PCEHR System will provide an Audit Service to record all activity on the PCEHR System and PCEHR-conformant repositories.

For each individual, the audit service will maintain an audit trail consisting of a number of audit entries. A separate audit entry must be logged for each key action. Definition of the complete set of auditable actions is deferred to the detailed design of the audit service. Each audit entry contains:

- The date and time that access was obtained (UTC Time).
- The name and identifier of the participating organisation (in small organisations this will typically be the seed HPI-O and for larger organisations this may be some other nominated network HPI-O). This field is not required for representatives.
- The name and identifier of the accessing organisation (used when the accessing organisation has a network HPI-O below that of the participating organisation). This field is not required for representatives.
- The name and identifier of the CSP or CPP (this field is only required if the system is accessed via a CPP or CSP).
- Information identifying the user who obtained access.
- The role of the user who obtained access.
- Whether the PCEHR was accessed using the individual's provider access code (PAC), a transferrable access key (TAK), by override (emergency or forgotten PAC) obtained by the healthcare provider, representative using the consumer portal, etc.
- Details of the action performed.

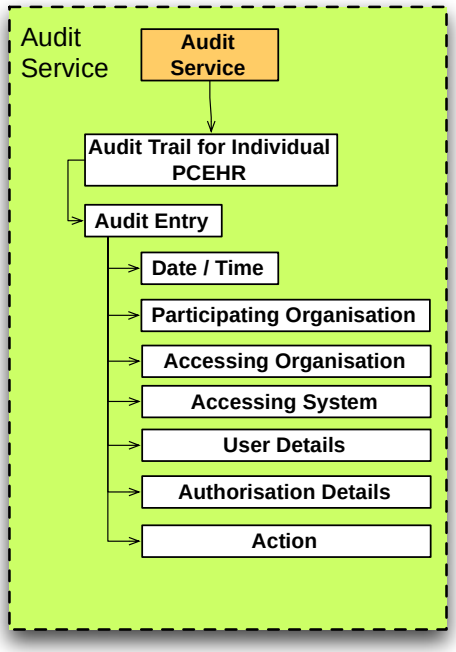


Figure 33: Information held by Audit Service

2.3.6.5 Report Service

The purpose of this service is to support operational reporting, to help evaluate take-up rates and to track progress around key performance indicators. In time, the reporting service may be extended to support additional approved uses.

The report service will deliver a range of reports, including:

- Operational reporting, such as, but not limited to:
  - Reporting against metrics in PCEHR System infrastructure service level agreements and conformant repository service level agreements (e.g. uptime, incident reports, incident resolution times, call centre reporting, etc.)
  - Audit reports
  - Data quality 'dashboard'
- PCEHR System uptake and usage reporting, including access to pre-defined reports showing:
  - Numbers of individuals registering, using the PCEHR System and withdrawing
  - Numbers of authorised users and healthcare organisations using the PCEHR System
  - Viewing of clinical documents, views and reports
  - Uploading new clinical documents

  This data will be able to be broken down by:
  - Demographics (age, location, gender)
  - Time (time of day, day of week, month)
  - Healthcare provider role (e.g. GP, specialist, ED doctor)
  - Kind of information accessed or uploaded (view name or clinical document types).
- Reports related to outcomes realisation related key performance indicators.

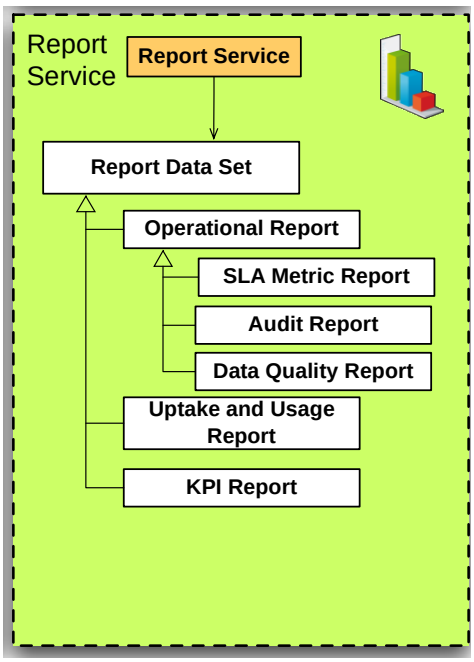


Figure 34: Information held by the Report Service

2.3.7 Repositories

The PCEHR System supports a national repositories service and the capability to connect to a range of conformant repositories.

The PCEHR System treats these repositories as clinical document stores. The assembly of information from those clinical documents are handled by the other core services.

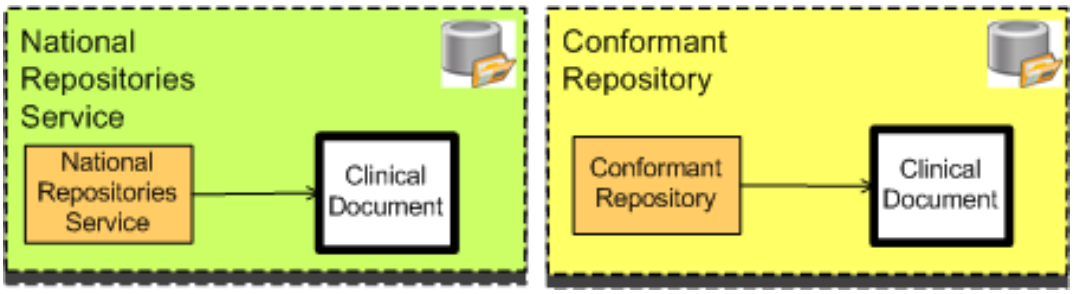


Figure 35: information held by repositories

3 Logical View of the System

The system logical view provides a more in-depth description of the system. It further decomposes the system to highlight functional areas and specifies key internal components. The focus on this section is to provide sufficient constraint to ensure that the solution is fit for purpose, while allowing the flexibility required to map to multiple tendered solutions.

The logical view is technical in nature and assumes a basic knowledge of modelling notations and fundamental solution design concepts such as service orientation, layering, service contract, APIs and interfaces.

Version 2.0 of the Universal Modelling Language (UML) is used extensively throughout this viewpoint.

3.1 Logical Computational Viewpoint

The computational viewpoint is concerned with describing the functional decomposition of the system into computational objects which interact at their interfaces.

The logical computational viewpoint provides a logical perspective of the solution and is inherently technical in nature. The focus is on detailed system interfaces, external dependencies and operational behaviour. Where relevant, the PCEHR System may be decomposed into sub-components and the interaction with the components will be identified. It is intended that this specification remain platform and technology agnostic and that a further process will be performed to bind the patterns and components identified onto one or more technology stacks.

3.1.1 The National PCEHR System as a conformant repository

In essence, the PCEHR System is itself a repository. It is made up of document data stores, a user index, access controls, rendering constructs and supporting operations (such as reporting and auditing). The PCEHR System also contains repositories (both national repositories and external conformant repositories).

Conformant repositories will be used as data stores by the PCEHR System and need not necessarily provide the full set of functions required by a document repository.

This document outlines a specification for a document repository. This specification provides the basis of the PCEHR System and may also be used as the basis for third party conformant repository implementations. However when a repository is conformant to all three levels of the specification, it allows the repository to be access and managed in a consistent way.

The PCEHR System does not require that all conformant repositories offer the full set of PCEHR repository services and conformance is therefore broken down into three levels.

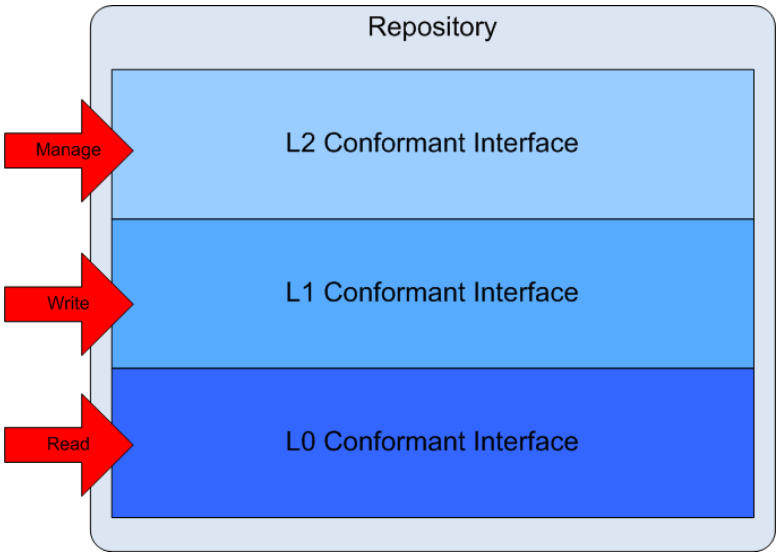


Figure 36: Levels of repository conformance

Level 0

This is the most basic level of conformance and provides all of the operations required to read (or access) documents within a repository. This is likely to form the basis of conformance for most repositories. A L0 conformant repository is effectively a read-only data store (although the repository may be written to by other means).

- An L0 conformant repository matches the pre-defined set of retrieval operations outlined within this specification.
- An L0 repository must also meet pre-defined security, privacy and availability requirements.
- This is the minimum level of conformance required for a repository to join the PCEHR repository network.
- It is expected that most conformant repositories will be L0 compliant.

Level 1

This level of conformance provides all of the operations required to read (or access) and write (store) documents within the scope of a repository. An L1 conformant repository is effectively a read and write capable data store (although again the repository may also be written to by other means).

- An L1 conformant repository meets the L0 conformance requirements and additionally offers a set of storage interfaces.
- The National Repositories is an L1 conformant repository.

Level 2

Level 2 compliance provides all of the interfaces required to read, write and manage the repository. A L2 repository represents a fully capable standalone repository with consistent interfaces for reading and writing data and administering the system.

- An L2 conformant repository meets the L1 conformance requirements and additionally offers a set of privacy and registration management interfaces.
- An L2 repository may be managed by appropriately trusted systems and portals.
- The PCEHR System is an L2 conformant repository.
- Standardising the management interface allows common tools to easily manage multiple repositories.

The intention behind this classification is to allow other repositories to be built using the same set of interfaces and behaviours. This consistency will allow common tools to manage multiple repositories and for repositories to optionally to act as slaves of one or more master repositories.

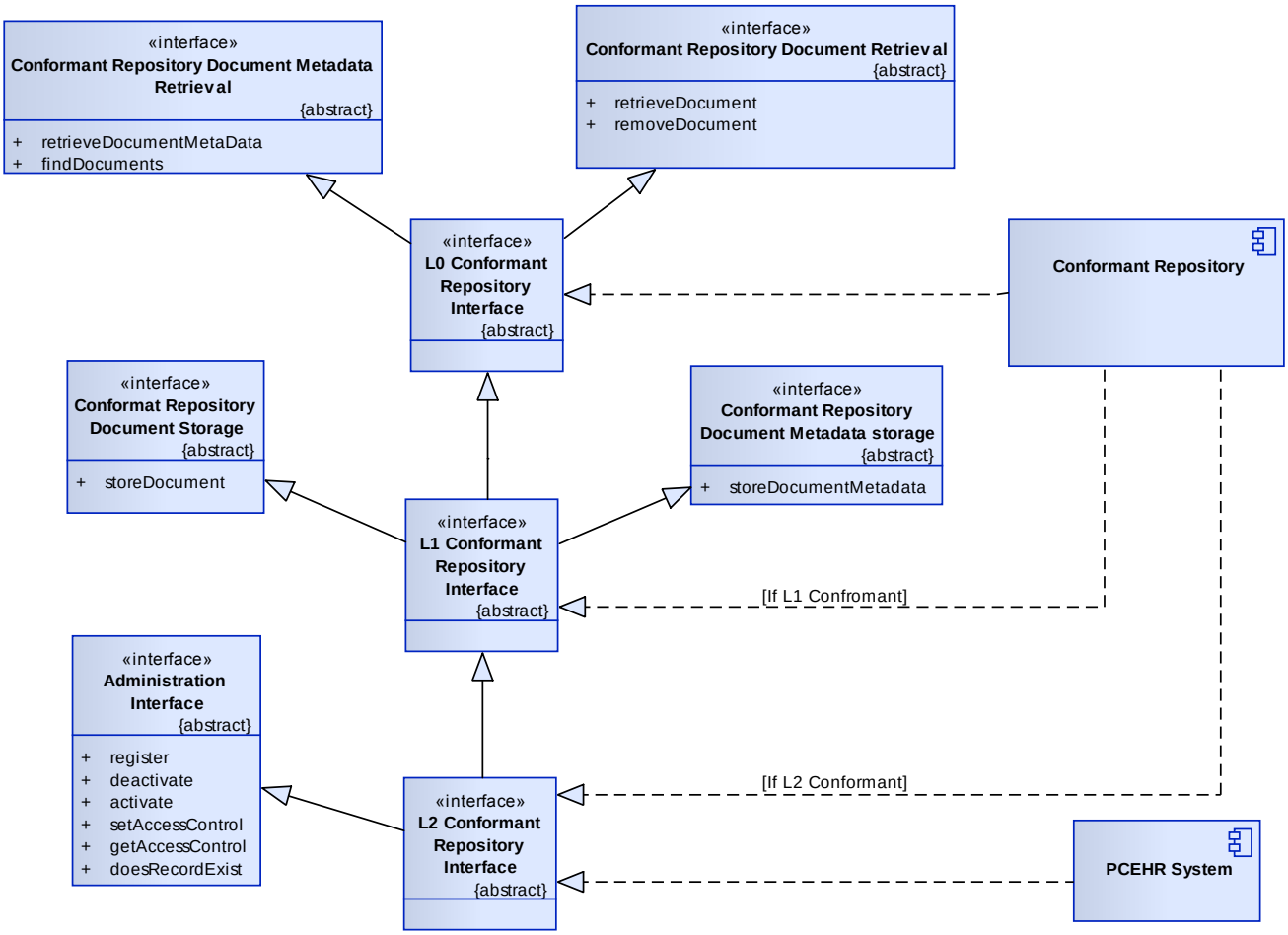


Figure 37: PCEHR interface relationships

3.1.2 System Composition

The below diagram outlines the key logical components within the system and the relationships between these components. Table 2 on page 52, provides a mapping between the components specified and the Concept of Operations [PCEHR_CON_OPS]. It is expected that the supplier implementation architecture will undertake a further separation of concerns process and break the solution into technical objects to aid functional re-use, support and extension.

3.1.2.1 System Component Diagram

A diagram showing the logical decomposition of the diagram is shown on the following page. An A3 version of this diagram is available in Appendix C at the end of this document. Each layer is shown individually across the following sections.

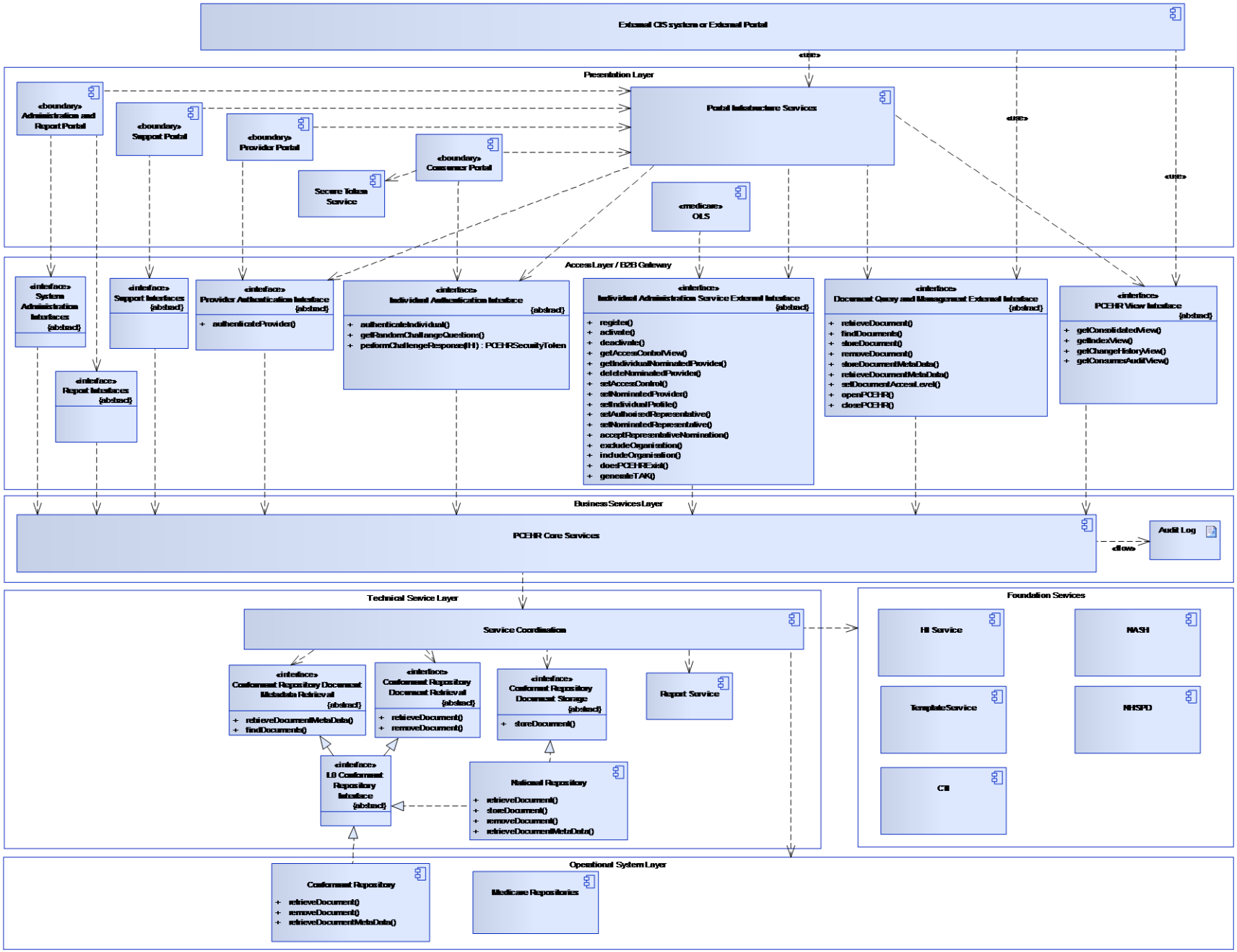


Figure 38: PCEHR System - Layers and components

Table 1: PCEHR logical system components

Component	Description
Provider Portal	A web browser based user interface used to centrally display and manage healthcare provider (identified by an HPI-I or HPI-O) PCEHR operations.
Consumer Portal	A web browser based user interface used to centrally display and manage consumer (identified by an IHI) PCEHR operations.
Administration and Report Portal	A portal used to administer the system and access reports.
Support Portal	A portal used to help provide operational support to system users. This may be used within Call Centres.
Secure Token Service	This component is responsible for issuing and validating the identity assertions related to an individual's portal account.
Portal Infrastructure Services	A generic framework component which supports the serving of portlets for use in disparate web portals.
OLS	The Medicare Online Services Portal
Individual Administration Interface	The external interface used to expose the functions associated with administrating an Individual's PCEHR.
Document Query and Management Interface	This set of external interfaces outlines the main mechanism used for external systems to access and add PCEHR records.
PCEHR View Interface	The view interface outlines the set of operations required to access views of data contained within a PCEHR. This includes both the three core views defined within Concept of Operations [PCEHR_CON_OPS] and a number of additional items including the users Access Control and privacy setting and recorded audit data.
Individual Authentication Interface	The Individual Authentication Interface provides the mechanism for Individual Consumer Portal Accounts to authenticate against the service.
Provider Authentication Interface	The PCEHR Provider Authentication Interface provides the mechanism for providers to authenticate against the PCEHR System.
Support Interfaces	The set of interfaces used to expose the functions required to provide operational support to users.
Report Interfaces	The exposed set of operations used to access PCEHR System reports.
System Administration Interfaces	The exposed set of operations used to administer the PCEHR System.
PCEHR Core Services	A "black box" containing the set of PCEHR Core services.
Audit Log	A log used to record the audit events associated with a PCEHR.
Service Co-ordination	The service co-ordination is a logical component used to join the disparate services into repeatable processes which may be used within the business services.
Conformant Repository Interface(s)	This represents the set of common interfaces which may be offered by conformant repositories.
Conformant Repository	One or more repositories which have been proven to meet the conformance requirements set out by PCEHR. This may include interfacing, availability, privacy and other conformance criteria.

Component	Description
National Repositories	National instances of a conformant repository.
HI Service	The Australian national Healthcare Identifier service.
NASH	The Australian National Authentication Service for Health
Medicare Databases	The set of Medicare data stores.
CTI	Common Terminology and Information
NHSPD	National Healthcare Service Provider Directory
Template Service	The national Template Service

Table 2: A mapping of logical components to the Con Ops set of components

PCEHR Con Ops Component	Solution Architecture Component
Index Service	Document Query and Management External Interface and PCEHR Core Services
View Service	PCEHR View Interface and PCEHR Core Services
Participation and Authorisation Service	Consumer Authentication Interface, Individual Administration Interface and PCEHR Core Services
Report Service	Report Service
Template Service	Template Service
National Repositories	National Repositories
Conformant Repository	Conformant Repository
Provider Portal	Provider Portal
Consumer Portal	Consumer Portal
Audit Service	Audit Log and PCEHR Core Services.
CTI	Clinical Terminology and Information core components and data.
NHSPD	The National Healthcare Service Provider Directory

3.1.3 Layering and Components

Figure 38 utilises layers to help group and separate system components. It is not intended that these layers map onto physical solution tiers or that these layers be directly realised. The layering is wholly focused on aiding understanding and readability.

The diagram shows a stack of conceptual layers.

3.1.3.1 Access and Presentation Layers

The access and presentation layers provide the components that realise interfaces into the system or external views of system state.

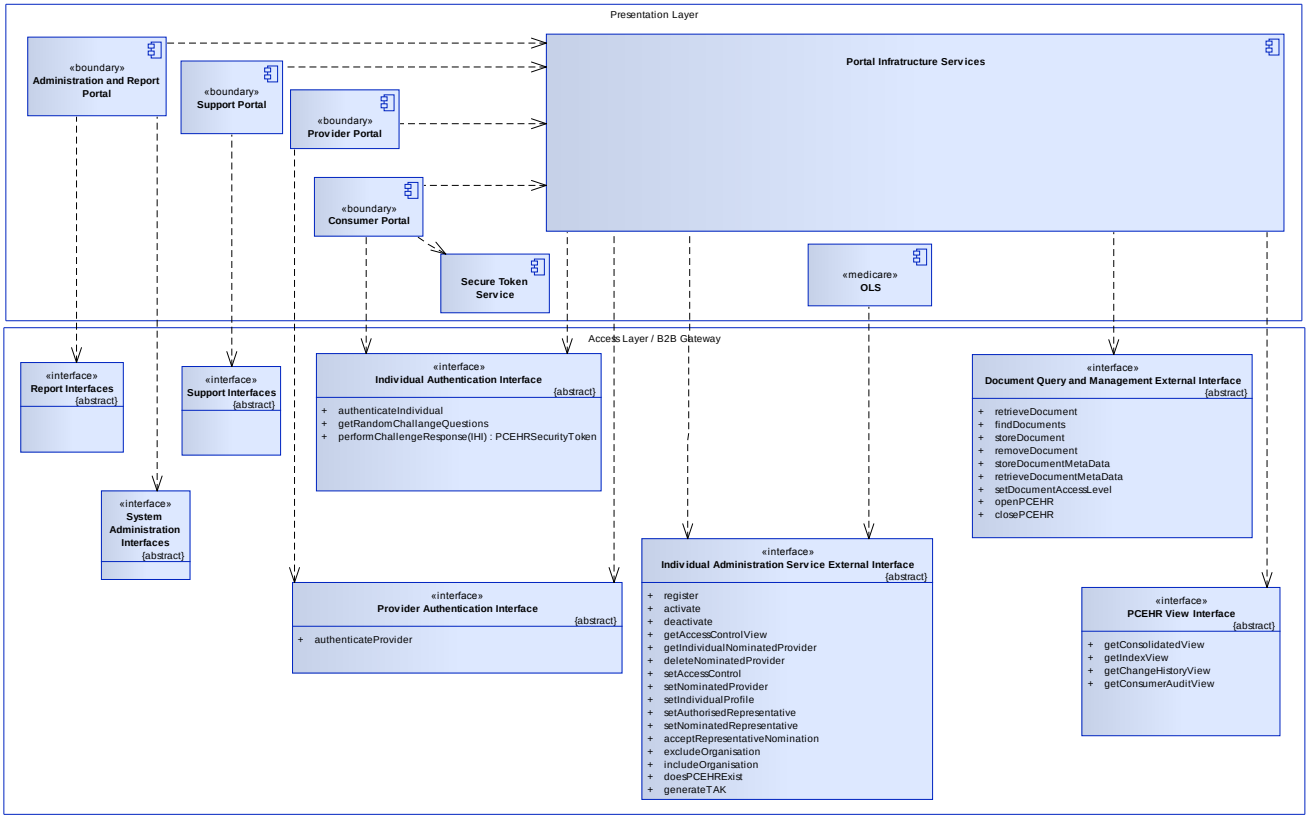


Figure 39: Presentation and access layers

Provider Portal

The provider portal provides a web-based mechanism for a clinical provider to access a PCEHR. This is the core option to be used where the provider is not able or it is not appropriate to access the PCEHR via a CIS system.

Consumer Portal

The consumer portal is a realisation of a conformant portal and allows the individual, or a nominated representative to register for and administer a PCEHR.

This is the primary mechanism provided to allow an individual or authorised representative to manage a PCEHR.

It is intended that this portal be multi-platform enabled and that the underlying interfaces and portlets may be re-used across multiple platforms and devices.

Administration and Report Portal

The PCEHR System will provide an Administration and Report Portal to support access to system administration functions and general operational reporting data.

The report portal requirements include the production of directly viewable reports and the extraction of report data in a format suitable for import into other analysis tools.

Support Portal

The support portal is used by support staff to perform user support activities. This portal maybe used by multiple channels including call centres.

Portal Infrastructure Services

The Portal Infrastructure Services support the provider, consumer portal and report portal (and any future conformant portal) by creating key portlets of common data elements.

Medicare Online Services

The set of Medicare Online Services provides the access required to administer a number of national medical and eHealth services. It is expected that this may also in future allow a user to register for and activate a PCEHR.

However it is not expected that OLS will be used to administer a PCEHR.

Provider Authentication Interface

authenticateProvider

This logical operation allows the PCEHR System to authenticate a system's assertion of identity.

Parameters	Returns	Business Faults
Provider Credential	Security Session Token	Invalid Credentials

Individual Authentication Interface

The consumer authentication interface provides the B2B interface required to allow compliant consumer portals to authenticate with the PCEHR System.

authenticateIndividual

This operation allows the PCEHR System to authenticate an individual's portal representation of an identity assertion. An individual identity token is used to verify the Individual and Consumer portal identity. Upon successful authentication a PCEHR Security Access Token will be returned which has a prescribed Time to Live (TTL).

Parameters	Returns	Business Faults
Individual's HI	Security Session Token	Authentication failure
Identity Token		
Consumer Portal Identifier		

getRandomSecretQuestions

This operation allows the PCEHR System to randomly generate a set of secret questions used as part of a challenge-response mechanism to further verify identity. This process may be used prior to performing restricted operations such as modifying data via the Consumer Portal.

Parameters	Returns	Business Faults
Individual's HI	A set of random Secret Questions	PCEHR not found
Security Session Token		Secret questions are not yet setup.

performChallengeResponse

This operation allows the PCEHR System to perform second level authentication to assert individual identity with sets of secret questions. Upon successful completion, a new Security Session Token will be generated that provides access to restricted operations.

Authentication via the consumer portal performs a strong level of user authentication, however an additional level of authentication will be required when performing key security operations such as nominating a representative, adding a provider to the include list or de-activating a PCEHR.

Parameters	Returns	Business Faults
Individual's HI	Security Session Token	PCEHR not found
Secret Questions		Verification failure
Security Session Token		

Individual Administration Service External Interface

The following section outlines the interfaces exposed to allow conformant consumer portals to perform administrative tasks on the PCEHR. This is the key B2B interface used to support the functionality offered within a conformant consumer portal.

register

This operation allows a registration organisation (e.g. Consumer Portal, Shop Front, etc.) to register an individual for a PCEHR. In order to complete the registration process an individual must set the access level and PCEHR profile. Where a PCEHR already exists the Individual's Identifier of the existing record will be returned.

Parameters	Returns	Business Faults
The IHI of the individual the PCEHR relates to.	None	Individual HI not found
Registration Organisation Identifier		Operation is not authorised
Security Session Token		PCEHR already Exists

activate

This operation allows an authorised organisation or a PCEHR Managing Individual to activate a PCEHR record.

Parameters	Returns	Business Faults
The IHI of the individual the PCEHR relates to.	None	Individual's HI not found
The Managing Individual's Identifier		Operation is not authorised
Authority Organisation Identifier		PCEHR not found
Security Session Token		

deactivate

This operation allows an authorised organisation or a PCEHR Managing Individual to deactivate a PCEHR record.

Parameters	Returns	Business Faults
The IHI of the individual the PCEHR relates to.	None	Individual's HI not found
The Managing Individual's Identifier		Operation is not authorised
Authorised Organisation Identifier		PCEHR not found
Security Session Token		

getAccessControlView

This operation allows a PCEHR Managing Individual to retrieve a representations of the access control settings associated with a PCEHR.

Parameters	Returns	Business Faults
The IHI of the individual the PCEHR relates to.	Access Control list	PCEHR not found
Security Session Token		

getIndividualNominatedProvider

This operation allows an authorised client system to retrieve the details of the Individual's Nominated Provider.

Parameters	Returns	Business Faults
The IHI of the individual the PCEHR relates to.	Nominated Provider	PCEHR not found
		Operation is not authorised
Security Session Token		

deleteNominatedProvider

This operation allows a PCEHR Managing Individual to remove a nominated provider via the consumer portal.

Parameters	Returns	Business Faults
The IHI of the individual the PCEHR relates to.	None	PCEHR not found
Security Session Token		Operation is not authorised

setAccessControl

This operation allows a PCEHR Managing Individual to manage their PCEHR access controls via the consumer portal.

Parameters	Returns	Business Faults
The IHI of the individual the PCEHR relates to.	None	PCEHR not found
Access Control Settings		
Security Session Token		Operation is not authorised

setNominatedProvider

This operation allows a conformant portal or clinical system to set the nominated provider. This operation will override any existing nominated provider entry.

Parameters	Returns	Business Faults
The IHI of the individual the PCEHR relates to.	None	PCEHR not found
Healthcare Provider Identifier - Individual		Nominated Provider does not exist

Parameters	Returns	Business Faults
Healthcare Provider Identifier - Organisation		Operation is not authorised
Security Session Token		

setIndividualProfile

This operation allows an individual to configure their PCEHR profile via the consumer portal.

Parameters	Returns	Business Faults
The IHI of the individual the PCEHR relates to.	None	PCEHR not found
PCEHR Profiles		Operation is not authorised
Secret Questions		
Security Session Token		

setAuthorisedRepresentative

This operation allows an authorised body to appoint an authorised representative. This process is typically used to allow adults to manage the PCEHRs relating to their dependants.

Parameters	Returns	Business Faults
The IHI of the individual the PCEHR relates to.	None	PCEHR not found
Proposed Authorised Representatives Individual's Identifier		Invalid Security Session Token
Security Session Token		Invalid Representative Identifier

setNominatedRepresentative

This operation allows a PCEHR Managing Individual to appoint a Nominated Representative. Upon successful completion of the process an access code is returned to the portal. This access code must be provided to the nominated representative in order to complete the process.

Parameters	Returns	Business Faults
The IHI of the individual the PCEHR relates to.	Access Code	PCEHR not found
Nominee Identifier		Invalid Security Session Token
Security Session Token		Invalid Representative Identifier

acceptRepresentativeNomination

This operation allows a nominated representative to accept a nomination as a Nominated Representative from a PCEHR Managing Individual via a conformant portal. The Nominated Representative must provide the access code which was generated via a previous call to setNominatedRepresentative by the PCEHR Managing Individual.

Parameters	Returns	Business Faults
The IHI of the individual the PCEHR relates to.	None	Invalid PCEHR
Nominee Identifier		Invalid Nominee
Security Session Token		Invalid Security Session Token
Access Code		Invalid Access Code

excludeOrganisation

This operation allows a PCEHR Managing Individual to exclude a healthcare organisation from accessing an individual's PCEHR. If the healthcare organisation is currently on the 'include' list it will be moved to the 'exclude' list.

Parameters	Returns	Business Faults
The IHI of the individual the PCEHR relates to.	None	Invalid Access Code
Healthcare Provider Identifier – Organisation to be excluded		
Security Session Token		Provider not found

includeOrganisation

This operation allows an individual to grant a Healthcare Organisation access to an individual PCEHR record. If the health organisation is on the 'exclude' list it will be moved to 'include' list.

Parameters	Returns	Business Faults
The IHI of the individual the PCEHR relates to.	None	Invalid Access Code
Healthcare Provider Identifier – Organisation to be excluded		
Security Session Token		Provider not found

doesPCEHRExist

The doesPCEHRExist operation tests for the existence of a PCEHR. The visibility of a PCEHR is dependent upon the individual PCEHR's access control settings and the content of the 'Include' and 'Exclude' lists.

Parameters	Returns	Business Faults
The IHI of the individual the PCEHR relates to.	Code indicating: NotFound PACRequired OpenAccess Suspended	PCEHR not found
Healthcare Provider Identifier - Organisation		
Emergency Access Flag		

generateTAK

This operation allows a CIS to generate a Transferrable Access Key (TAK) for an Individual's PCEHR. This key is required in order for a referring provider to provide "Forward Consent" to another provider when sending a referral document. This key will allow the recipient to obtain access to the PCEHR.

Parameters	Returns	Business Faults
Security Session Token	TAK Expiry Date	Invalid Security Session Token
The IHI of the individual the PCEHR relates to.		PCEHR or Provider Identifier does not match the Security Session Token
		Invalid PCEHR
Healthcare Provider Identifier - Organisation		Insufficient access rights

Document Query and Management External Interface

The Document Query and Management interface provides the key set of operations required to access and add documents within the context of an individual PCEHR.

The list below is not intended to represent the final set of realised service interfaces. A separate NEHTA interface specification will be produced to tie this logical set of operations onto an implementable realisation. This realisation will take into account the standards used within this area (such as HSSP RLUS and IHE XDS.b), protocol constraints and NEHTA's supporting suite of documents, specifications and standards (including the National E-Health Web Service Profile).

openPCEHR

The open operation is intended to aid access management and the persistence of sessions. The open operation must be called in advance of any attempts to access PCEHR data.

Parameters	Returns	Business Faults
Provider Credentials	Security Session Token	Invalid credentials
The IHI of the individual the PCEHR relates to.		Invalid PCEHR

closePCEHR

The close operation is called when the client explicitly wants to end a PCEHR access session. This operation is only valid when called during a valid authenticated session.

Parameters	Returns	Business Faults
Security Session Token	None	Invalid or Expired Security Session Token
The IHI of the individual the PCEHR relates to.		Invalid PCEHR

retrieveDocument

The retrieveDocument operation returns exactly one document from a given PCEHR. Logically a combination of the find and retrieve functions may be used to return multiple documents.

Parameters	Returns	Business Faults
Security Session Token	Envelope including: Envelope header Clinical Document Template Identifier	Invalid Security Session Token
The IHI of the individual the PCEHR relates to.		Individual or Provider Identifier does not match the Security Session Token
		Invalid PCEHR
Healthcare Provider Identifier - Organisation		
PCEHR Document Identifier		Invalid Document Identifier
		Insufficient access rights

findDocument

The find operation allows the user to search for one or more documents within the context of a single PCEHR. The search operations include but are not limited to the ability to search for documents of a given type, documents added or authored between specific dates, documents containing specific keywords or documents produced by particular authoring individuals or organisations. In order to support this requirement the solution will offer multiple logical find operations each with a pre-defined set of specific parameters. Search queries will be maintained within the PCEHR server and there will be no requirement to allow clients to specify custom queries or to specify a cross enterprise query language.

Parameters	Returns	Business Faults
Security Session Token	List of Document Envelopes including the Envelope Header (but not the document).	Invalid Security Session Token
The IHI of the individual the PCEHR relates to.		Individual or Provider Identifier does not match the Security Session Token
		Invalid PCEHR
Healthcare Provider Identifier - Organisation		
Search type and parameters		Invalid Search Criteria

storeDocument

The store document operation is used store a document within a specific PCEHR. The document may represent a new document or an update to a previous document. The client application must provide both the document to be stored and the set of metadata required to facilitate storage. As there is a requirement to support various levels and types of document structure there is no guarantee that the internal document metadata will be sufficient to populate the necessary internal data elements required to support document access. Consequently all of the necessary document metadata must be carried within the document envelope in order for the document to be added to the repository.

Parameters	Returns	Business Faults
Security Session Token	PCEHR Document Identifier	Invalid Security Session Token
The IHI of the individual the PCEHR relates to.		Individual or Provider Identifier does not match the Security Session Token
Healthcare Provider Identifier - Organisation		Invalid PCEHR
Envelope including: Clinical Document Envelope Header Identifier of related documents (and relationship type) Template Identifier		Invalid Document, Metadata or template.
		Insufficient access rights

removeDocument

The remove document operation is used to logically remove a document from a specific PCEHR. The removal should remove the document from all queries performed on the PCEHR System and all data views produced from PCEHR data.

Whilst the document will be removed from all Consumer and Provider views of the PCEHR the physical document (and any associated audit data) will not be removed from the system.

Parameters	Returns	Business Faults
Security Session Token	None.	Invalid Security Session Token
The IHI of the individual the PCEHR relates to.		Individual or Provider Identifier does not match the Security Session Token
PCEHR Document Identifier		Invalid PCEHR
		Insufficient access rights
Reason for removal.		
Removal code.		

storeDocumentMetadata

The storeDocumentMetaData operation is intended to allow clients to add a document which is stored within a conformant repository without sending the physical document to the PCEHR System. This will be particularly relevant for large documents.

Parameters	Returns	Business Faults

Parameters	Returns	Business Faults
Security Session Token	PCEHR Document Identifier	Invalid Security Session Token
The IHI of the individual the PCEHR relates to.		Individual or Provider Identifier does not match the Security Session Token
Envelope including: Envelope Header		Invalid PCEHR
Atomic Data		Insufficient access rights
		Invalid document metadata

retrieveDocumentMetaData

This method is intended to allow systems to pull the meta data associated with a document from the PCEHR. This functionality will typically be used to populate index views and document synopsis data in CIS systems and portals without the need to retrieve entire documents.

Parameters	Returns	Business Faults
Security Session Token	Envelope including: Envelope Header	Invalid Security Session Token
The IHI of the individual the PCEHR relates to.		Individual or Provider Identifier does not match the Security Session Token
PCEHR Document Identifier		Invalid PCEHR
		Insufficient access rights
		Invalid document identifier

setDocumentAccessLevel

This function is used to change the access level associated with a document. Documents may be marked as being available for "general access", "limited access" or "no access" and may be repeatedly moved between states.

Parameters	Returns	Business Faults
Security Session Token	None.	Invalid Security Session Token
The IHI of the individual the PCEHR relates to.		Individual or Provider Identifier does not match the Security Session Token
PCEHR Document Identifier		Invalid PCEHR
Desired Access Level (pre-defined)		Insufficient access rights
		Invalid document identifier

PCEHR View Interface

The view service is responsible for returning views of PCEHR data which span more than one document. They are explicitly views of a PCEHR rather than views of a document.

getConsolidatedView

The getConsolidatedView function is responsible for constructing the representation of the consolidated view from the internal atomic data model. This may be realised in many different ways, for example the atomic data view could be modelled as a set of relational database tables and the XML representation of a view constructed from this data on demand. Alternatively the atomic data model may be stored directly as an XML construct which is updated as a new document is inserted and converted to individual view representations using an XML conversion technology such as XSLT.

The consolidated view presented to a requestor must only contain data drawn from documents appropriate for the requestor's access rights.

Parameters	Returns	Business Faults
Security Session Token	PCEHR Consolidated View	Invalid Security Session Token
The IHI of the individual the PCEHR relates to.		Individual or Provider Identifier does not match the Security Session Token
Healthcare Provider Identifier - Organisation		Invalid PCEHR
Healthcare Provider Identifier - Individual		Insufficient access rights

getIndexView

The getIndexView provides a view of the set of documents associated with a PCEHR. The view must be sensitive to the requestors access rights and the associated access sensitivity of each document.

Parameters	Returns	Business Faults
Security Session Token	PCEHR Index View	Invalid Security Session Token
The IHI of the individual the PCEHR relates to.		Individual or Provider Identifier does not match the Security Session Token
Healthcare Provider Identifier - Organisation		Invalid PCEHR
Healthcare Provider Identifier - Individual		Insufficient access rights

getChangeHistoryView

The getChangeHistoryView provides a view of the documents changed within a pre-defined timeframe. The view must be sensitive to the requestor's access rights and the associated access sensitivity of each document.

Parameters	Returns	Business Faults
Security Session Token	PCEHR Change History View.	Invalid Security Session Token
The IHI of the individual the PCEHR relates to.		PCEHR or Provider Identifier does not match the Security Session Token
Healthcare Provider Identifier - Organisation		Invalid PCEHR

Parameters	Returns	Business Faults
Healthcare Provider Identifier - Individual		Insufficient access rights

getConsumerAuditView

Audit data is logged whenever a key business event is performed within the PCEHR System. In order to avoid the consumer being overloaded with information the consumer view limits this data to the set of key events relevant to consumer portal usage scenarios. Further detail may be available on request from the system administrators.

Parameters	Returns	Business Faults
Security Session Token	PCEHR Audit View	Invalid Security Session Token
The IHI of the individual the PCEHR relates to.		Individual's Identifier does not match the Security Session Token
		Invalid PCEHR
		Insufficient access rights

Dependencies

The Core Infrastructure Service Layer is dependent upon a number of internal technical services and external services. It is expected that this list will include:

- The National Repositories
- One or more conformant repositories
- The Template Service

Support Interfaces

The set of support interfaces are used to expose the set of functionality required to aid the support portal.

Report Interfaces

The report interfaces expose the functionality required to access system reports.

System Administration Interfaces

The System Administration Interfaces may be used by System Administration interfaces (including the Administration and Report Portal) to monitor and administer the PCEHR System.

3.1.3.2 Technical and Business Service Layers

The business services layer encompasses the key *business* services. These are business specific services, not intended for re-use and are typically composed of one of more technical or entity services.

The technical service layer incorporates encapsulated non-business specific services intended for re-use. It is intended that series of interactions across these process will provide parts of the upper level business services.

The co-ordination of these series of interactions is logically deferred to a service co-ordination layer. This document does not stipulate that this layer be realised through orchestration, choreography, event driven messaging or any other such process management paradigm. Whilst not explicitly part of the PCEHR scope where possible these services should be built with consideration for re-use in other E-Health initiatives.

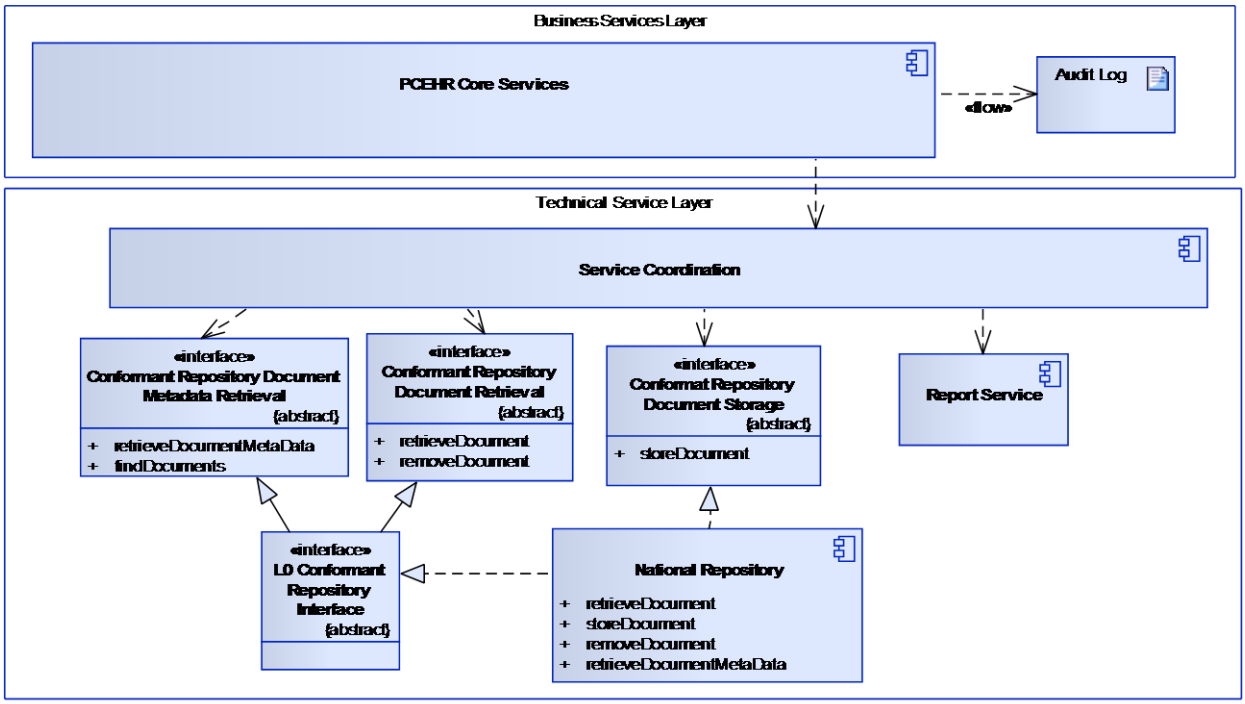


Figure 40 - Technical and business services

Core PCEHR Services

The core PCEHR Services is an encapsulation of the conceptual services represented in [PCEHR_CON_OPS]. The focus within the computational view is on system boundaries – interfaces and internal components are only specified when they must be realised separately.

This "black box" service grouping logically includes the View Service, Index Service, Participation and Authorisation Service and any other internal functional offerings. It is highly desirable that the internal components of this piece be realised as re-usable self-contained entities which can be composed, choreographed or orchestrated into wider functional offerings.

Audit Log

The audit log is used to capture key events within the PCEHR System. It is not intended that external systems will add entries to the Audit Log.

National Repositories

The National Repositories are a logically centralised set of repositories for clinical documents. [PCEHR_CON_OPS] states that all health summaries, discharge summaries and event summaries will be stored within this repository.

The National Repositories do not represent the sole document data stores and documents may also be stored across other conformant repositories.

The National Repositories interface is a PCEHR L1 compliant conformant repository. Please refer to the conformant repository specification for interface details.

While there are no direct in line dependencies, it is assumed that all documents within the repository will be conformant against one or more templates stored within the Template Service and that the mechanism for accessing data will be managed via the Document Query and Management Service.

Service Co-ordination

The Service Co-ordination component is a logical component responsible for executing sequences of processes across internal and external sub-components or services. While this is not a mandatory component, it is strongly encouraged that functional components be realised as atomic, re-usable services and that the execution plan by which these services are orchestrated be highly configurable. There is no explicit requirement for this to be realised through a business process execution language.

Report Service

The PCEHR Report Service allows operational reports to be extracted from the PCEHR System. These reports are limited to the purposes of understanding PCEHR programme take-up and usage. The service is not intended to support the use of PCEHR data within documents for analytical purposes.

3.1.3.3 Operational System Layer

The operation systems layer is intended to incorporate the set of existing systems which are relied upon to perform dependent composite parts of internal service execution. While not specified here, it is expected that services may require adaptor services to allow them to be introduced into the internal processing flow.

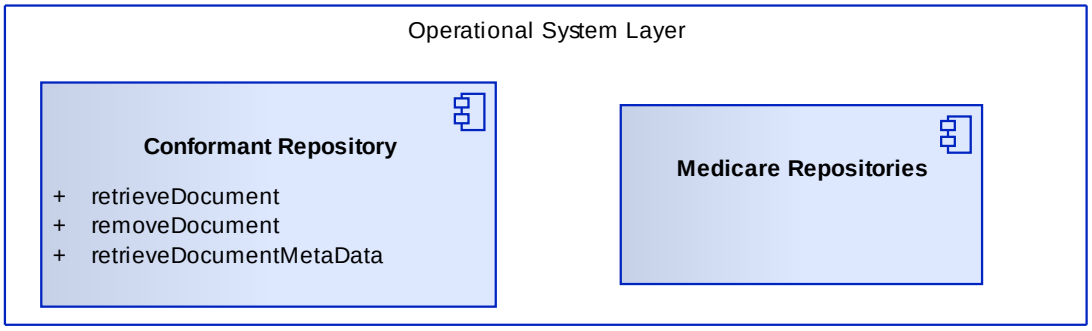


Figure 41: Operational systems layer

Conformant Repository

A conformant repository is any repository that is conformant with the PCEHR specification. This specification will be realised as a sub-system solution design and include technical interfacing, privacy, security, storage and availability requirements.

The detailed specification of what is required for repository conformance is deferred to the Conformant Repository Solution Design.

Each conformant repository may need to maintain a local index in order to facilitate external referencing and data access.

Many conformant repositories may be created by grafting the PCEHR conformant repository interface and requirements onto existing repositories. As such conformant repositories may be used by consumers other than PCEHR and across other interfaces.

Each conformant repository must support the set of operations required to retrieve document from the repository. This will be deemed L0 Interface compliant. Repositories which support retrieval and storage will be L1 interface compliant. Repositories that support retrieval, storage and the set of PCEHR administration interfaces will be deemed L2 compliant.

It is expected that most repository systems will be L0 compliant.

In isolation the National Repositories represents a L1 compliant repository. The PCEHR System as a whole is in effect a L2 compliant repository.

retrieveDocument

The retrieveDocument operation returns exactly one document to the calling system.

Parameters	Returns	Business Faults
Security Session Token	Document Envelope including: Document	Invalid Security Session Token – If validated.
The IHI of the individual the PCEHR relates to.		Individual or Provider Identifier does not match the Security Session Token – If verified.
Healthcare Provider Identifier - Organisation		
Local Document Identifier		Invalid Document Identifier
		Insufficient access rights

removeDocument

The find document operation allows the caller to inform the repository of the request or remove a document.

Parameters	Returns	Business Faults
Security Session Token	None.	Invalid Security Session Token – If validated.
The IHI of the individual the PCEHR relates to.		Individual or Provider Identifier does not match the Security Session Token – If verified.
Local Document Identifier		Insufficient access rights
Reason for removal.		
Removal code.		

retrieveDocumentMetaData

The retrieveDocumentMetadata operation allows a system to extract the meta data associated with a document from a repository. This method is primarily used to allow the PCEHR System to "pull" document data from other repositories.

Parameters	Returns	Business Faults
Security Session Token	Envelope containing: Envelope Header	Invalid Security Session Token – If validated.
The IHI of the individual the PCEHR relates to.		PCEHR or Provider Identifier does not match the Security Session Token – If verified.
Local Document Identifier		Insufficient access rights
		Invalid document identifier

Medicare Repositories

The set of Medicare Repositories may be leveraged where appropriate to support PCEHR functionality. A key example of this is the potential use of the Medicare Databases in order to validate user credentials against stored demographic data. All potential access must be subject to an appropriate level of privacy, security and legal scrutiny and may require changes in legislation.

3.1.3.4 Foundation Services

The Foundation Services layer contains the set of relevant national components which will be present at the current expected PCEHR System activation date. This includes but is not limited to the set of NEHTA managed foundation services.

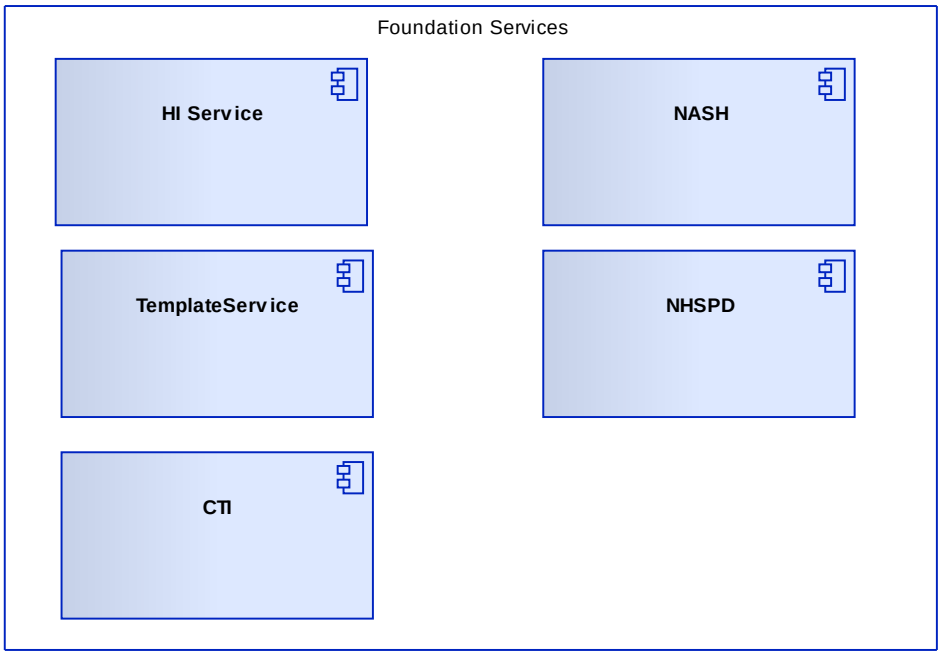


Figure 42: Foundation Services

Template Service

The Template Service is a national service providing access to data definitions. Each document within the PCEHR System must relate to one or more templates in the national Template Service.

A template is a logical construct which contains:

- The definition of the data type structure (typically an XSD)
- A set of validation specifications (such as schematron schemas)
- Rendering definitions (such as XSLTs)
- Supporting reference and lifecycle management data.

Each template must provide the definition required to support the management of the atomic data model.

HI Service

The Healthcare Identifier (HI) Service provides the mechanism to identify every individual (IHI), healthcare provider organisation (HPI-O) and healthcare provider (HPI-I) in Australia.

Within the PCEHR System, the individual's health identifier (IHI) will relate to zero to one PCEHR. Organisations and healthcare individuals will be identified by their HPI-O and HPI-I.

NASH

The National Authentication Service for Health (NASH) provides a nationwide solution for authenticating healthcare organisations and individuals for purposes relating to the exchange of eHealth data.

NASH provided credentials will form the basis for authenticating healthcare providers and individuals within the PCEHR System. Although individuals do have a unique healthcare identifier there is currently no national mechanism for an individual to assert their identity or for this assertion to be validated.

NHSPD

The National Healthcare Service Providers Directory provides a mechanism to search for and query the details of National Healthcare Services Providers. The PCEHR System is not dependent upon the NHSPD.

CTI

The Common Terminology and Information components and processes provide the mechanism for defining a common ontology for Clinical Terminology and include the definition of SNOMED-CT AU, AMT along with the definition of National CDA messages.

3.1.4 Key System Interaction Scenarios

The section below elaborates a number of end-to-end interaction scenarios for key events within the system. Only those interactions deemed particularly relevant or where specific functional points require highlighting are shown.

3.1.4.1 Open a PCEHR

The scenario focuses on the interactions involved in opening a PCEHR. The open operation provides an upfront mechanism for ensuring the correct identification of a PCEHR and determining the authorisation level of the requestor.

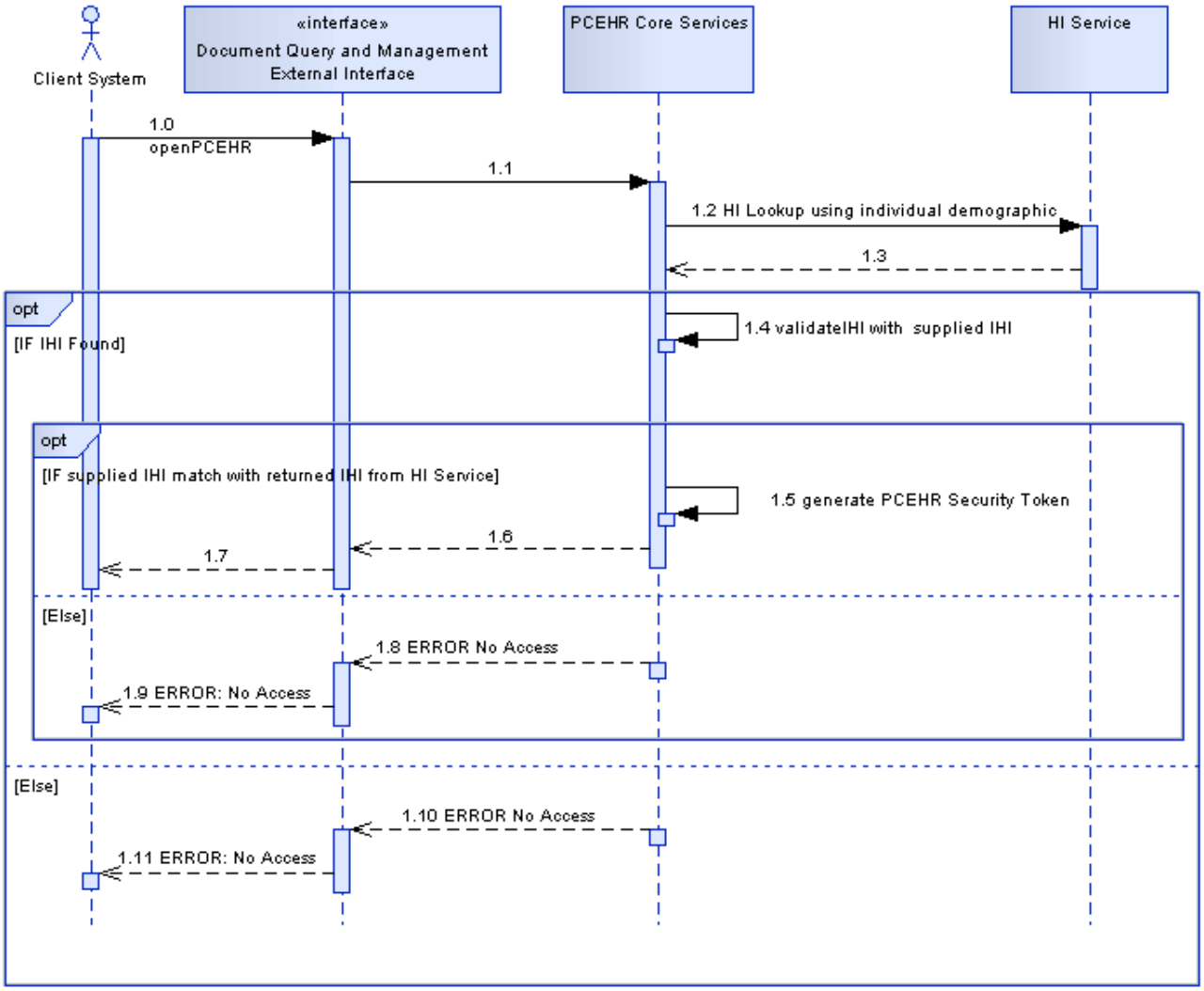


Figure 43: Open PCEHR - Identify PCEHR

Key points:

- The PCEHR is identified using both an IHI and a set of demographic data relating to the individual.
- Access is denied if the demographic data does not match the data associated with an IHI.

After the correct PCEHR is located, the system must determine the provider's level of authorisation for the identified PCEHR.

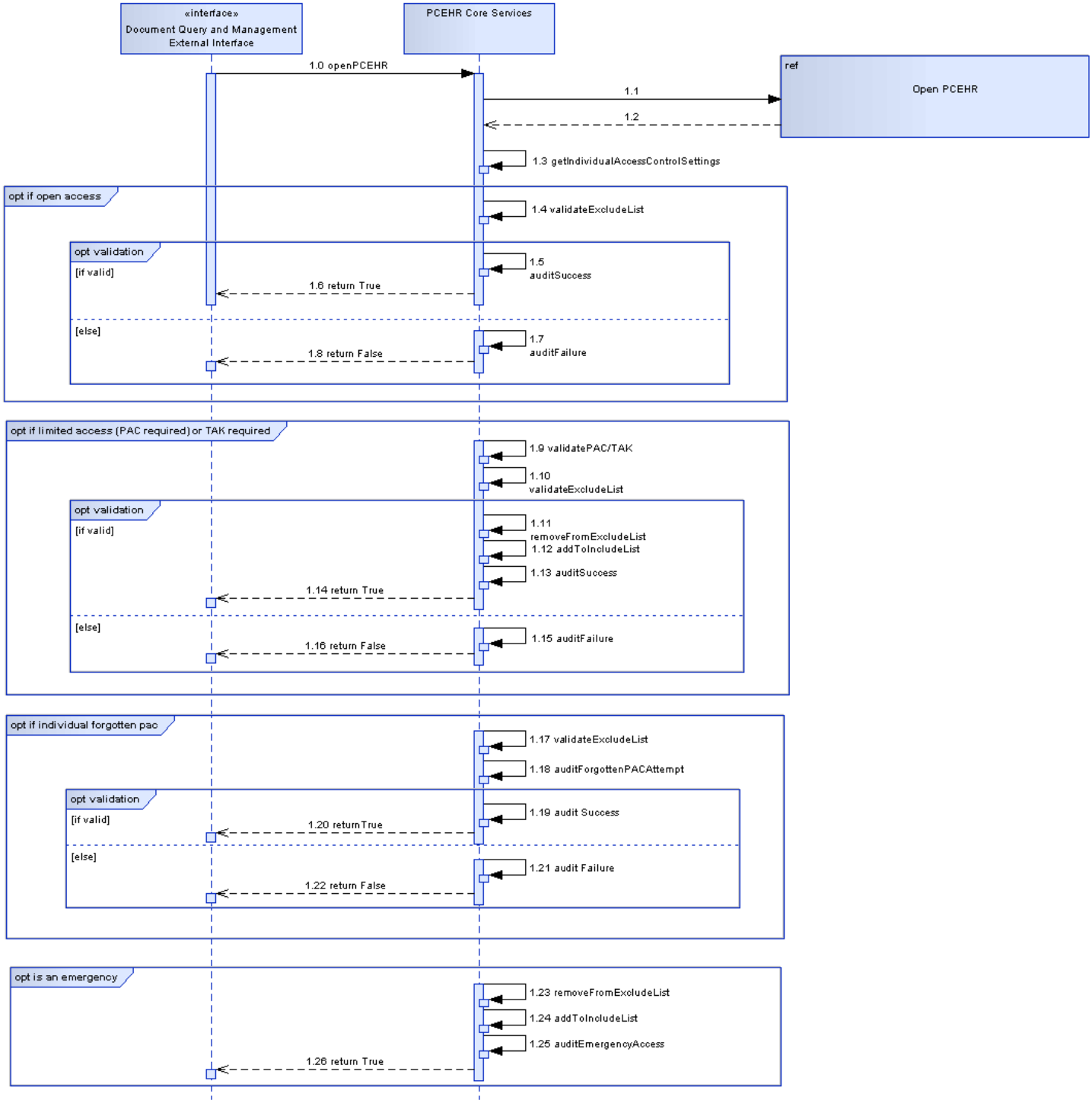


Figure 44: Open a PCEHR - provider authorisation

Key points:

- The open operation must be called in advance of any attempts to access PCEHR data.
- If the PCEHR is set to "General Access", the provider has access unless they are representing an organisation on the exclude list.
- If the PCEHR is set to "Limited Access" (PAC Required) the provider does not have access unless they are on the include list.
- If the user forgets their PAC code, the provider may manually add themselves to the include list.

- If the provider requires emergency access to the PCEHR, they are granted access and added to the include list (although they may be later excluded).
- The PCEHR must be opened and the accessor appropriately authenticated before a document is retrieved.
- Documents may be stored within a National Repository or a Conformant Repository.
- If the user does not have sufficient access rights, the presence of the document or the PCEHR is hidden.

3.1.4.2 Retrieve a Document

This scenario outlines the process for a CIS system or portal to retrieve a document from the PCEHR System. This document may be stored in the National Repositories or an external Conformant Repository.

Prior to retrieving a document, the requestor must have been successfully authenticated and the appropriate IHI must have been determined.

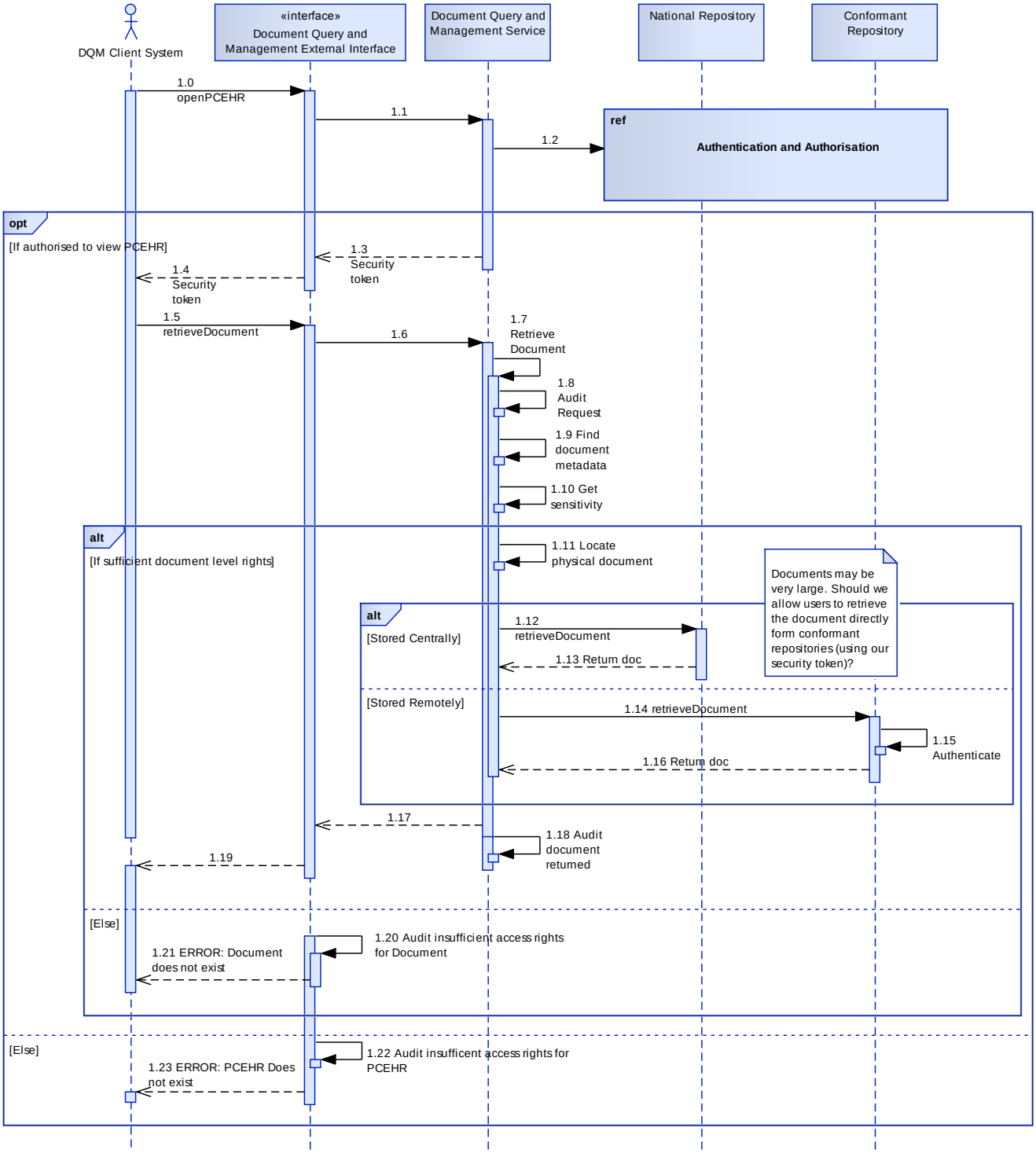


Figure 45: Retrieve a document

Key points:

- The PCEHR must be opened and the accessor appropriately authenticated before a document is retrieved.
- Documents may be stored within a National Repository or a Conformant Repository.
- If the user does not have sufficient access rights, the presence of the document or the PCEHR is hidden.

3.1.4.3 Get Consolidated View

This section outlines the process for retrieving a consolidated view.

Prior to retrieving a document, the requestor must have been successfully authenticated and the appropriate IHI must have been determined.

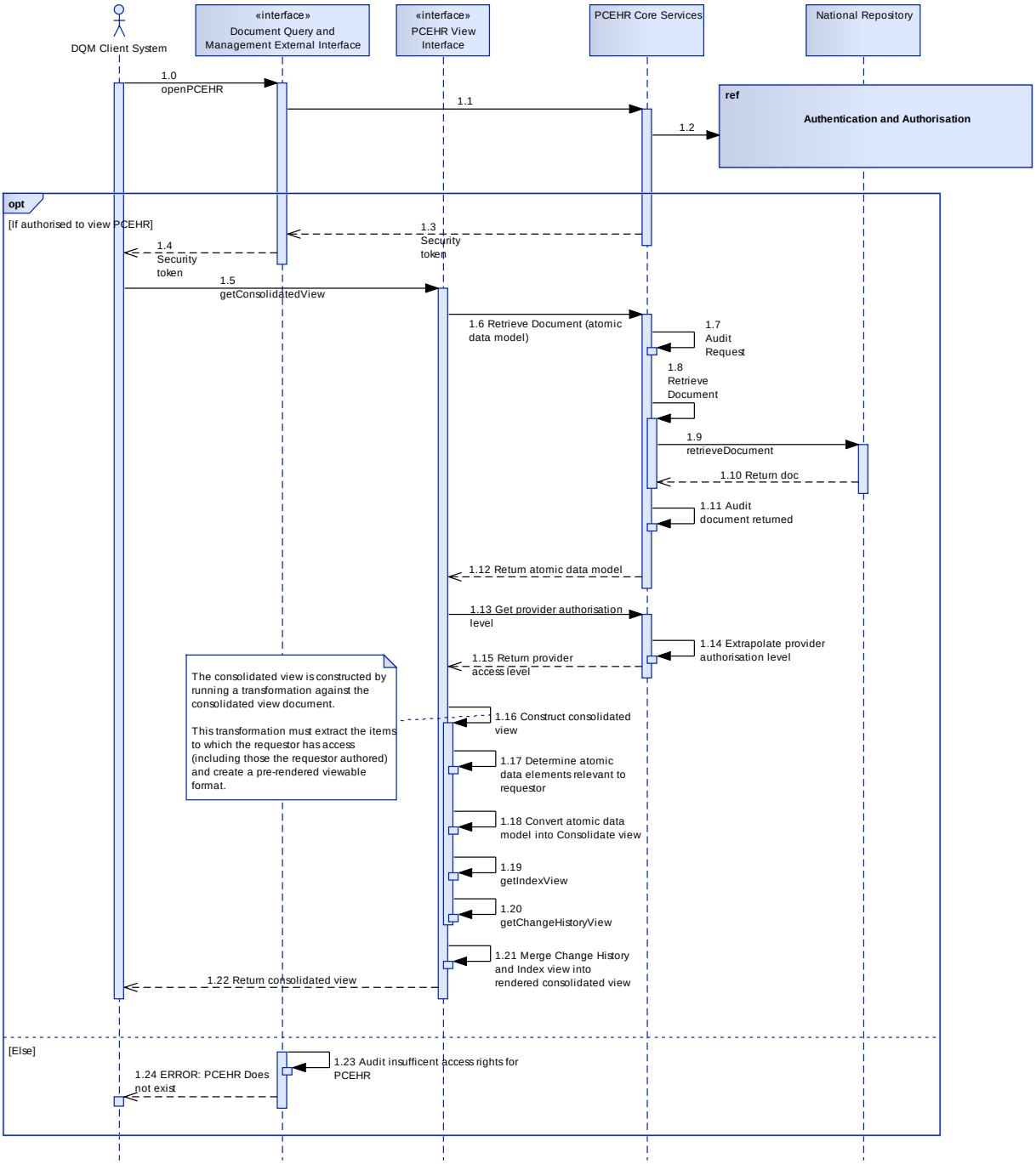


Figure 46: Retrieve a consolidated view

Key points:

- The underlying PCEHR documents are not accessed in order to create the consolidated view.
- The atomic data model contains all of the key data associated with the individual (from all sources).
- The atomic data model is stored as a single document.
- A rendering process creates viewer specific views of the atomic data model on demand.
- The index and change history views are re-used as composite parts of the consolidated view.
- The consolidated view is returned in a pre-rendered form. Client systems should merely be able to understand the definition of the rendering specification rather than the content of the fields. This is analogous to a browser being able to understand HTML but not the content all web pages.

3.1.4.4 Find a Document

The find process allows a client to search for one or more documents within a single PCEHR.

Prior to finding a document, the requestor must have been successfully authenticated and the appropriate IHI must have been determined.

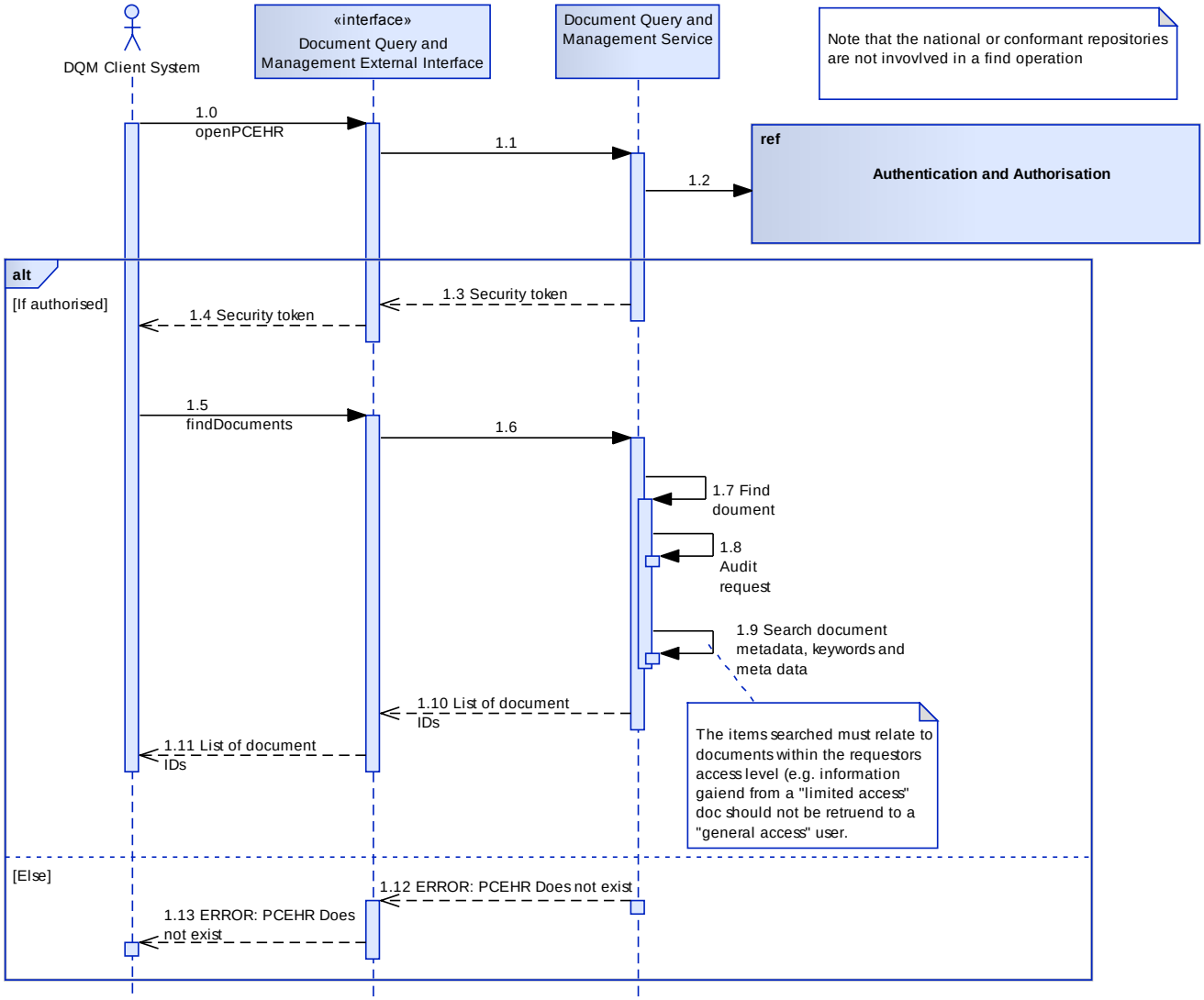


Figure 47: Find document(s)

Key points:

- The PCEHR must be opened and the accessor appropriately authenticated before a document is retrieved.
- The operation returns a list of document identifiers rather than the documents themselves.
- For extremely large documents, it may be prudent to allow the client to retrieve the document directly from conformant repositories (using the retrieved Security Session Token and document identifier).
- Documents may be stored within a National Repository or an external Conformant Repository.
- The presence of the document or the PCEHR is hidden where the user does not have sufficient access rights.
- This process allows a user to find a document within a single PCEHR according to it is pre-defined index metadata. There is no requirement to search or index document contents.

3.1.4.5 Store a Document

This scenario outlines the process for storing a document within a PCEHR. The user need not have sufficient permissions to view a PCEHR in order to upload data.

As part of the store operation, the data within a structured document may be extracted and used in the production of data views, such as the consolidated view outlined in [PCEHR_CON_OPS]. When a document is stored, the PCEHR will query the national Template Service to retrieve the document template. This template must provide a definition of how to extract data elements from a document. Once the data is extracted, it will be added to a centralised atomic data model (there is no constraint placed on how this is realised).

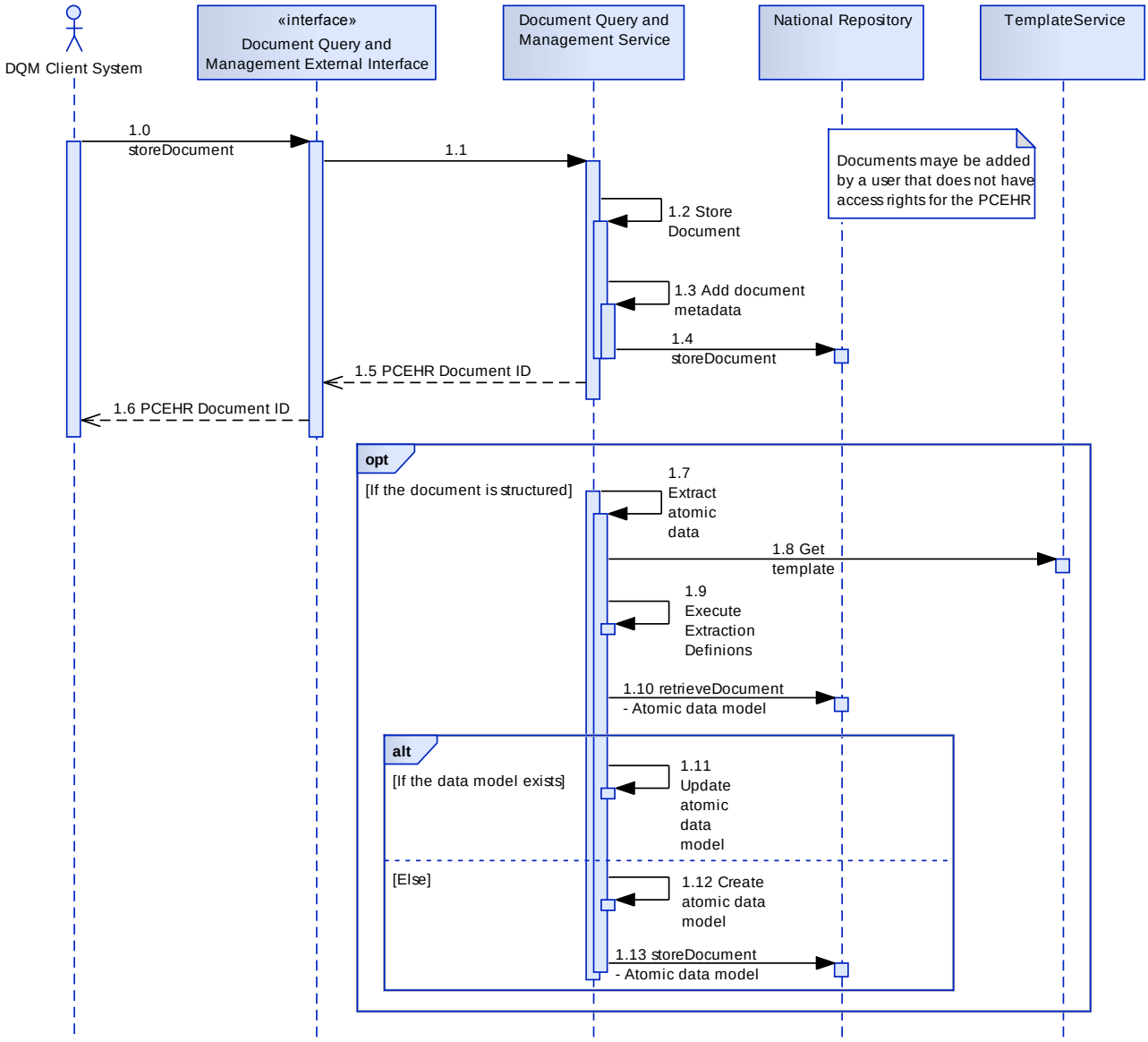


Figure 48: Store a document

Key points:

- Documents may be structured or unstructured.
- Structured documents must be associated with a template present within the National Template Service.
- Atomic data may be extracted from documents for use within PCEHR views.

3.1.4.6 Remove a Document

The remove scenario outlines the process associated with a logical record deletion. It is unlikely that documents will be physically deleted, but they may be marked as inactive. Inactive documents or any data obtained from these documents should not be returned to the client or used within the PCEHR views.

The ability to remove elements from an atomic data view will require any atomic data repository or centrally stored data view representations to maintain a link between each data element and the source document from which they were extracted. Where a data item is sourced from multiple documents, the removal of one source document should not lead to the removal of the data element but rather the removal of the data source associated with the element.

A reason and description of why the document is being removed must be provided.

The removal process must be audited. The removal reason code will be used to determine the nature of the removal. Depending on the code supplied, a work item may be raised for the system administrator to review the action.

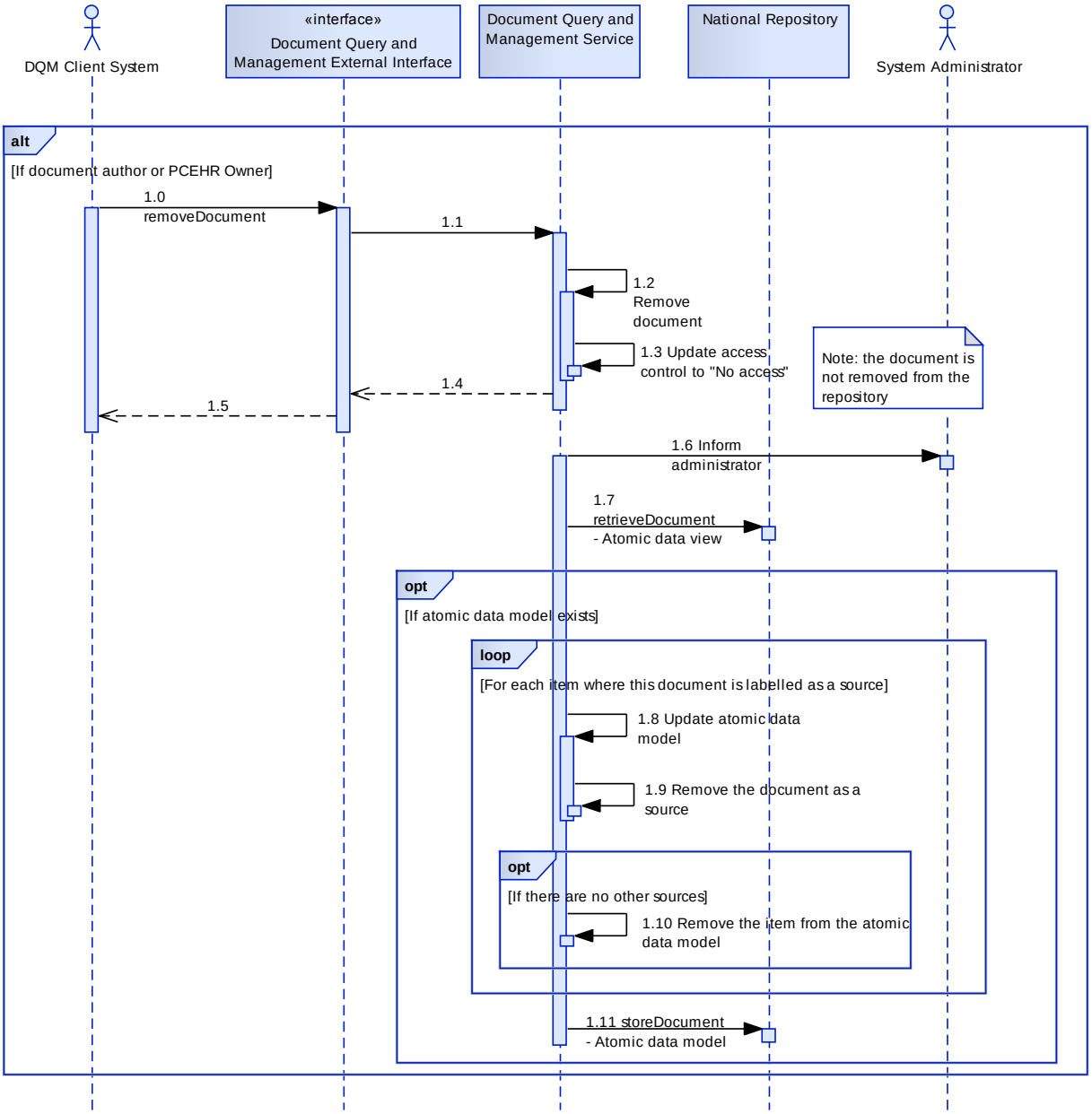


Figure 49: Remove a document

Key points:

- The PCEHR must be opened and the accessor appropriately authenticated before a document is removed.
- Documents may be stored locally or remotely.
- All data elements extracted from the document must also be removed.

3.1.4.7 Direct Store on a Conformant Repository

Documents may be stored directly within a conformant repository. This process may be performed in accordance with the PCEHR specification for a store operation or via alternate local storage policies. When a document is added to a conformant repository, either the client or the repository itself may then register the document with the PCEHR System and logically add it to the Individual's PCEHR.

In order to achieve this, the document metadata must be passed to the PCEHR System. This in effect involves the presentation of a message envelope containing only the message header component.

However, the population of the internal atomic data model used to support the production of data views requires that each document be parsed against the document template.

In this instance, the client program takes the optional responsibility to perform this parsing operation and provide the atomic data to the PCEHR System.

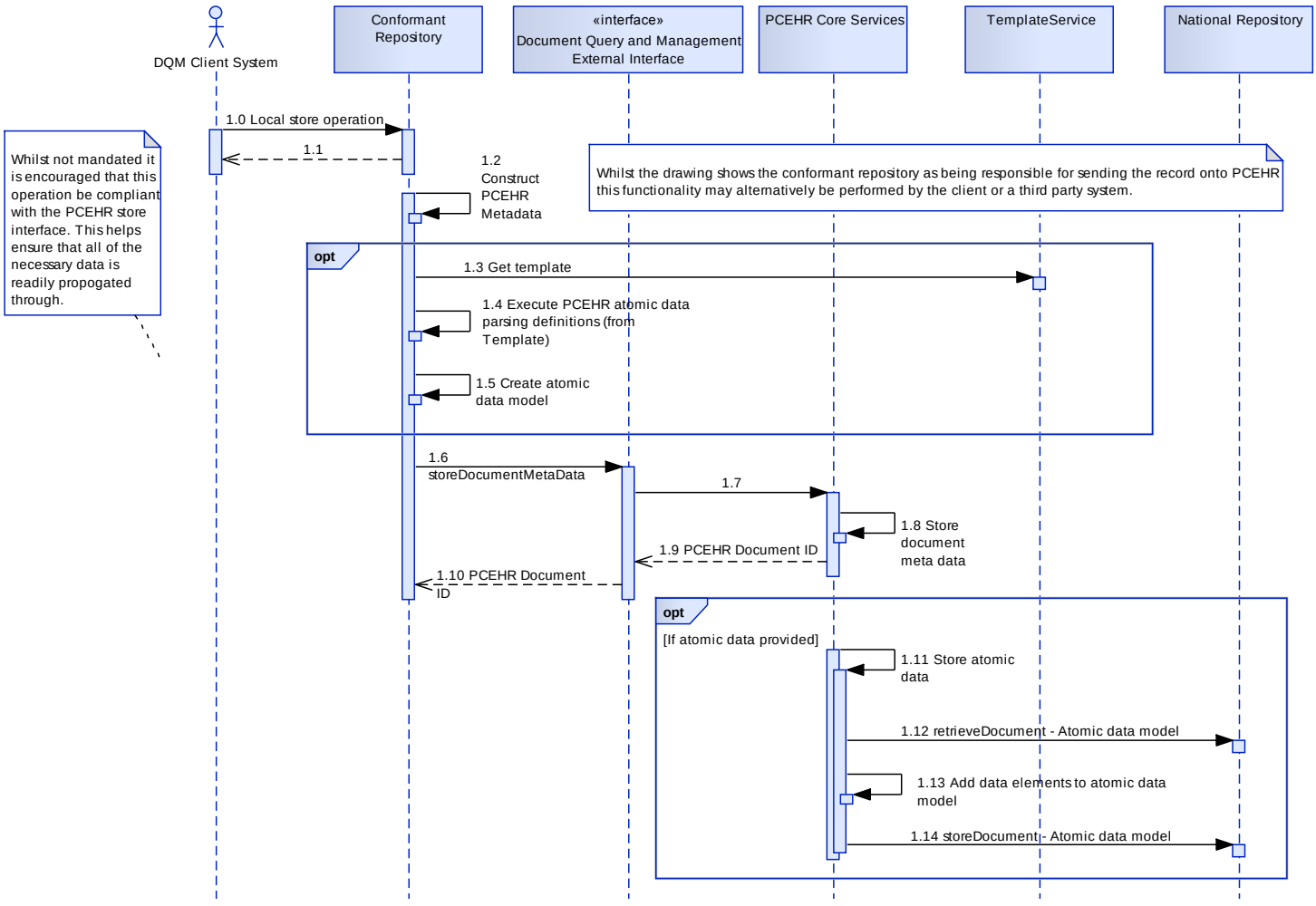


Figure 50: Store document metadata

Key points:

- The document is not passed to the PCEHR System.
- The conformant repository may optionally parse the document in accordance with a national template and provide the output to the PCEHR System.
- The presence of the PCEHR is hidden if the user does not have sufficient access rights.

It is essential that the document reference (the fully qualified mechanism used to refer to a single document version) provided to the PCEHR System by the conformant repository is not re-used for other documents or versions within the repository. This requirement must form part of the conformant repository specification. Additionally, the PCEHR System should, where document size allows, store a hashed representation of the document which may be used to verify that the document link consistently points to the same document.

3.1.4.8 Set Document Access Level

The set document access level scenario outlines the end-to-end process required for a user to explicitly set the access level associated with a document.

All documents are initially added in accordance with the author's access level. For example:

- Where the author has general access, any documents created by the author will be added with an access type of "General Access".
- Where the provider has explicitly been granted access to limited access documents, all documents added by that author to the specified PCEHR will also be marked as being for "Limited Access". This second case is largely driven by the need to handle the case where a provider may reference limited access documents within other documents.

The individual may change the document access level at any point (either marking it as being for limited or general access).

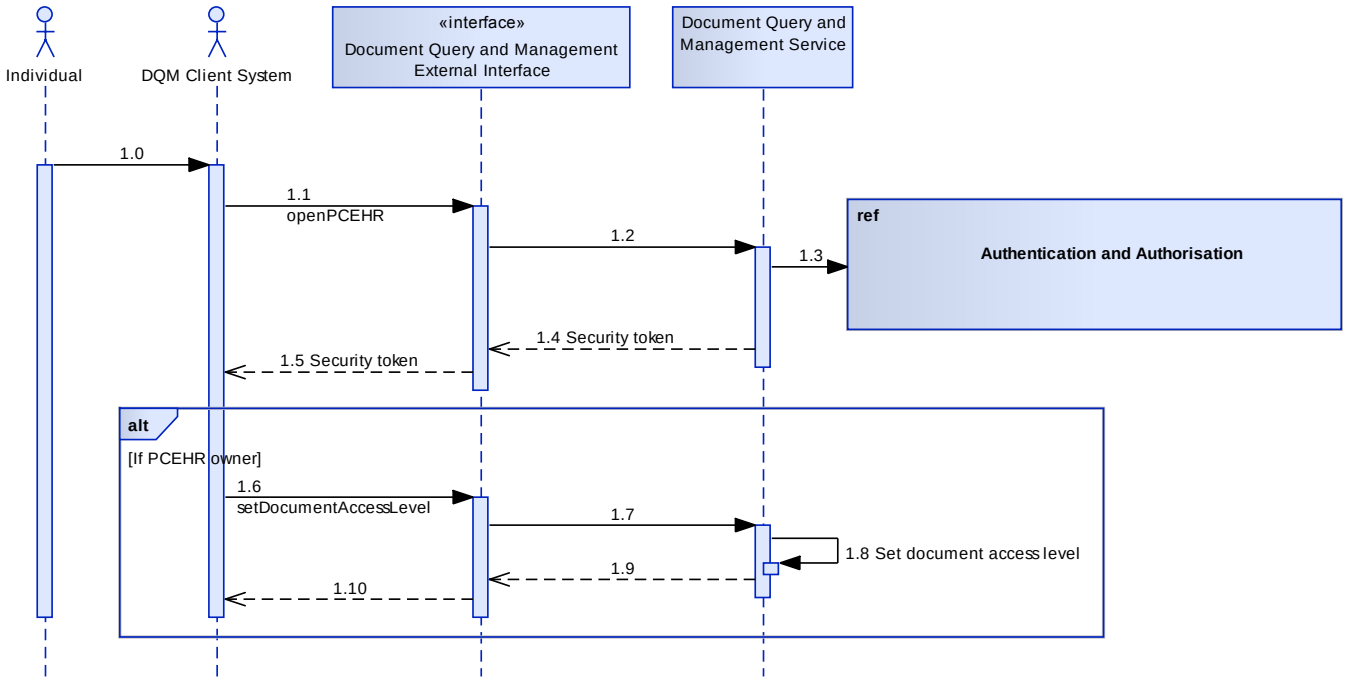


Figure 51: Set document access level

3.1.4.9 Provider CIS Authentication

Individual level provider authentication within a CIS is deferred to the CIS system. The process of assuring that a system is PCEHR conformant should include a security/risk assessment of the system with a focus on the strength of the system's authentication process.

The PCEHR System will authenticate the clinical organisation (HPI-O) via the organisation's NASH certificate. Authorisation will be assigned to the authenticated organisation and, by default, to all individuals within that organisation who are authorised by the CIS to access the PCEHR.

3.1.4.10 Provider Portal Authentication

A provider must present their NASH credentials in order to log onto the Provider Portal.

The credentials may be stored on a provider smartcard and accessed through a smart card reader attached to a compliant terminal.

The provider's NASH credentials are provided to the portal and authenticated in accordance with NASH specifications.

3.1.4.11 Provider Authorisation

Provider authorisation within PCEHR is managed at the organisation level, however user credentials are provided at the individual level. The HI Service is used to manage this linkage.

The provider portal is responsible for querying the HI Service for the list of HPI-Os relating to an authenticated provider and returning these to the user. The user then selects the HPI-O most appropriate for the current usage scenario. The user may not use an HPI-O which is not associated with the user's HPI-I within the HI Service.

An authenticated provider organisation may make a request to open a specific PCEHR. The PCEHR System then checks the relevant PCEHR's global access level and for the presence of the clinical organisation on the PCEHR's include and exclude lists. Access is granted if the provider organisation is on the 'include' list, or if the PCEHR is set to "General Access" and the provider organisation is not on the exclude list, or if the provider presents a valid access code (PAC, PAC-X or TAK), or if the provider asserts that they require emergency access to the PCEHR.

If the provider organisation is granted access, a secondary check is made to determine whether the provider organisation has access to "Limited Access" documents within the PCEHR.

If the access request is granted, a time-limited Security Session Token is returned to the provider CIS or portal. This token must be submitted to the system on future calls in order to gain access to views and documents within the PCEHR. The token is specific to one session with one PCEHR.

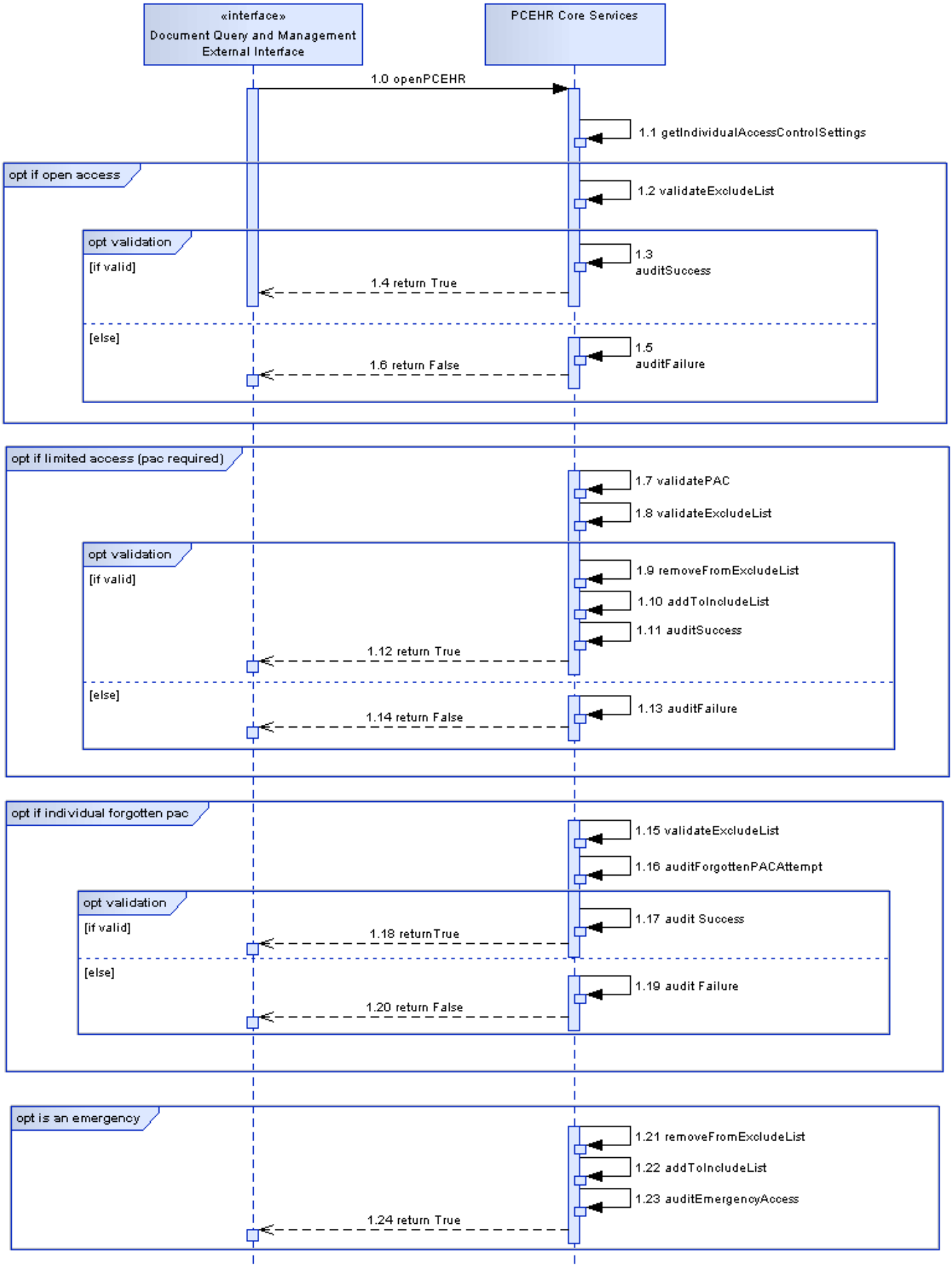


Figure 52: Provider authorisation

Key points:

- Authorisation applies to a clinical organisation and not an individual.
- A security session token is used to avoid excessive re-authorisation overheads.
- It is highly desirable that this token be re-usable for direct communication with conformant repositories.

3.1.4.12 Consumer Portal Authentication

Initialisation

Consumer portal authentication is multi-faceted and intrinsically linked with registration. The individual must first create a user account directly with the portal. The information associated with this account is local to the portal and the portal's local security policies.

After creating an account, the user must link this account with a PCEHR. In order to create this link, the user must provide a set of demographic details which can be validated within the set of Medicare databases. If the association is successfully validated, a secondary stage validation may take place (such as the sending of an authorisation code to the individual's registered address).

After the successful completion of this process, the portal account is associated with a PCEHR. The PCEHR may or may not already be activated (multiple portal accounts could be linked to the one PCEHR).

The conformant portal must contact the Secure Token Service (STS) in order to complete the association process. The STS validates the relationship (and any secondary authentication code) and returns an Identity Assertion Token to the portal. This represents the primary credential for representing a consumer portal encapsulation of an individual's identity. The token must be retained for the lifetime of the portal and PCEHR relationship. If the token is lost or corrupted, the association process must be repeated.

Once the portal account is linked to an activated PCEHR, the user may log in and manage the account.

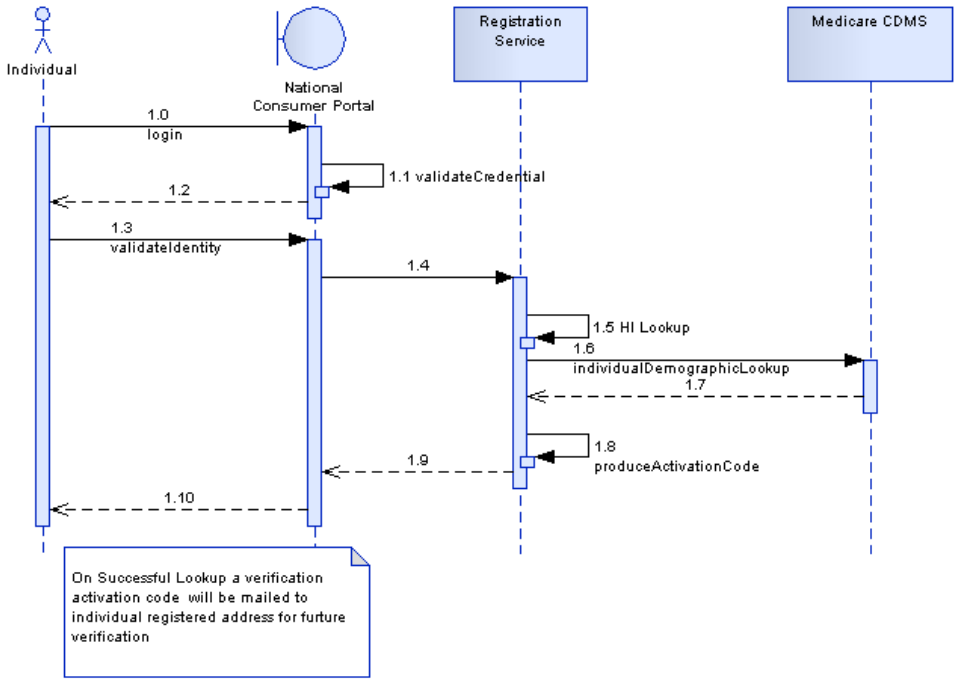


Figure 53: Linking a portal account to a PCEHR – Step 1

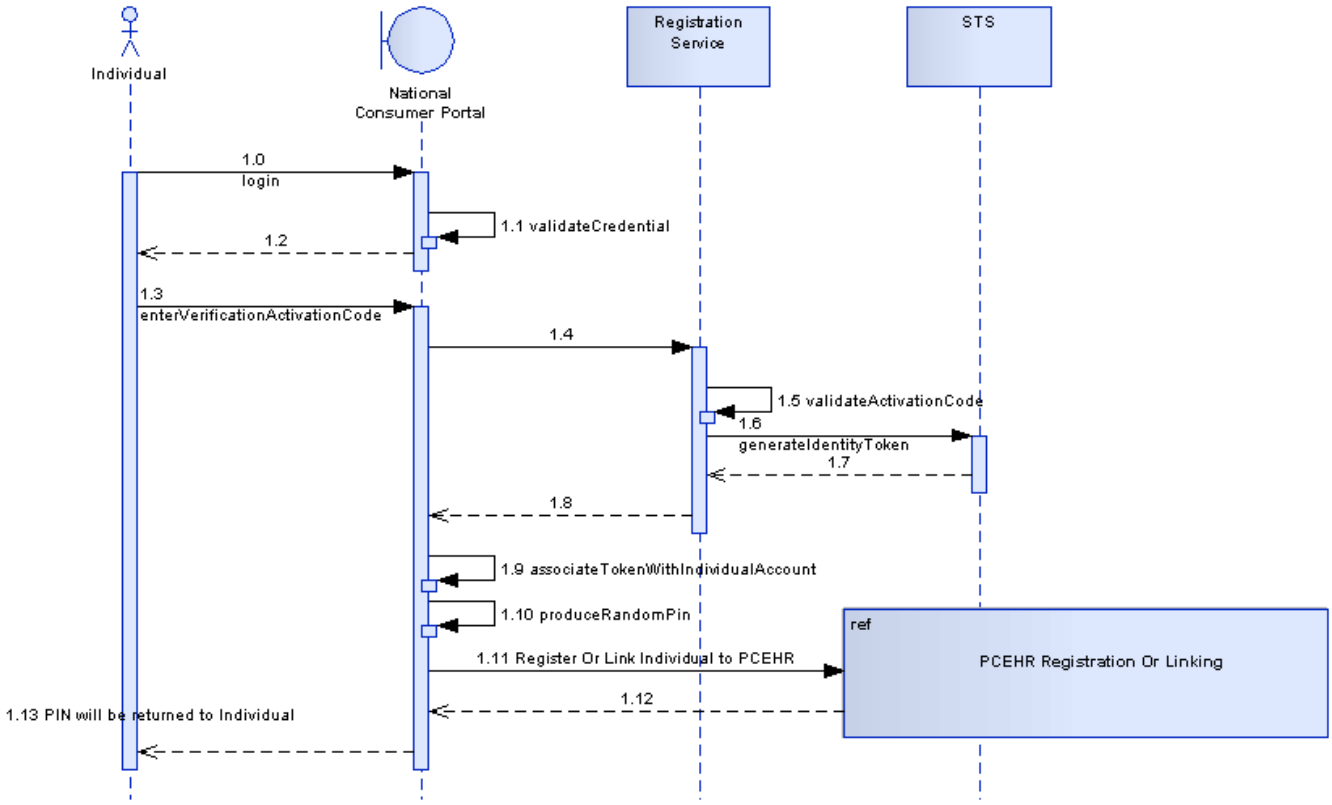


Figure 54: Linking a portal account to a PCEHR – Step 2

Logging in

The first step of the log in process is for the user to log locally into the portal and attempt to access the portal's representation of PCEHR functionality. If this log on is successful, the portal establishes a secure connection session with the PCEHR using the portal provider's certificate and providing both the identity token and the IHI of the individual.

An STS identity token may be protected by the use of a passphrase or personal identification number (PIN). Where this is the case, an appropriately encrypted version of the passphrase or PIN must be provided alongside the token.

Upon receiving a connection request, the PCEHR System must first validate the organisation's certificate. If connectivity level authentication is successful, the PCEHR System must then contact the STS to validate the PCEHR Managing Individual's Identity Assertion Token. The provider's organisational certificate, the individual's IHI and any optional PIN or pass code must match the details provided to the STS during registration. If this secondary level of authentication completes, the STS system returns a positive response.

If a positive response is received from STS, then the PCEHR System verifies whether the user is the PCEHR owning individual or a representative and a time-limited security access token appropriate to the role is returned to the clinical application. This token is specific to the given portal session and must be provided to the PCEHR System in all subsequent portal operations. While authentication processes differ considerably, the consumer and provider authorisation processes are identical.

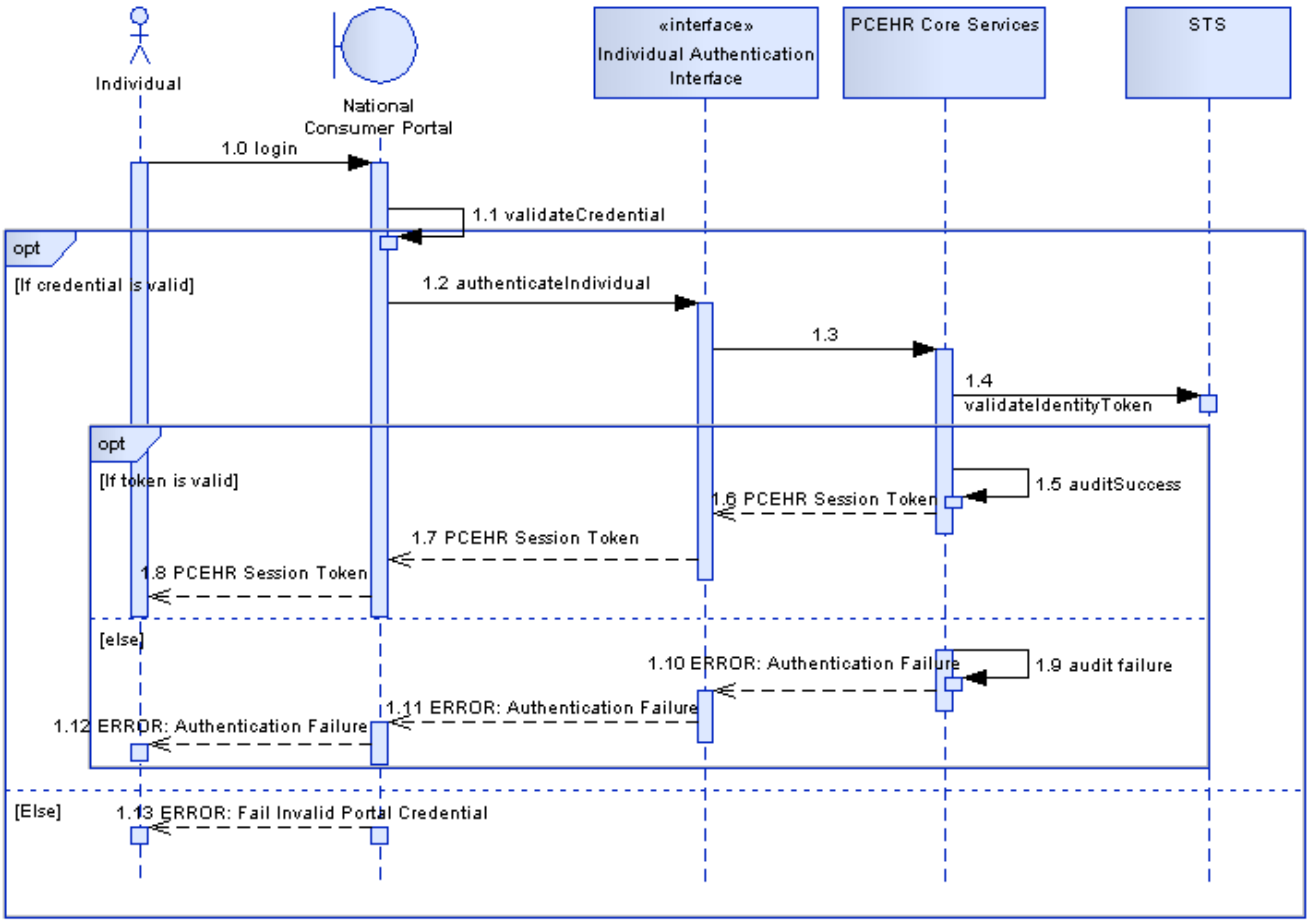


Figure 55: Consumer portal authentication

A further level of authentication may be required in order to perform certain pre-defined restricted operations. This process may be realised though a challenge-response mechanism. The challenge-response mechanism prompts the user to answer questions provided during registration or linked to the individual to verify their identity.

Although the questions will be rendered within the portal, the challenge response process will be managed by the PCEHR System (and STS). The consumer portal must not store or attempt to auto-populate the responses to a challenge.

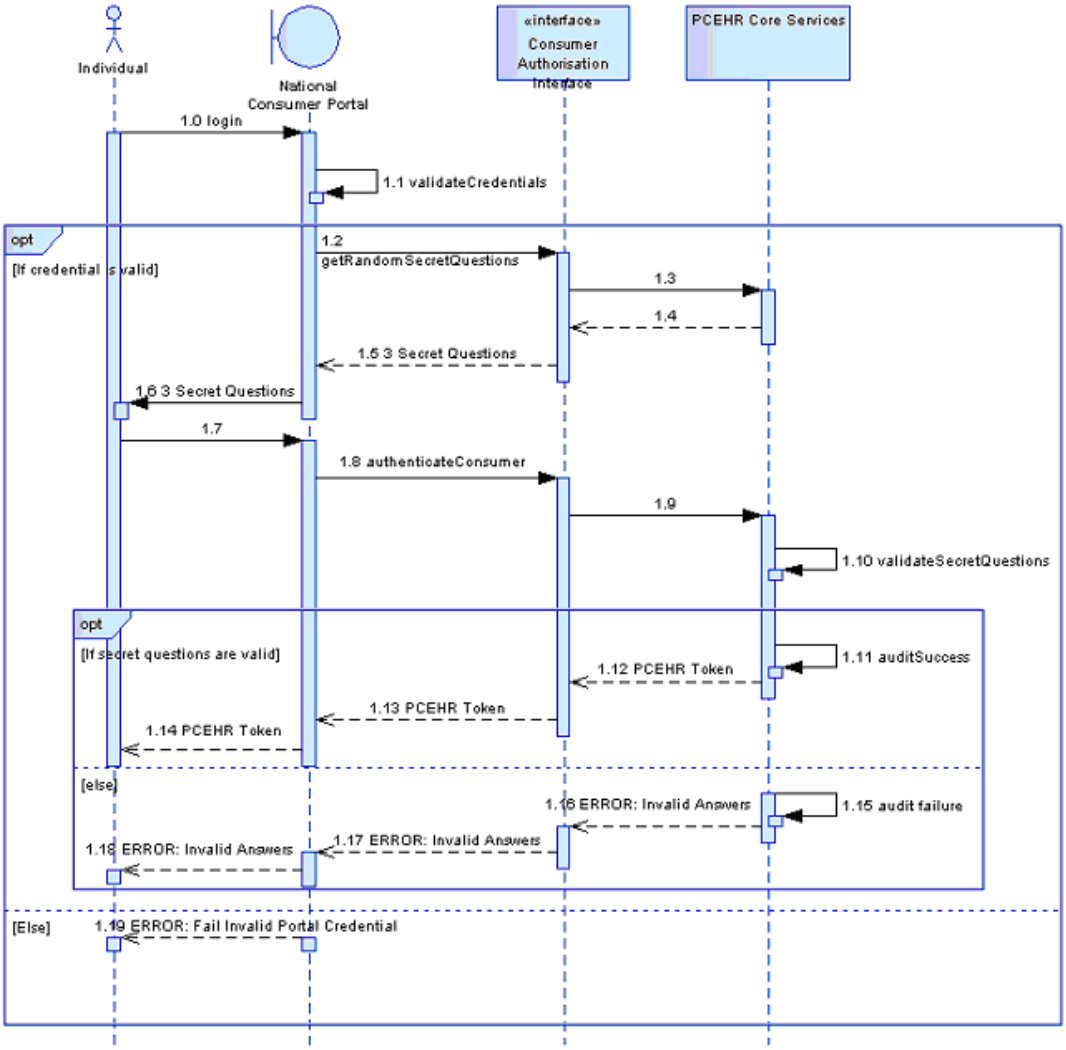


Figure 56: Additional secret questions

Key points:

- Users are locally authenticated by the portal.
- An identity token is used to link a portal identity to a specific PCEHR.
- The identity token is validated by the PCEHR System (using STS).
- Users may be further authenticated by the PCEHR System using a challenge response process.

3.1.4.13 Setting Consumer Access Controls

The PCEHR Managing Individual may set the access control levels associated with a PCEHR. Figure 57 outlines the key system interactions involved in completing this process.

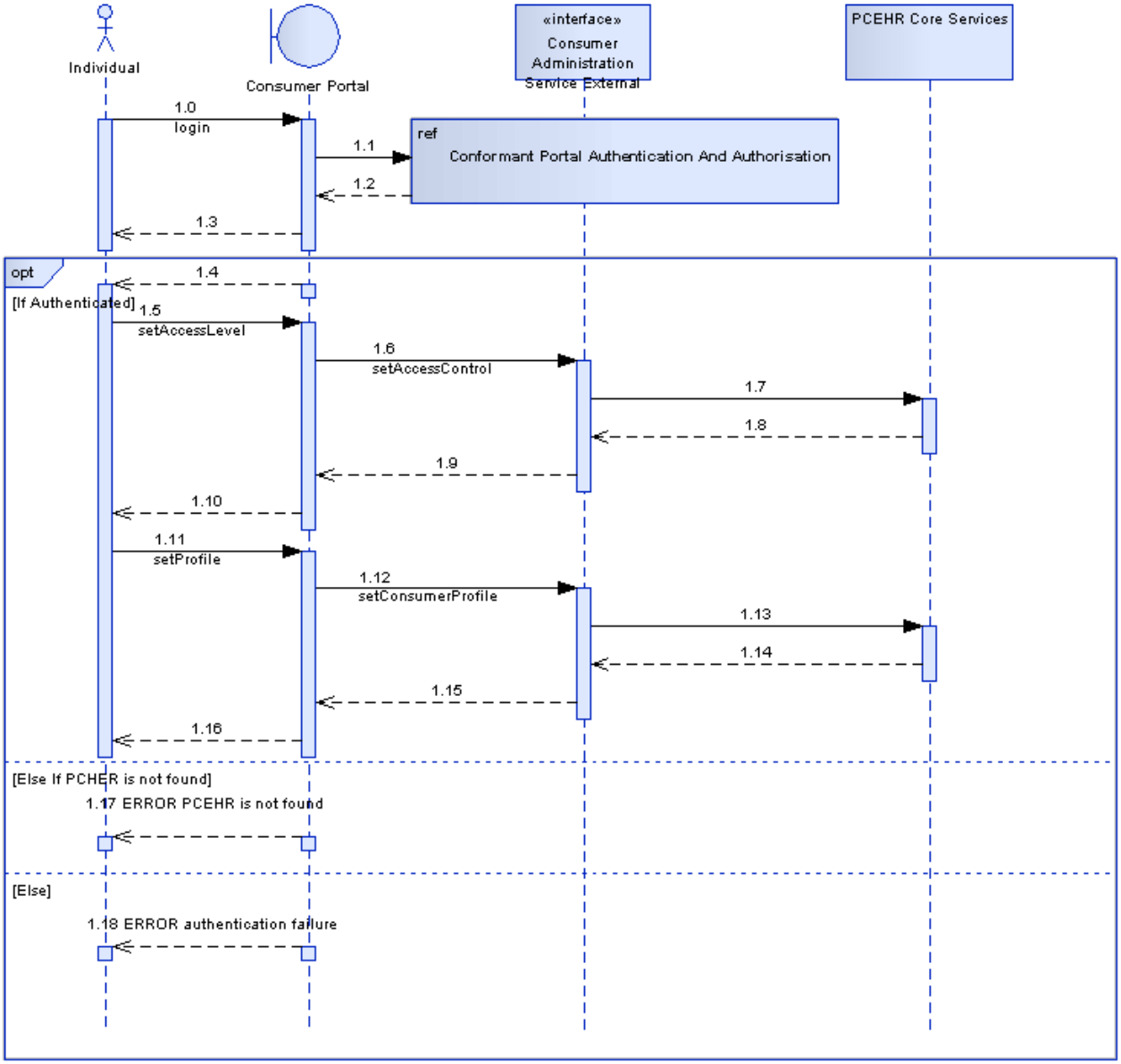


Figure 57: Setting consumer access controls

3.1.4.14 Setting a Nominated Representative

An individual may nominate a representative to access the PCEHR on their behalf. Figure 58 outlines the key system interactions involved in completing this process.

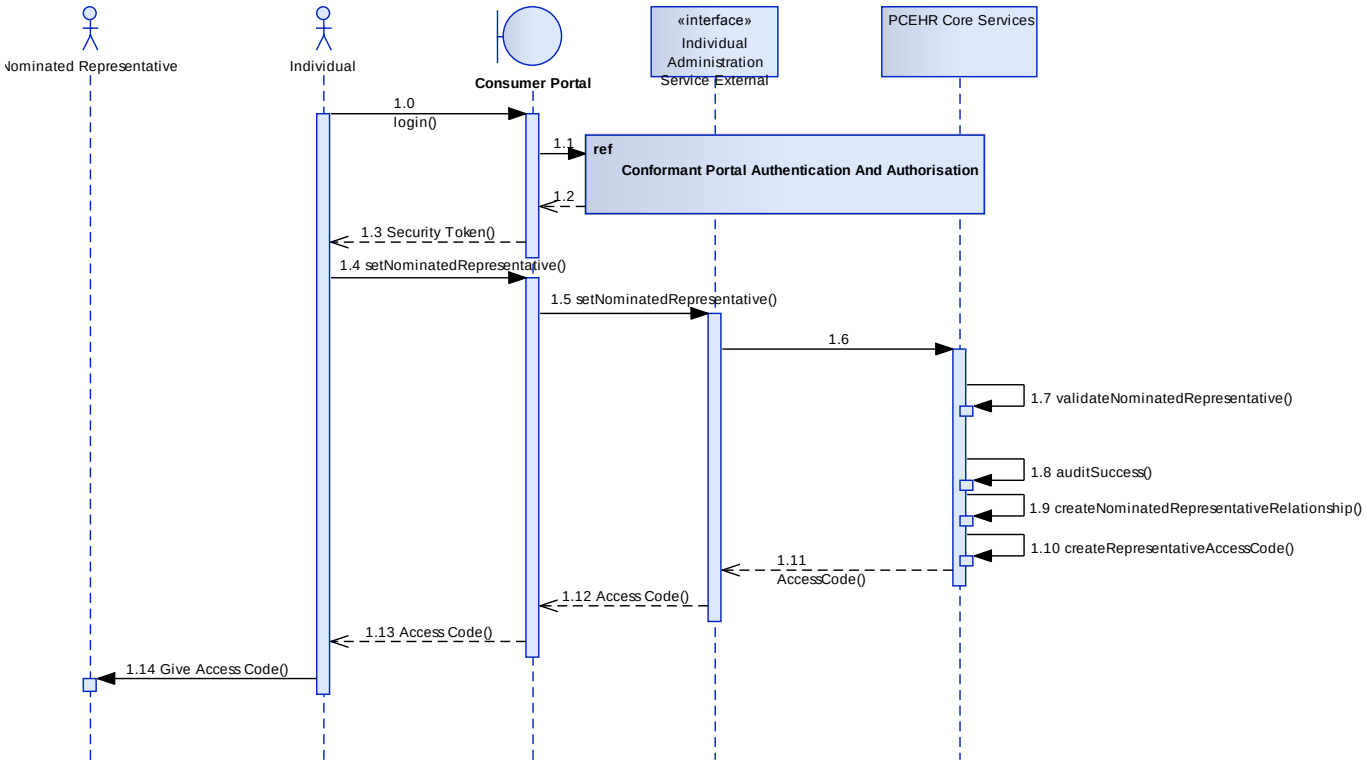


Figure 58: Set nominated representative

3.1.4.15 Accept Representative Nomination

Figure 59 outlines the process associated with an individual accepting the nomination to access another individual's PCEHR.

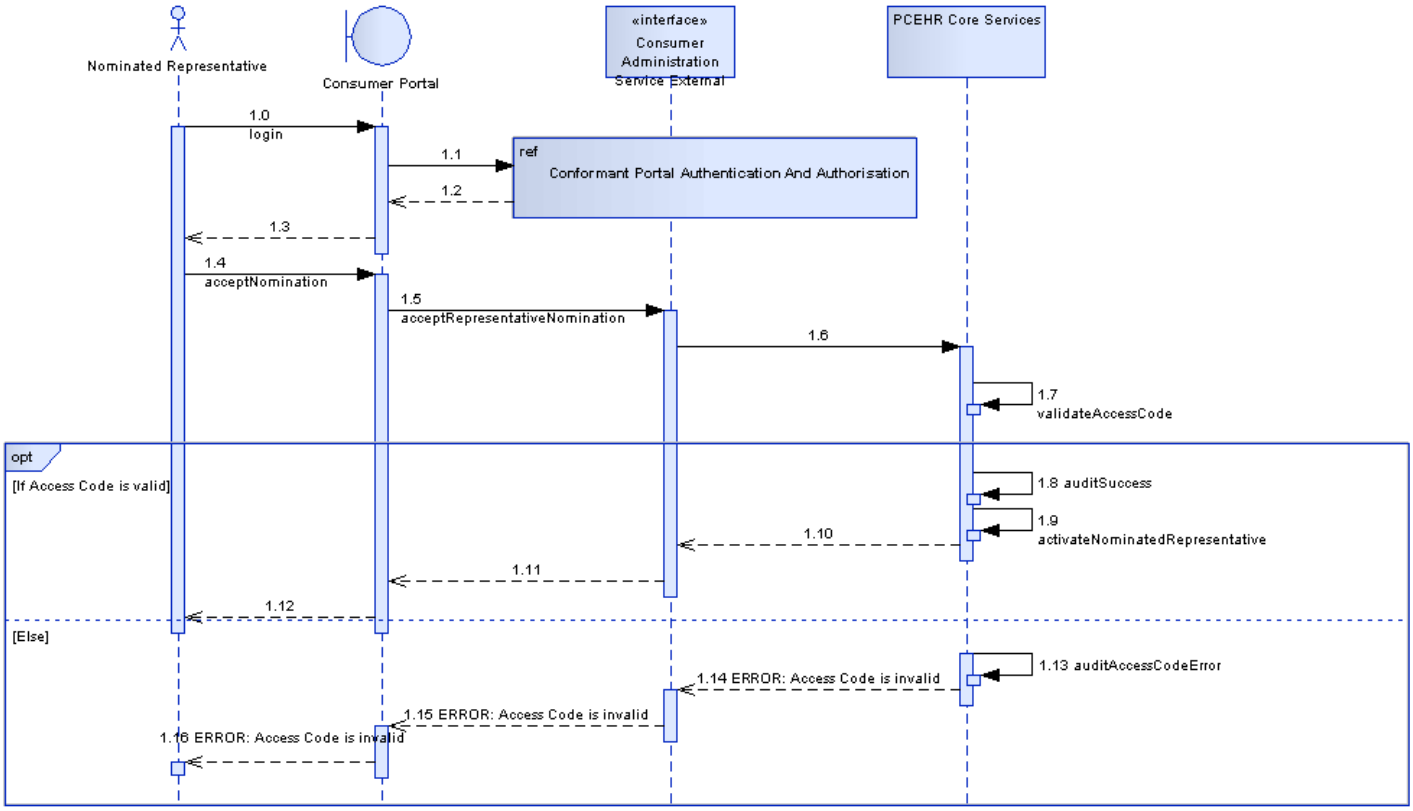


Figure 59: Accept nominated representative

Key points:

- The nominee must log into a conformant portal using their own credentials.
- The access code generated during the "Nominate a representative" must be entered into the portal and sent to the PCEHR System in order to associate the portal account with the individual's PCEHR.
- The access code is specific to the combination of the nominee's credentials and the specific PCEHR. It cannot be used to link other nominees to the PCEHR or to link the nominee to other PCEHRs.

3.1.4.16 Set Authorised Representative

This operation allows an appropriate individual to gain administration access for their dependent's PCEHR. The appropriateness of the relationship and the list of PCEHRs an individual may manage will be controlled by the PCEHR System and may be suggested to the user.

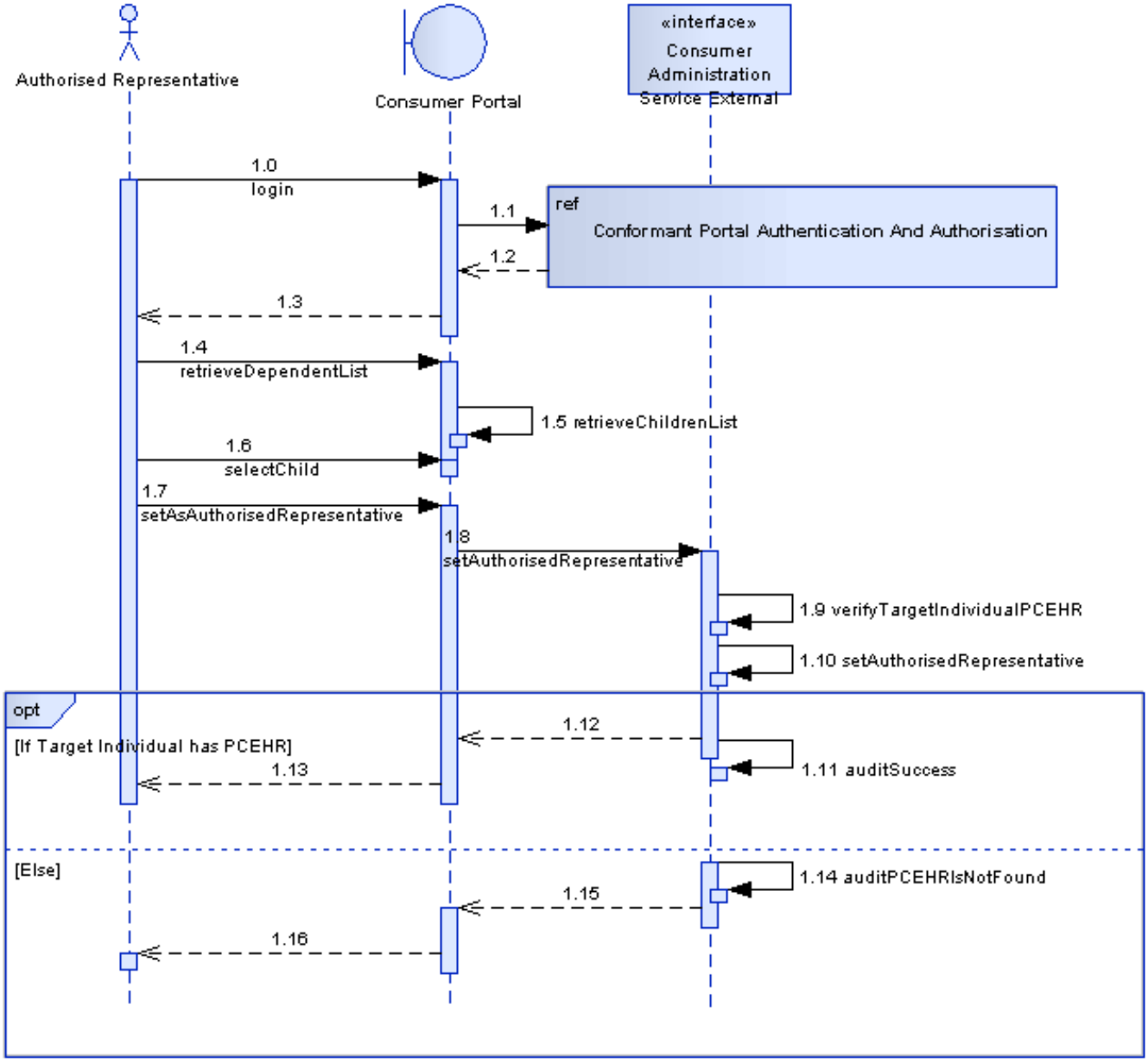


Figure 60: Set authorised representative

3.1.4.17 Managing Include and Exclude Lists

The PCEHR Managing Individual may manage the include or exclude lists associated with a PCEHR. These lists are used during the provider authorisation process for a given PCEHR. Figure 61 outlines the key system interactions involved in completing this process.

There are multiple ways by which this may be achieved. The process for performing this manually via the consumer portal is similar to the process for setting an access control or profile setting and is therefore not repeated here. The below diagram highlights the process involved with adding a user to the include list via the provision of a Provider Access Code.

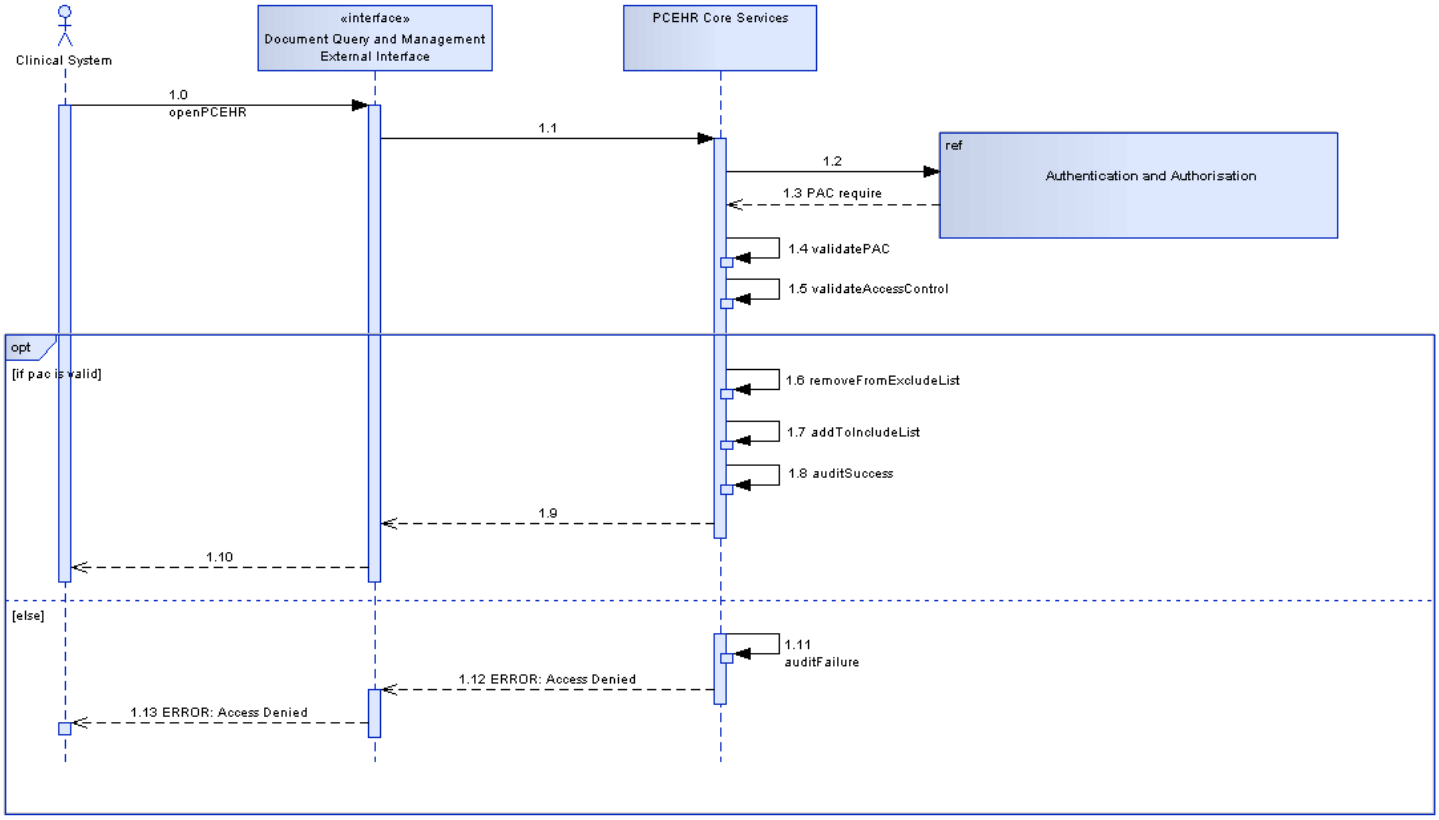


Figure 61: Adding a provider to the include list using a PAC

Key points:

- Access is granted or revoked at the organisation level.
- If an organisation on the exclude list presents a valid PAC, PAC-X or TAK for the PCEHR, or asserts that emergency access is required to the PCEHR, the organisation will be moved from the exclude list to the include list.
- If the PCEHR is set to "General Access" and the provider is on the exclude list, when a provider is given a PAC they will be added to the include list and also removed from the exclude list. This will mean that if the PCEHR is later set to "Limited Access" mode, the provider in question will still have explicit access.

3.2 Logical Information Viewpoint

The logical information viewpoint takes a deeper look into the key informational elements. Data elements are decomposed and the more technical relationships are exposed.

Formal design notation, specifically UML, is used extensively throughout this section.

3.2.1 Informational Elements

Table 3 lists the key data entities within the PCEHR. The entities are only modelled where there is a need to illustrate a concept or mandate a structure.

Table 3: Informational elements

Data Element	Comment	Modelled
PCEHR Unstructured Document	This is a document which has been added to the PCEHR without a guaranteed machine interpretable structure.	Y
PCEHR Structured Document	This is a document which has been added to the PCEHR with a guaranteed machine interpretable structure.	Y
Document Envelope	A wrapper to allow documents to be added to the PCEHR.	Y
Index Entry	A logical entity representing the internal list of documents (and associated metadata).	Y
View	A representation of data relating to a PCEHR.	Y
Atomic Data Model	A set of data elements extracted from one or more documents from within a single PCEHR.	Y
Health Summary	A summary of an individual's key health information maintained by a nominated provider.	N
Audit Entry	A log of a key system event relating to a specific PCEHR. This may be used to track access (including unsuccessful attempts) to a PCEHR.	N
Report Entry	Data item recording operational events. This is a logical entity and may be extracted from other data within the PCEHR (such as audit logs and the index).	N
Document Template	A logical construct holding the definition of a structured template, the means to validate instance documents, rendering definitions and other usage and guidance notes.	N

3.2.2 Data Access, Ownerships and Management

The below CRUD (Create, Read, Update, Delete) table shows the relationship between data users and the above data elements.

Table 4: Informational create, read, update, delete

CRUD Table	PCEHR Managing Individual	Author	Provider	Nom. Provider	PCEHR System	PCEHR Sys Admin	Provider CIS	Template Service
PCEHR Unstructured Document	R, D	C, R, D	R (also acts as an author)	R (also acts as an author)				
PCEHR Structured Document – Clinical	R (human readable sections only), D	C, R, D (with support of a CIS)	R (with support of a CIS)	R (with support of a CIS)	R		C, R	
PCEHR Structured Document - Consumer Entered Information	C, R , D	(See PCEHR managing Individual)	R	R	R		R	
Document Envelope					R	R	C	
Index Entry					C, R, U, D	C, R, U, D		
View	R	R	R	R	C, U, D		R	
Atomic Data Model					C, R, U, D			
Shared Health Summary	R	See Nom. Provider	R	C, R, U, D	R		R	
Audit Entry	R	See Provider	R	See Provider	C	R	R	
Report Entry					C	R		
Document Template					R		R	C, R, U

Key points:

- The Atomic Data Model is internal to the PCEHR System.
- Views may only be modified by the PCEHR System.
- The PCEHR System cannot read unstructured documents.
- Providers may view audit data relating to their access to a PCEHR.
- Individuals can read and logically delete clinical documents but they cannot edit them.
- Message envelopes are only used by the CIS and PCEHR Systems.

Table 5: Information entity usage and size

Data Element	Retention Period	Add to PCEHR or Update Frequency	Get From PCEHR or Read Frequency	Avg Size	Max Size.
PCEHR Unstructured Document	Life of system	Once (per version)	V. Low	Moderate	Enormous
PCEHR Structured Document	Life of system	Once (per version)	V. Low	Moderate	Enormous
Document Envelope	None	N/A	N/A	V. Small (excl. document)	Small
Index Entry	Life of document	Once	Medium	V. Small	Small
View	None (although caching may be used to aid performance)	Medium	Medium	Moderate	Moderate
Atomic Data Model	Life of the PCEHR	Medium	Medium	Moderate	Large
Shared Health Summary	Life of system	Low	Medium	Small	Moderate
Audit Entry	60 Months	High	Low	V. Small	Small
Report Entry	60 Months	High	V. Low	V. Small	Small
Document Template	Life of system	Rarely	V. High	Small	Moderate

The above table uses the following categories for modification frequency. All read/write frequency figures are for individual entities (e.g. for a specific index entry rather than the set of index).

- Rarely – Generally no more than once every few months.
- V. Low – Generally no more than once a day.
- Low – Generally no more than once an hour.
- Medium – Generally no more than once every few minutes
- High – Generally no more than once every few seconds
- V. High – Many times per second.

The above table uses the following categories for data sizes:

- V. Small < 500KB
- Small < 1MB
- Moderate < 10 MB
- Large < 100MB
- V. Large < 1GB
- Huge < 10GB
- Enormous > 10GB (and into petabytes).

3.2.3 Document Query and Management

3.2.3.1 PCEHR Document Envelope

The message envelope is a container for holding a clinical document and the associated metadata.

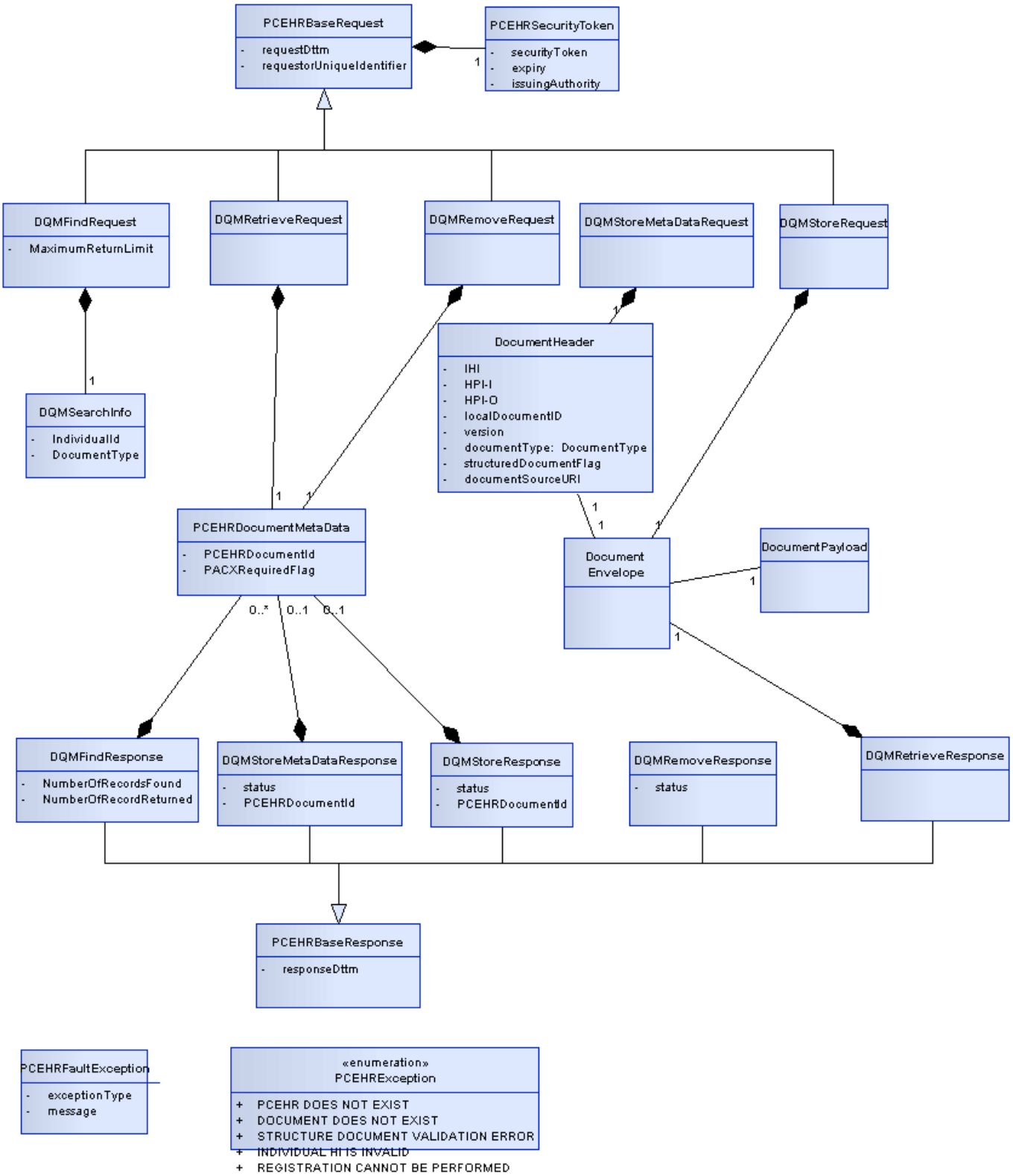


Figure 62: PCEHR document envelope - logical view

Table 6 describes each of the entities within the drawing.

Table 6: Document envelope entities

Entities	Notes
PCEHRBaseRequest	Common request and security information
PCEHRBaseResponse	Common response and security information
DQMFindRequest	Find Operation Request information which contain search keywords and maximum record limit
DQMFindResponse	Find Operation Response information which contain Number of records found, number of records return and PCEHR document metadata
DQMRemoveRequest	Remove Operation information which contain document information
DQMRemoveResponse	Remove Operation Response information to indicate operation success or failure
DQMRetrieveRequest	Retrieve Operation information which contain document information
DQMRetrieveResponse	Retrieve Operation Response information which contain document
DQMStoreMetaDataRequest	Store Meta Data Operation information which contain the document header and metadata
DQMStoreMetaDataResponse	Store Meta Data Operation Response information to indicate operation success or failure and PCEHR document metadata
DQMStoreRequest	Store Operation information which contain the document
DQMStoreResponse	Store Operation Response information to indicate operation success or failure and PCEHR document metadata

Key points:

- A document envelope contains both the document and the associated metadata.
- The document envelope does NOT describe the service action to be performed and it is assumed that there will be an additional level of service specific wrapping. Some examples of the service level requests and responses are shown in the diagram.

3.2.4 Index Data

A document management system typically needs to maintain a list of documents within the system along with supporting associative and descriptive data.

This document set or list is referred to as the index. Figure 63 shows the key information entities associated with a PCEHR specific index.

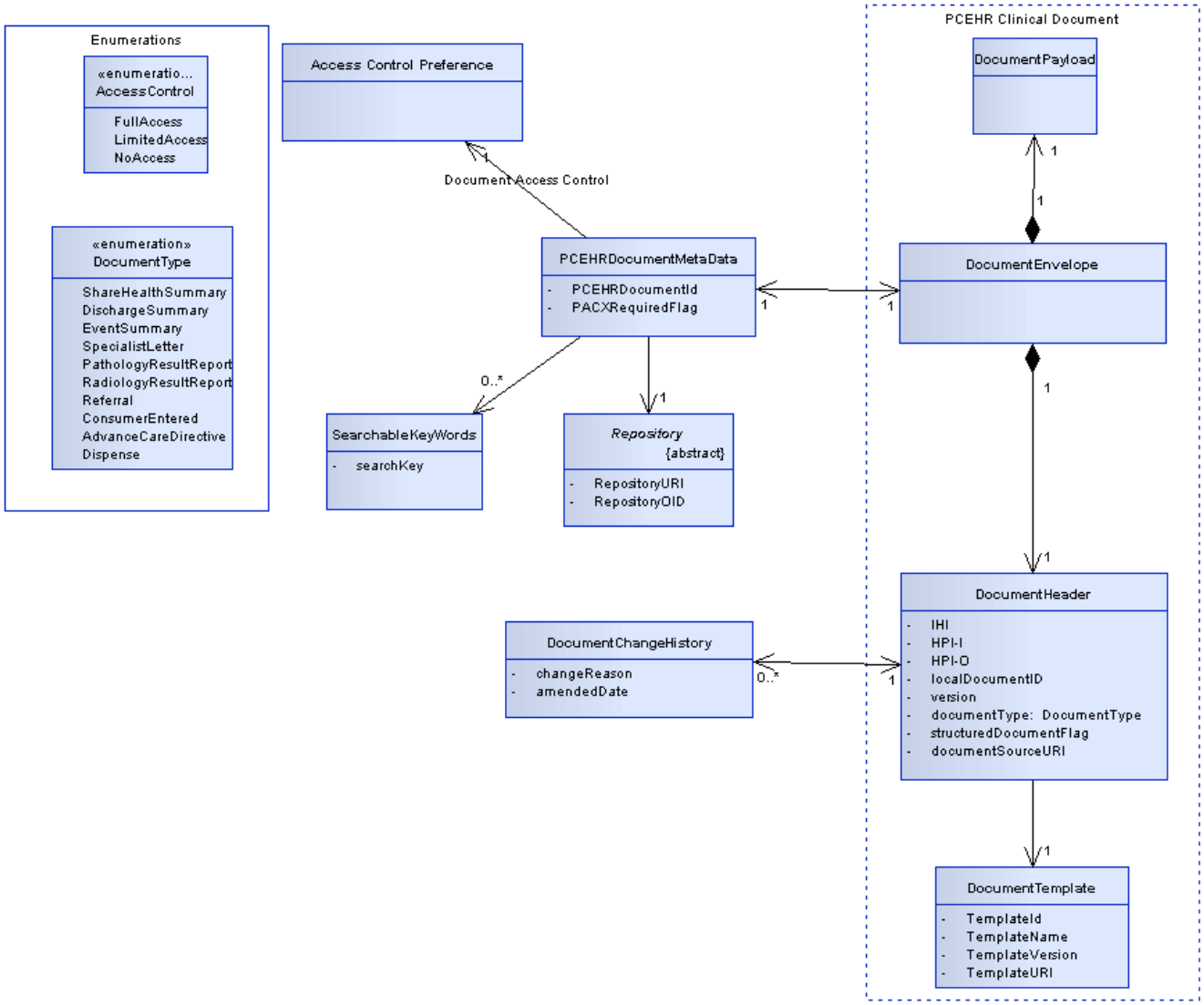


Figure 63: Logical index data

Table 7: Logical index entities

Entity	Notes
PCEHRDocumentMetaData	PCEHR Document Index which contains PCEHR document ID and document access settings
SearchableKeywords	Search keywords
AccessControlPreference	Access control settings
Repository	Repository information
DocumentHeader	Document header which contains the author, individual, document type, etc.
DocumentEnvelope	PCEHR clinical document
DocumentPayload	Document payload i.e. CDA or CCA
DocumentTemplate	Document template reference
AccessControl	Access control enumeration
DocumentType	Document type enumeration

Key points:

- A document index entry may also be associated with multiple searchable key words. Searches may also span any index or atomic data. Due to the distributed nature of document storage, there is no requirement for searches to directly search document content.

3.2.5 Atomic Data

Structured documents may be parsed to extract individual data items. These items are referred to as atomic data elements. The atomic data model is a representation of key atomic data elements extracted from one or more documents.

The atomic data model is an internal construct and is never exposed to any user. However views derived from this data (such as the consolidated view) may be exposed externally.

It is essential that the link to the original source document is maintained to ensure that any associated data elements are removed when a document is logically deleted. Each data element must also map back to the access control level of the parent document. Any views created form the atomic data model must be sensitive to the access rights of the user and the access control level associated with each data element (these are relative to the document the element is retrieved from and cannot be directly altered at the atomic level).

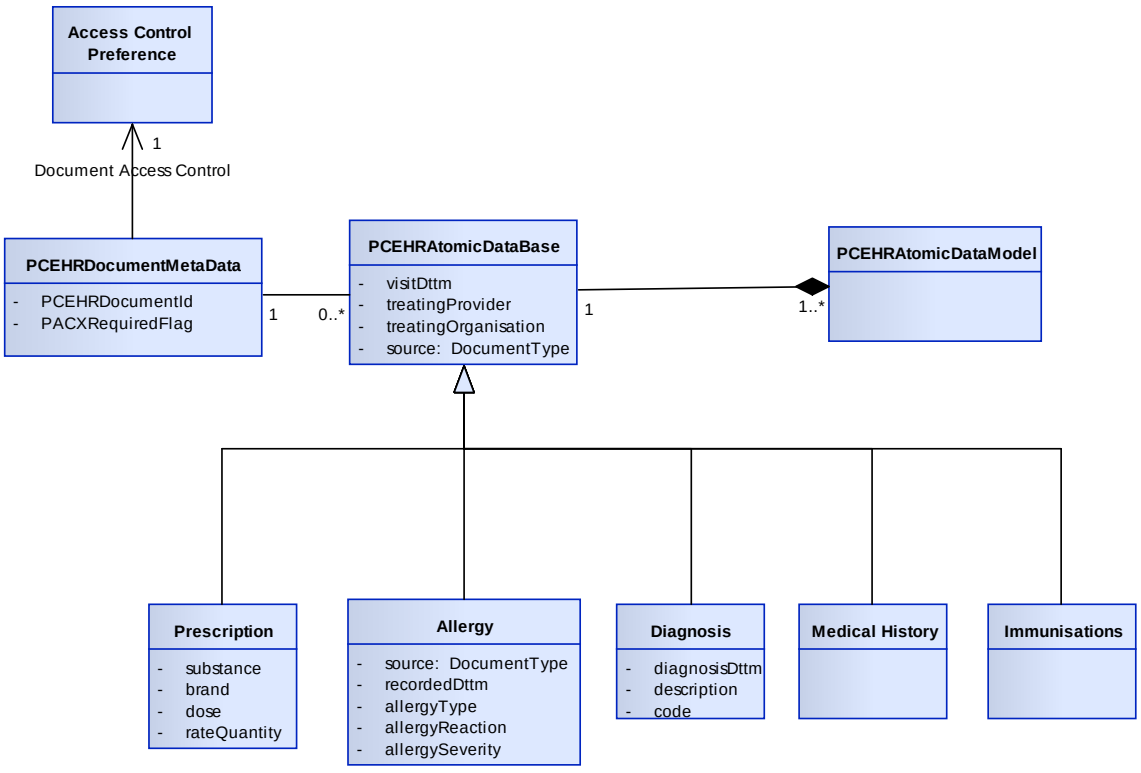


Figure 64: Logical atomic data

Table 8: Atomic data entities

Entity	Notes
PCEHRAtomicDataModel	The Atomic Data Model
PCEHRAtomicBase	An atomic data element. This forms the basis of all elements within the atomic data model.
Diagnosis	Diagnosis information – medical history
Prescription	Prescription (medicines) information
Allergy	Allergy/adverse reaction information
Medical History	Data items relating to individual's medical history
Immunisations	Data items relating to immunisations

Key points:

- Each atomic data element is relatable back to the document it came from.
- This link allows the system to relate the atomic data element to an access level.
- When source documents are logically deleted, the source of the data element must also be deleted. Where a data element has no remaining sources, the data element must be removed.
- If the document is reinstated the data element should be reinstated.

3.2.6 Views

A view is a representation of data related to a specific PCEHR. The view may utilise any centrally managed data elements including index data, change histories, the atomic data model and approved Medicare data sources.

All views must only be created from content which is appropriate for the target audience. For example, if a provider with general access requests a view, the returned view item must not contain any items derived from sources marked as being restricted to Limited or No Access.

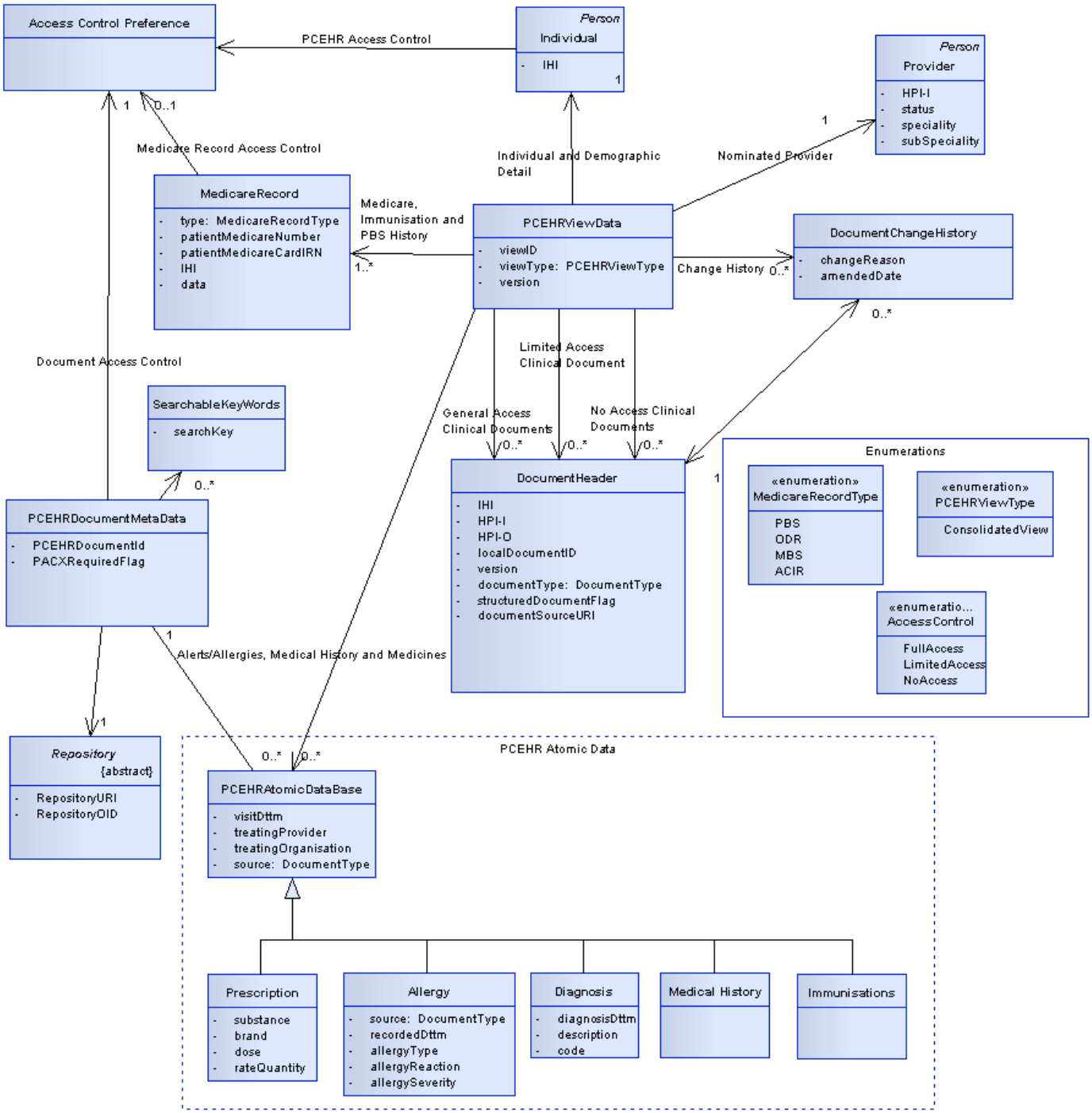


Figure 65: Logical data view

Table 9: Logical view entities

Attribute	Notes
Provider	Healthcare Provider
Individual	Patient
AccessControlPreference	Access Control settings
MedicareRecord	Medicare information e.g. ACIR, ODR, MBS,PBS
PCEHRViewData	PCEHR view raw data
PCEHRAtomicData	
Repository	Repository information
SearchableKeywords	Search keywords
PCEHRDocumentMetaData	PCEHR Document Index
DocumentHeader	Document header which contains the author, individual, document type, etc.
MedicareRecordType	ACIR, ODR, MBS, PBS, etc.
PatientEncounter	Patient (individual) interaction with healthcare providers
Diagnosis	Diagnosis information – medical history
Prescription	Prescription (medicines) information
Allergy	Allergy/adverse reaction information
AccessControl	Access control enumerations
PCEHRViewType	PCEHR view type enumerations
Medical History	The individual's medical history
Immunisation	The individual's immunisation details

Key points:

- Views are created from multiple sources and provide a PCEHR-wide representation.
- Views will not cover more than one PCEHR (for example to provide a family view).
- Multiple views may be added to meet future needs. The view process must be created so that the creation of new views can be done rapidly and at minimal cost.
    - An XSLT may be used to provide a platform independent rendering of the view (with the obvious exception of the XML format). It is strongly encouraged that Clinical System vendors provide a mechanism for displaying the content of all views in a generic manner. Significant effort may be required where systems need to map the view format onto internal data model for use in internal CIS screens (in this instance the view becomes a clinical document message rather than a rendering of data).

3.2.7 Documents

A document within the PCEHR System may be either structured or unstructured. A structured PCEHR document is defined as a document for which a machine readable data definition exists within the national Template Service.

Each document within the PCEHR will be associated with a globally unique identifier (likely an OID). Where a document is stored externally, the document may also have an identifier local to the external conformant repository. The index is responsible for storing the mapping between the two elements.

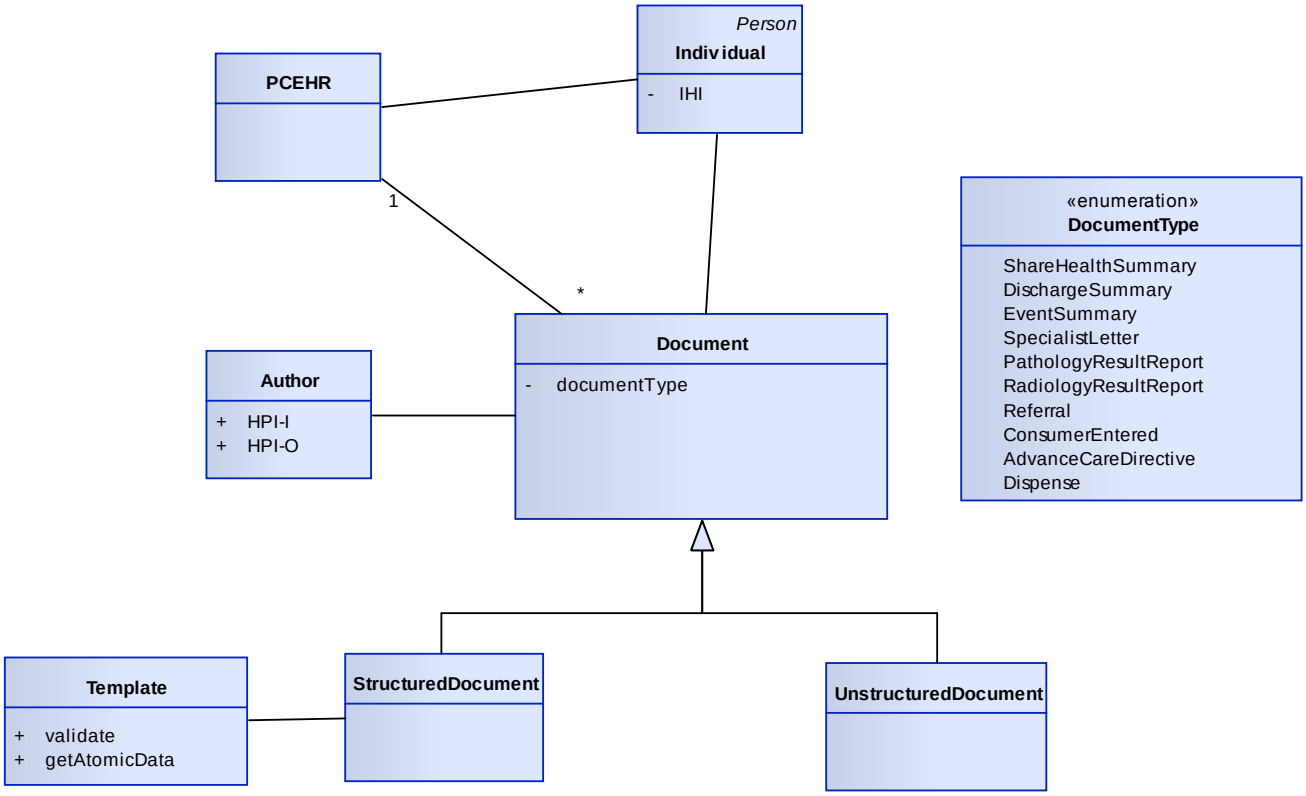


Figure 66: PCEHR document

Key points:

- A document has an author. Authors are granted special permissions for the documents they have produced. As authorisation only applies at the organisation level, this access control is inherited by the author's organisation.
- Documents may be structured or unstructured.
- The level and type of structure is defined by an external template. All structured documents must conform to at least one template.

3.2.8 Relationships Between Information Entities

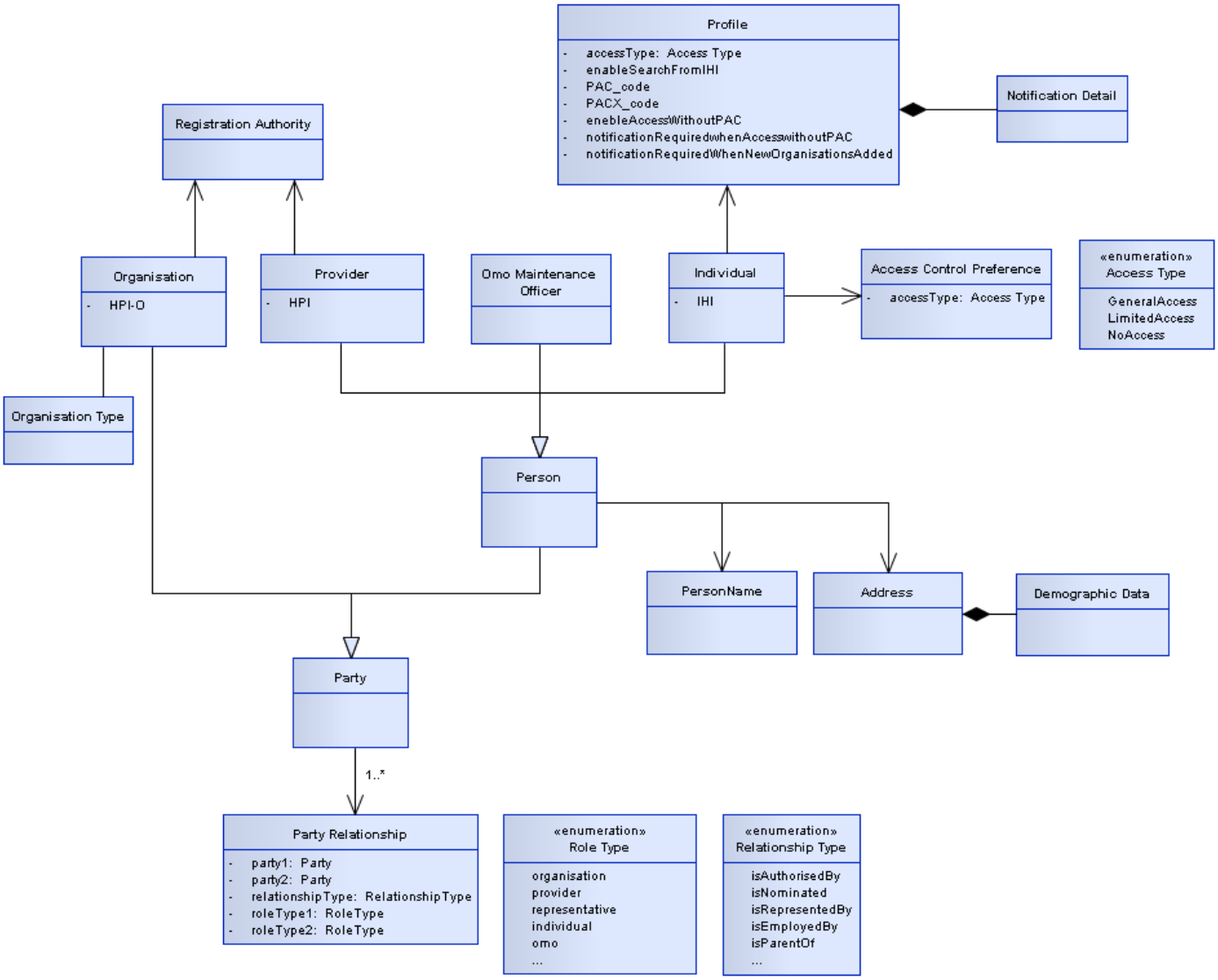


Figure 67: Entities and parties

The section below outlines the relationships between informational entities within a PCEHR. Each informational entity may be logically related to one or more entities in multiple ways. Various mechanisms may be used to display these relationships including class diagrams (with associations\classes) and entity relationship diagrams. The diagram below uses the OMG Party Specification originally proposed by Rumbaugh, Booch and Jacobsen in [OMG_PARTY_SPEC].

Party	Party Role	Party Relationship	Party Role	Party	Description
Modern Medical Group	Organisation	isAuthorisedBy	Individual	Mr John Wilson	Modern Medical Group is one of Mr John Wilson's authorised organisations.
Modern Medical Group	Organisation	isParentOf	Organisation	Brooker Medical Clinic	Brooker Medical Clinic is a part of the Modern Medical Group.
Dr. Stephen Antony	Provider	isEmployedBy	Organisation	Brooker Medical Clinic	Dr. Stephen Antony is employed by Brooker Medical Clinic.
Alana Lubikova	OMO	isEmployedBy	Organisation	Brooker Medical Clinic	Alana Lubikova is an OMO at Brooker Medical Clinic.
Brooker Medical Clinic	Organisation	isAuthorisedBy	Individual	Mr John Wilson	Brooker Medical Clinic is one of Mr John Wilson's authorised organisation. (added into include list)
Collins Place Medical Clinic	Organisation	isNotAuthorisedBy	Individual	Mr John Wilson	Collins Place Medical Clinic is one of Mr John Wilson's not authorised organisation. (added inot exclude list)
Dr. Stephen Antony	Provider	isNominatedBy	Individual	Mr John Wilson	Dr. Stephen Antony is Mr John Wilson's nominated provider.
Mrs Paulina Gonzales	Representative	isNominatedBy	Individual	Mr John Wilson	Mrs Paulina Gonzales is Mr John Wilson's nominated representative.
Ronaldo Da Silva	Representative	isAuthorisedBy	Individual	Ronaldinho Junior Da Silva	Ronaldo Da Silva is Ronaldinho Junior Da Silva's authorised representative.

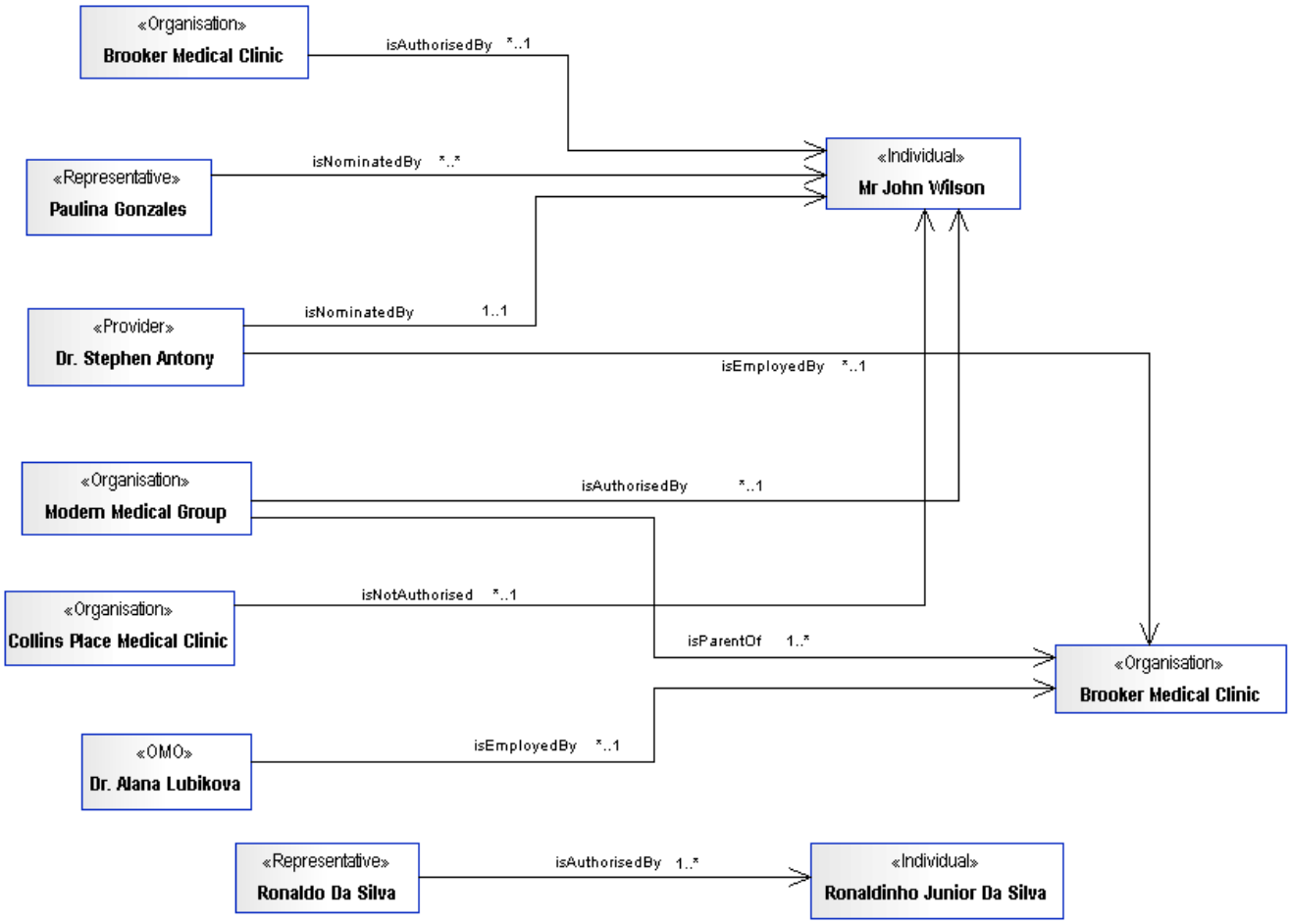


Figure 68: Party relationships

The above diagram shows the key relationships within a PCEHR. The stereotype (<< stereotype >>) within each box specifies the entity name and the bold text gives an example. Arrows indicate directional relationships.

Key points:

- An individual may nominate a provider to manage their health summary.
- A PCEHR may be managed by either the individual or an authorised representative.
- An individual may authorise a provider to view their PCEHR.
- A provider is employed by one or more organisations.
- An individual may have more than one authorised and/or nominated representatives.

3.2.8.1 Nominated Provider

Individuals will have the option of nominating a healthcare provider to manage their Shared Health Summary and to ensure that other healthcare providers accessing the individual's PCEHR have access to a clinically moderated summary of the individual's allergies/adverse reactions, medicines, medical history and immunisations. Only the nominated provider may update an individual's Shared Health Summary.

The nominated provider can either be an individual healthcare provider or a healthcare organisation. If the nominated provider is a healthcare organisation, any healthcare provider authorised by that organisation may, if they are providing health services to the individual, update the individual's Shared Health Summary.

The establishment of a nominated provider can only occur in a consultation between the provider and the individual involved and requires the agreement of both parties. An individual may have zero or one nominated providers.

3.2.8.2 Authorised Representative

For the purposes of managing an individual's PCEHR, an individual may be represented by one or more authorised representatives. These relationships will be recorded in an individual's PCEHR.

There are a range of existing laws and arrangements in place to support individuals who are deemed not to have the capacity to act on their own behalf or the capability to communicate their wishes.

Authorised representatives will be able to represent individuals without capacity to act for themselves in their interactions with the PCEHR System. The authorised person will be given the same access and controls as the individual. There may be more than one authorised person for an individual.

Except where special circumstances exist, parents (or other authorised representatives) will have control of their children's PCEHR from 0 to 14 years, including the decision as to whether the child participates or withdraws, as well as managing their access controls.

After a child turns 14 years old the PCEHR System will enable the child to choose to manage their own PCEHR, including the capacity to participate, withdraw, manage their access controls or disassociate representatives.

3.2.8.3 Nominated Representative

An individual or their authorised representative may also appoint a nominated representative. A nominated representative is typically a family member, carer or other person who helps manage their care. A nominated representative may view records to which they have explicitly been given access in the individual's PCEHR, but they do not have the ability to manage PCEHR information or provide consent on behalf of the individual.

3.2.8.4 Include List

An include list is a logical construct holding the identifiers of the healthcare organisations that currently have access to view the PCEHR.

3.2.8.5 Exclude List

An exclude list is a logical construct holding the identifiers of the healthcare organisations that have been explicitly denied access to view a PCEHR.

Appendix A Sample Technical Service Design

A.1 Introduction

This section does not attempt to mandate or constraint the system implementation or the core component interactions in any way.

It provides technical advice and guidance only, demonstrating a possible implementation approach.

A.2 The Approach

The following sections outline how individual services may be used to realise given operations.

The specification does not attempt to constrain the technical realisation or to specify service coordination methods.

No assumption is made as to the use of an orchestration engine, event driven messaging bus or shared choreography.

The services shown represent the key services identified in [PCEHR_CON_OPS] and are intentionally limited to those building blocks which may be re-used in other eHealth initiatives.

No attempt is made to describe implementation-specific technical services that would not offer wider eHealth re-use (such as validation services, ESBs, etc.).

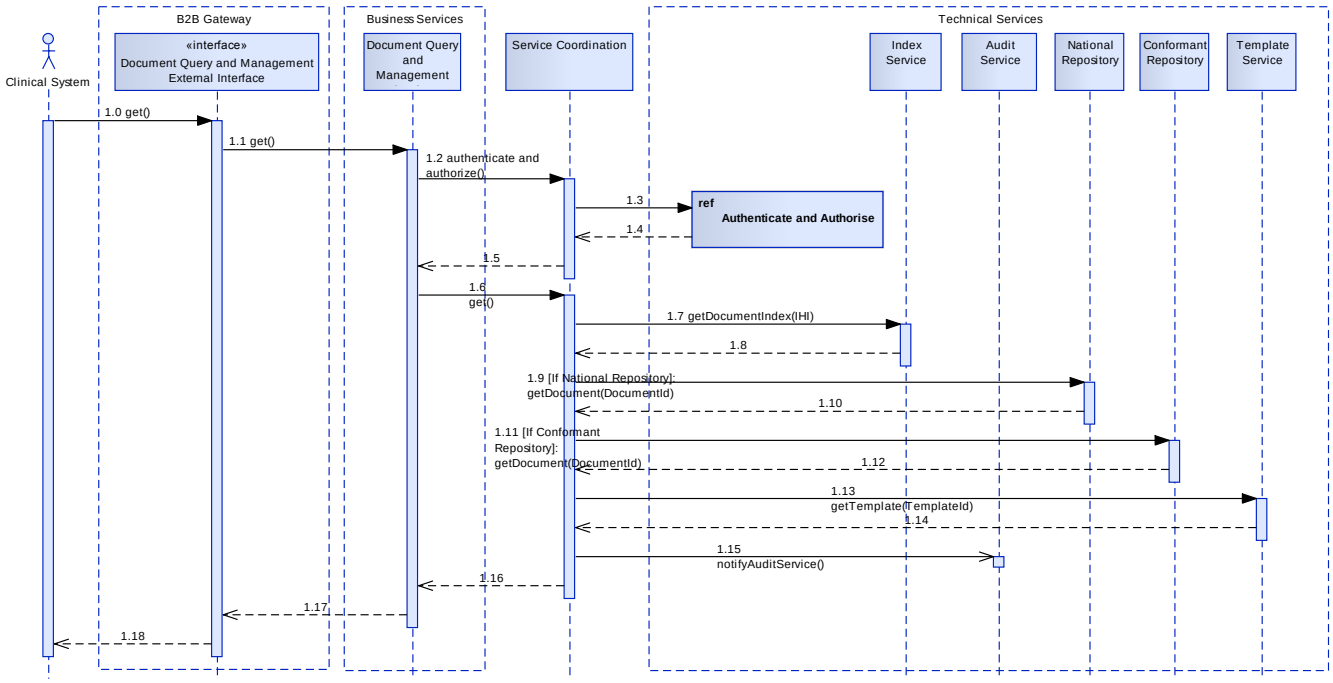
In all cases, the description is meant to define a possible logical process and a further mapping onto an implementation.

Key points:

- Only those services which may be re-used across eHealth areas are explicitly defined.
- The Document Query and Management (DQM) Service directly performs the business service specific tasks (such as validation). This is a logical view and the technical realisation may use further technical services to support common operations.
- The service co-ordination layer is used to logically group multiple calls across entity services.
- Direct inline dependent calls from one service to another are minimised.

A.3 DQM – Get

The Document Query and Management Get operation is used to retrieve exactly one document. The below sequence diagram shows the high level component interactions required to achieve this process.

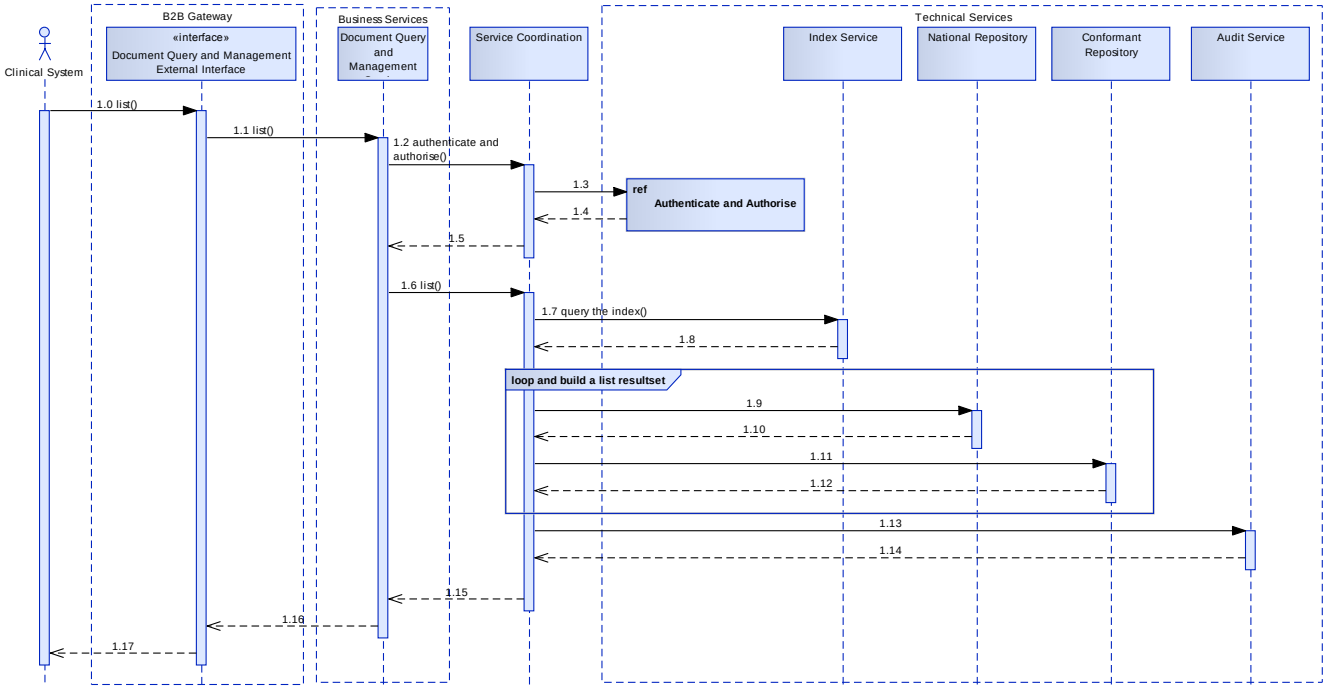


Key points:

- The client interface is compliant with the RLUS Get definition.
- The view service is not involved in the rendering of the document.
- The identifier of the associated template is returned (but not the template itself).

A.4 DQM – List

The Document Query and Management List operation is used to retrieve one to many documents (zero documents would be treated as an error). The below sequence diagram shows the high level component interactions required to achieve this process.

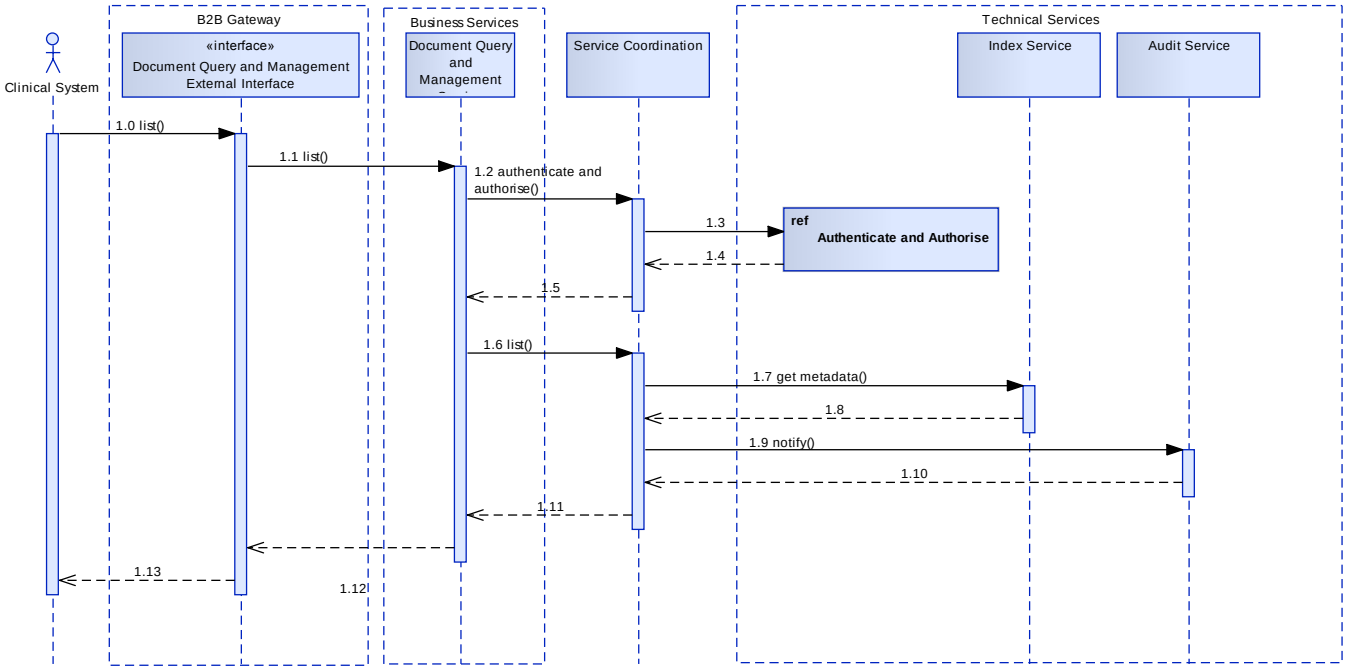


Key points:

- The client interface is compliant with the RLUS List definition.
- The view service is not involved in the rendering of the documents.
- The identifier of the associated template is returned (but not the template itself).
- The operation returns a set of documents rather than pointers to documents.

A.5 DQM – Locate

The Locate operation is used to find one or more documents matching a specified set of search criteria. The operation returns one to many pointers to documents and the limited metadata required to understand key document attributes such as type, creation date and location.

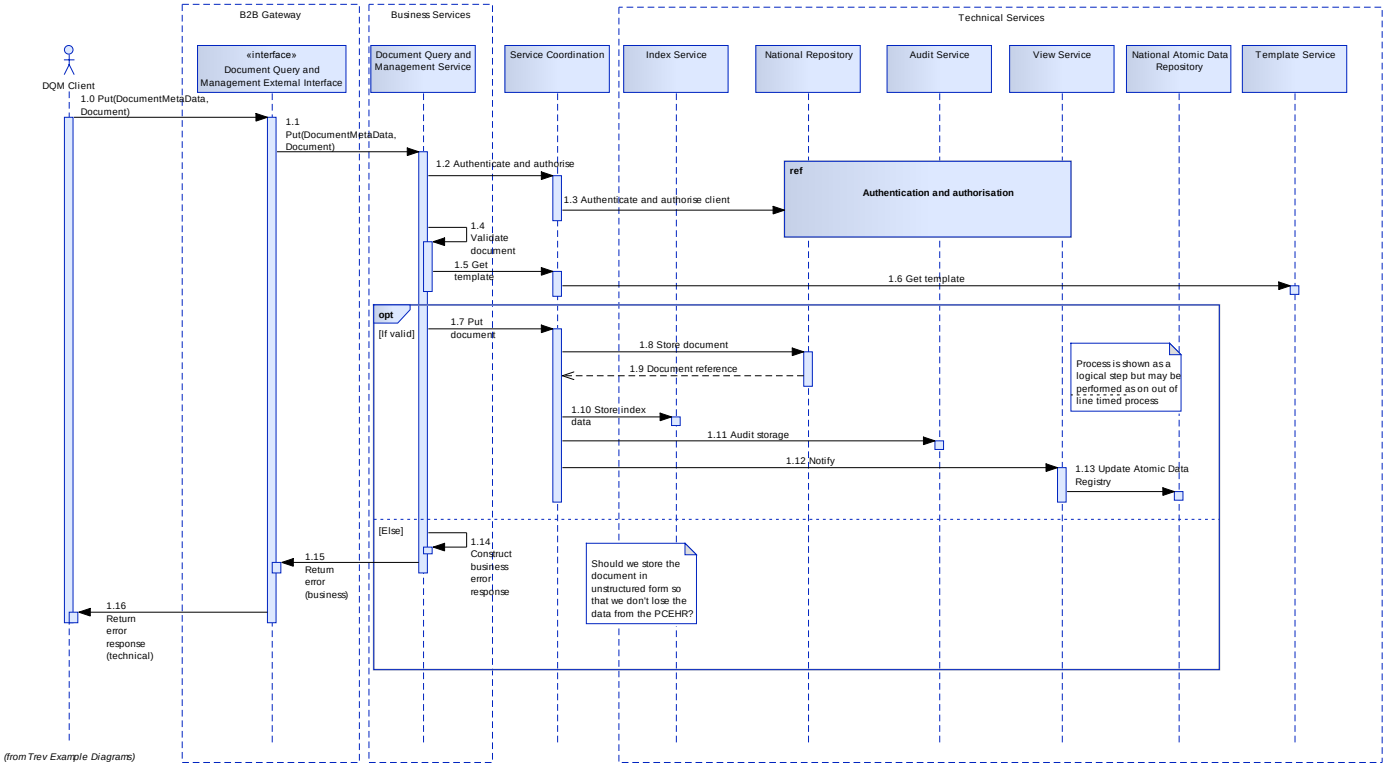


Key points:

- The client interface is compliant with the RLUS List definition.
- The operation returns a set of document pointers and associated metadata rather than documents.

A.6 DQM – Put

The Put operation is the principal mechanism used to add a document to the National Repositories. It is anticipated that documents will be added to other Conformant Repositories directly and that an initialize call will be made to copy the metadata into the PCEHR System.

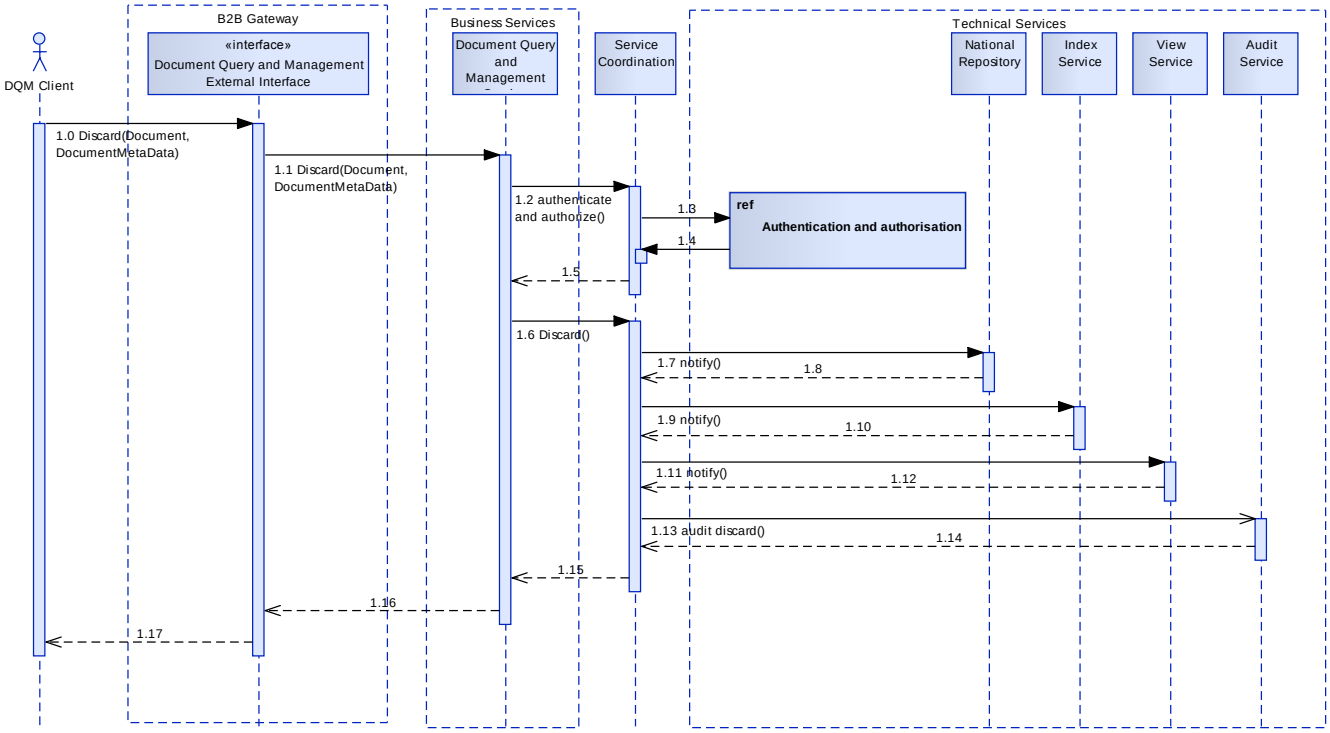


Key points:

- The client interface is compliant with the RLUS Put definition.
- If a document fails validation it is not added to the PCEHR System or underlying repository.

A.7 DQM – Discard

The discard operation is used to logically remove a record from a PCEHR. Due to medico-legal restrictions, it is unlikely that the document will be physically removed, however it may be removed from all physical views of the PCEHR.

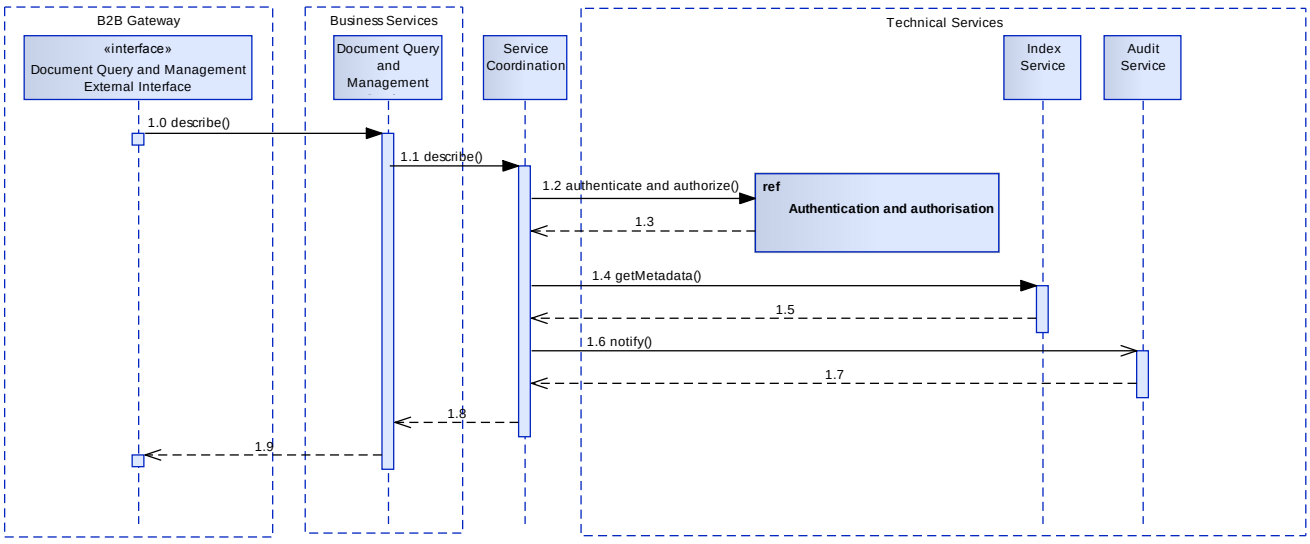


Key points:

- The client interface is compliant with the RLUS Discard definition.

A.8 DQM – Describe

The describe operation is used to retrieve the metadata associated with a given entry. In effect it extracts the index metadata stored for a given record.

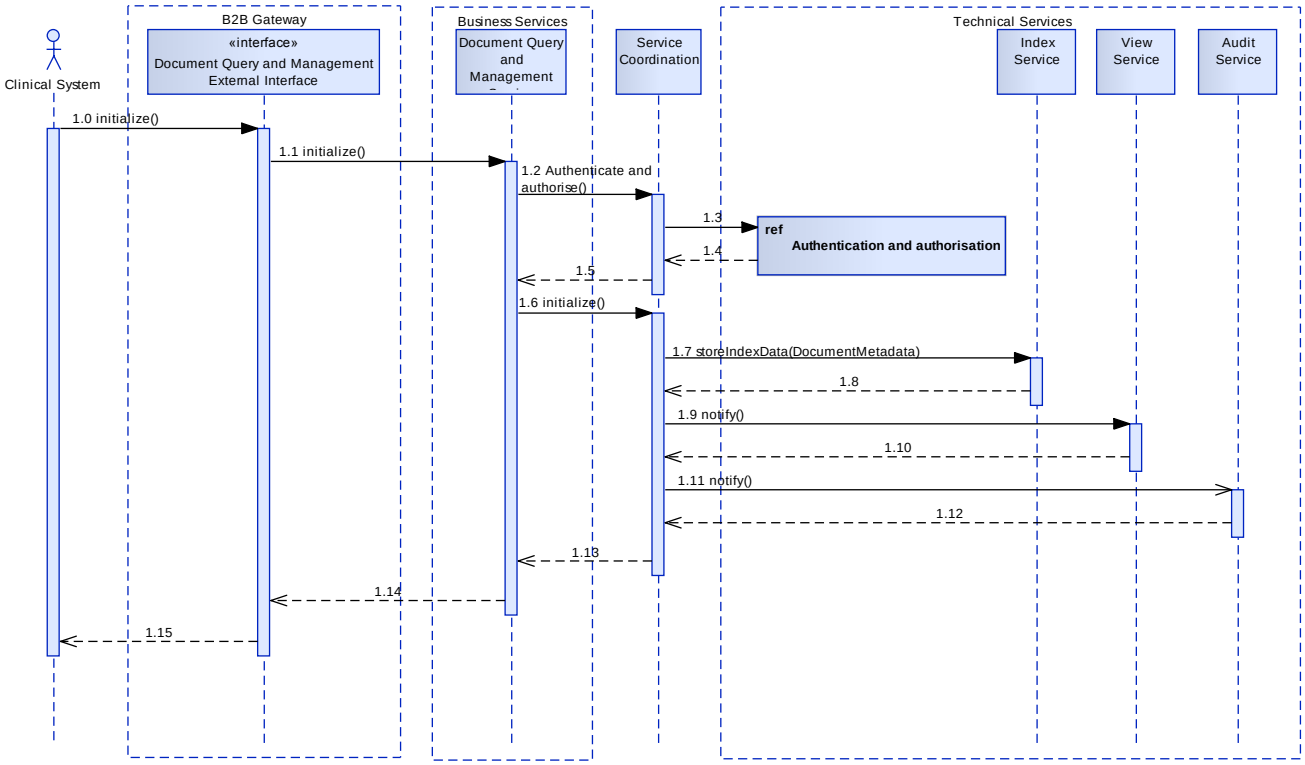


Key points:

- The client interface is compliant with the RLUS Describe definition

A.9 DQM – Initialize

The initialize operation is used to populate the required system metadata (largely the index data) where a document is added directly to a conformant repository.



Key points:

- The client interface is compliant with the RLUS initialize definition.
- The data required to populate the Index is passed directly to the service.

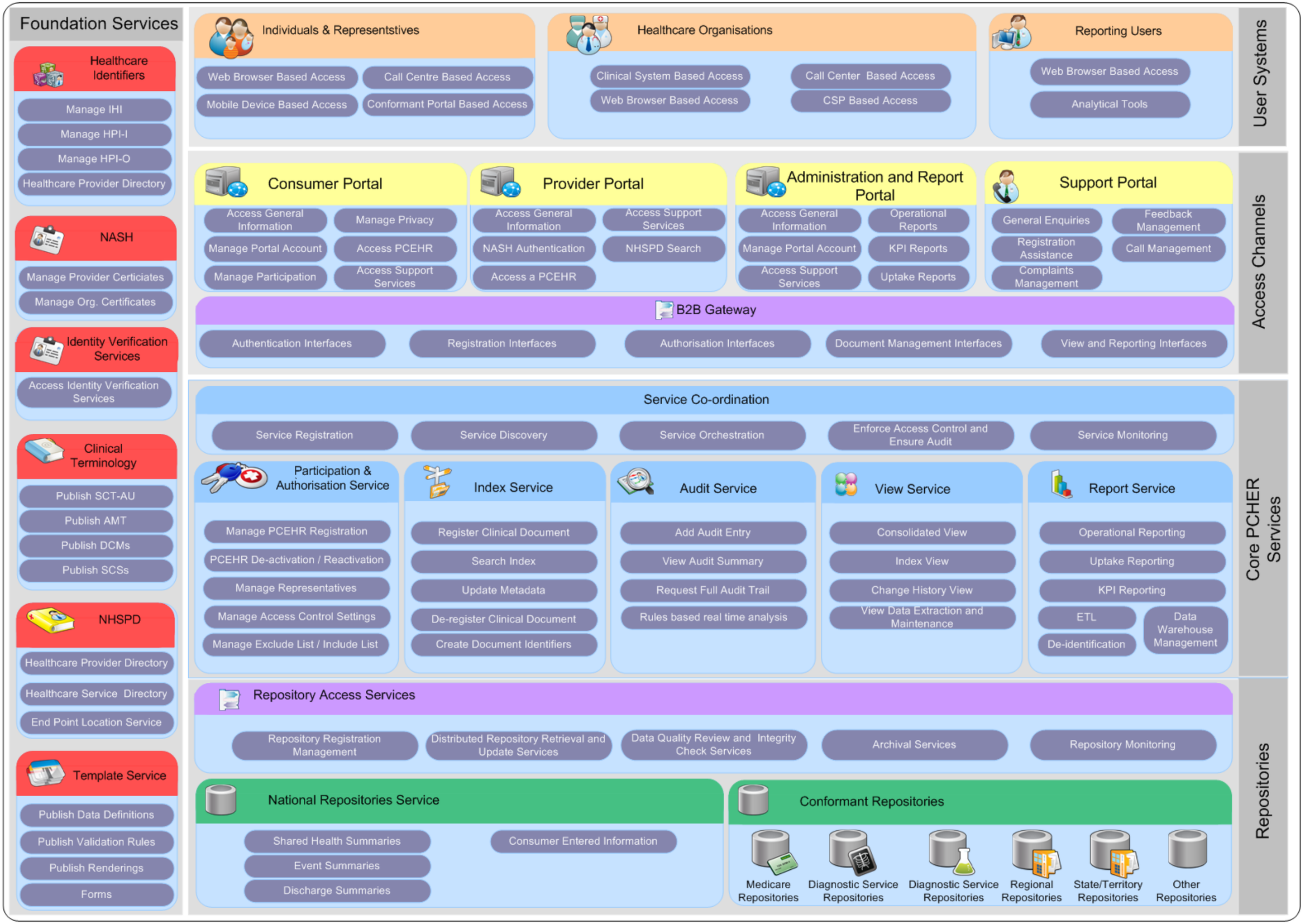
Appendix B References

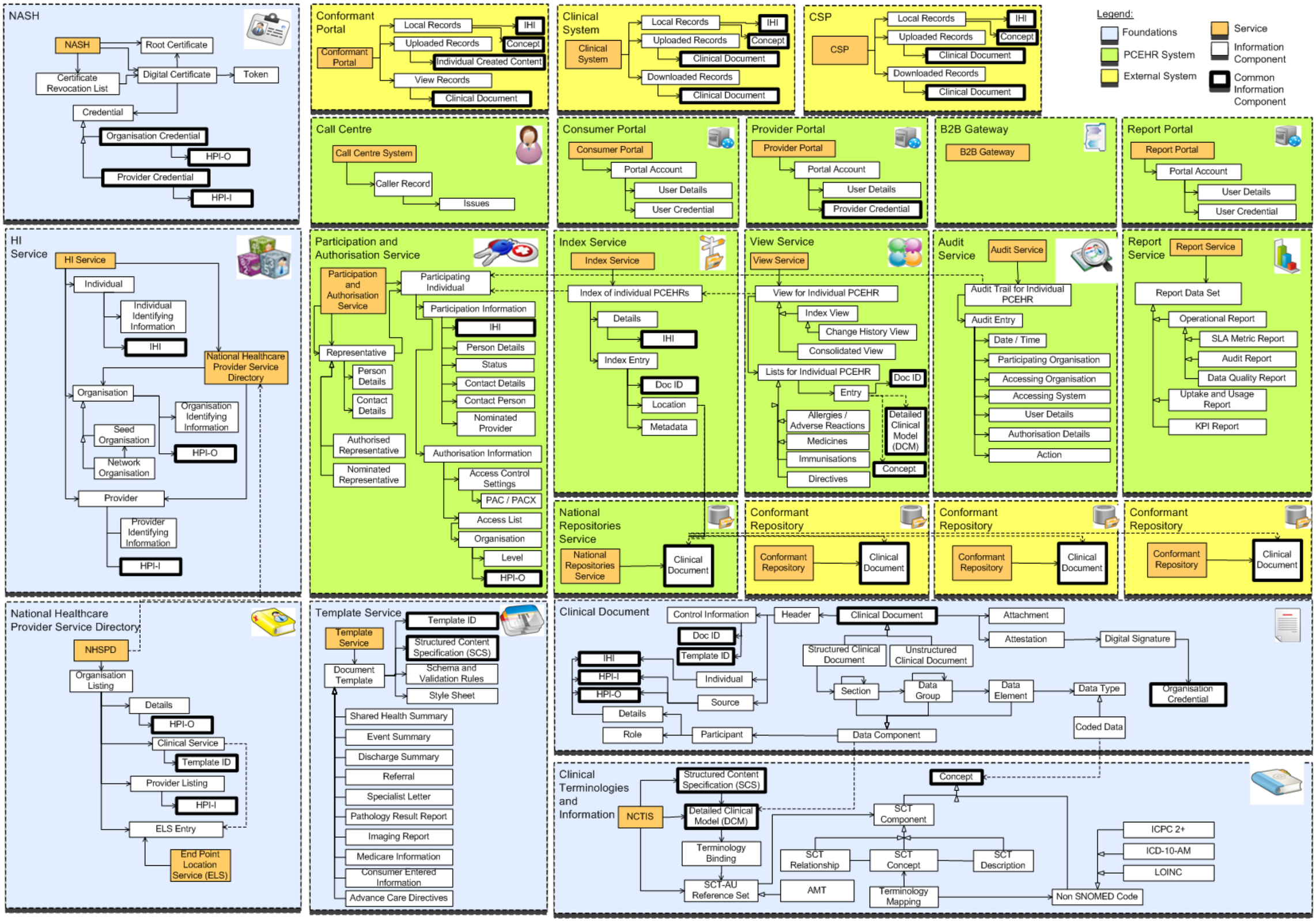
Tag	Name	Version Release/ Date
[NEHTA2010e]	National E-Health Transition Authority, E-Discharge Summary Package, Release 1.1, October 2010. http://www.nehta.gov.au/e-communications-inpractice/ edischarge-summaries	Release 1.1, October 2010.
[OMG_PARTY_SPEC]	http://www.omg.org/spec/PARTY/1.0	V 1.0, February 2001
[PCEHR_CON_OPS]	PCEHR Concept of Operations	0.13.6 April 2011
[PCEHR_HIGH_LEVEL_REQS]	PCEHR System - Business Requirements	1.0 06/05/2011
[RACGP2010]	Royal Australian College of General Practitioners, Standards for General Practices	4th Edition, October 2010.
[PCEHR_SYSTEM_GLOSSARY]	PCEHR System - Glossary	1.0 6/05/2011

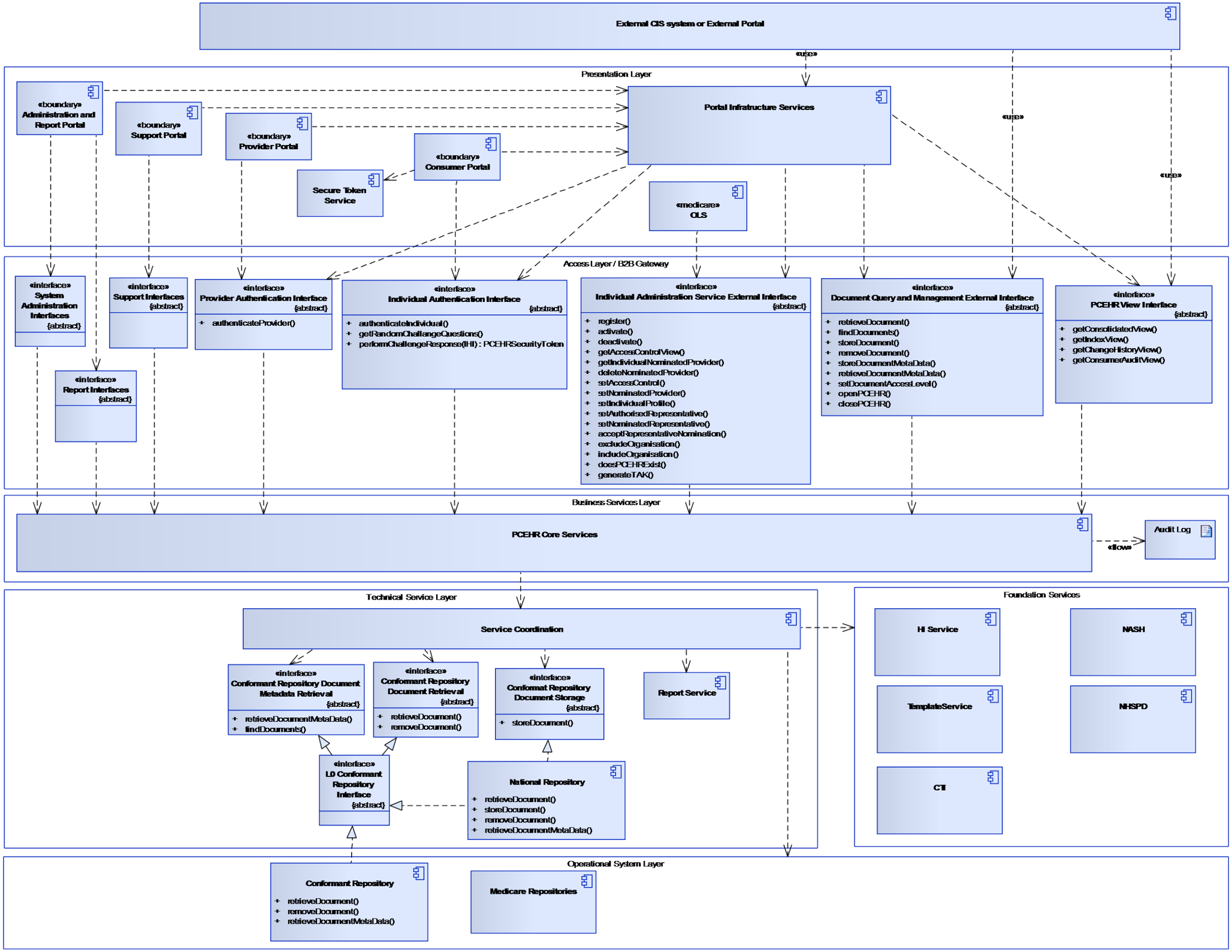
Appendix C Large Diagrams

The following pages contain A3 versions of key diagrams

.


Foundation Services
Healthcare Identifiers
Manage IHI
Manage HPI-I
Manage HPI-O
Healthcare Provider Directory
NASH
Manage Provider Certiciates
Manage Org. Certificates
Identity Verification Services
Access Identity Verification Services
Clinical Terminology
Publish SCT-AU
Publish AMT
Publish DCMs
Publish SCSs
NHSPD
Healthcare Provider Directory
Healthcare Service Directory
End Point Location Service
Template Service
Publish Data Definitions
Publish Validation Rules
Publish Renderings
Forms
Individuals & Representstives
Web Browser Based Access
Call Centre Based Access
Mobile Device Based Access
Conformant Portal Based Access
Healthcare Organisations
Clinical System Based Access
Call Center Based Access
Web Browser Based Access
CSP Based Access
Reporting Users
Web Browser Based Access
Analytical Tools
User Systems
Consumer Portal
Access General Information
Manage Privacy
Manage Portal Account
Access PCEHR
Manage Participation
Access Support Services
Provider Portal
Access General Information
Access Support Services
NASH Authentication
NHSPD Search
Access a PCEHR
Administration and Report Portal
Access General Information
Operational Reports
Manage Portal Account
KPI Reports
Access Support Services
Uptake Reports
Support Portal
General Enquiries
Feedback Management
Registration Assistance
Call Management
Complaints Management
B2B Gateway
Authentication Interfaces
Registration Interfaces
Authorisation Interfaces
Document Management Interfaces
View and Reporting Interfaces
Access Channels
Service Co-ordination
Service Registration
Service Discovery
Service Orchestration
Enforce Access Control and Ensure Audit
Service Monitoring
Participation & Authorisation Service
Manage PCEHR Registration
PCEHR De-activation / Reactivation
Manage Representatives
Manage Access Control Settings
Manage Exclude List / Include List
Index Service
Register Clinical Document
Search Index
Update Metadata
De-register Clinical Document
Create Document Identifiers
Audit Service
Add Audit Entry
View Audit Summary
Request Full Audit Trail
Rules based real time analysis
View Service
Consolidated View
Index View
Change History View
View Data Extraction and Maintenance
Report Service
Operational Reporting
Uptake Reporting
KPI Reporting
ETL
De-identification
Data Warehouse Management
Core PCEHR Services
Repository Access Services
Repository Registration Management
Distributed Repository Retrieval and Update Services
Data Quality Review and Integrity Check Services
Archival Services
Repository Monitoring
National Repositories Service
Shared Health Summaries
Event Summaries
Discharge Summaries
Consumer Entered Information
Conformant Repositories
Medicare Repositories
Diagnostic Service Repositories
Diagnostic Service Repositories
Regional Repositories
State/Territory Repositories
Other Repositories
Repositories


NASH
NASH
Root Certificate
Certificate Revocation List
Digital Certificate
Token
Credential
Organisation Credential
HPI-O
Provider Credential
HPI-I
Conformant Portal
Local Records
IHI
Uploaded Records
Concept
Individual Created Content
View Records
Clinical Document
Clinical System
Local Records
IHI
Uploaded Records
Concept
Clinical Document
Downloaded Records
Clinical Document
CSP
Local Records
IHI
Uploaded Records
Concept
Clinical Document
Downloaded Records
Clinical Document
Legend:
Foundations
PCEHR System
External System
Service
Information Component
Common Information Component
Call Centre
Call Centre System
Caller Record
Issues
Consumer Portal
Consumer Portal
Portal Account
User Details
User Credential
Provider Portal
Provider Portal
Portal Account
User Details
Provider Credential
B2B Gateway
B2B Gateway
Report Portal
Report Portal
Portal Account
User Details
User Credential
HI Service
HI Service
Individual
Individual Identifying Information
IHI
National Healthcare Provider Service Directory
Organisation
Organisation Identifying Information
Seed Organisation
HPI-O
Network Organisation
Provider
Provider Identifying Information
HPI-I
Participation and Authorisation Service
Participation and Authorisation Service
Participating Individual
Participation Information
IHI
Person Details
Status
Contact Details
Contact Person
Nominated Provider
Representative
Person Details
Contact Details
Authorised Representative
Nominated Representative
Authorisation Information
Access Control Settings
PAC / PACX
Access List
Organisation
Level
HPI-O
Index Service
Index Service
Index of individual PCEHRs
Details
IHI
Index Entry
Doc ID
Location
Metadata
View Service
View Service
View for Individual PCEHR
Index View
Change History View
Consolidated View
Lists for Individual PCEHR
Doc ID
Entry
Allergies / Adverse Reactions
Medicines
Immunisations
Directives
Detailed Clinical Model (DCM)
Concept
Audit Service
Audit Service
Audit Trail for Individual PCEHR
Audit Entry
Date / Time
Participating Organisation
Accessing Organisation
Accessing System
User Details
Authorisation Details
Action
Report Service
Report Service
Report Data Set
Operational Report
SLA Metric Report
Audit Report
Data Quality Report
Uptake and Usage Report
KPI Report
National Repositories Service
National Repositories Service
Clinical Document
Conformant Repository
Conformant Repository
Clinical Document
Conformant Repository
Conformant Repository
Clinical Document
Conformant Repository
Conformant Repository
Clinical Document
National Healthcare Provider Service Directory
NHSPD
Organisation Listing
Details
HPI-O
Clinical Service
Template ID
Provider Listing
HPI-I
ELS Entry
End Point Location Service (ELS)
Template Service
Template Service
Document Template
Template ID
Structured Content Specification (SCS)
Schema and Validation Rules
Style Sheet
Shared Health Summary
Event Summary
Discharge Summary
Referral
Specialist Letter
Pathology Result Report
Imaging Report
Medicare Information
Consumer Entered Information
Advance Care Directives
Clinical Document
Control Information
Header
Clinical Document
Attachment
Doc ID
Attestation
Digital Signature
Template ID
Structured Clinical Document
Unstructured Clinical Document
IHI
HPI-I
HPI-O
Individual
Source
Section
Data Group
Data Element
Data Type
Organisation Credential
Details
Role
Participant
Data Component
Coded Data
Clinical Terminologies and Information
NCTIS
Structured Content Specification (SCS)
Detailed Clinical Model (DCM)
Terminology Binding
SCT-AU Reference Set
AMT
Concept
SCT Component
SCT Relationship
SCT Concept
SCT Description
Terminology Mapping
ICPC 2+
ICD-10-AM
LOINC
Non SNOMED Code


External CIS system or External Portal
«use»
Presentation Layer
«boundary»
Administration and Report Portal
«boundary»
Support Portal
«boundary»
Provider Portal
«boundary»
Consumer Portal
Secure Token Service
Portal Infratructure Services
«medicare»
OLS
«use»
«use»
Access Layer / B2B Gateway
«interface»
System Administration Interfaces
{abstract}
«interface»
Support Interfaces
{abstract}
«interface»
Provider Authentication Interface
{abstract}
+ authenticateProvider()
«interface»
Individual Authentication Interface
{abstract}
+ authenticateIndividual()
+ getRandomChallangeQuestions()
+ performChallengeResponse(HI) : PCEHRSecurityToken
«interface»
Individual Administration Service External Interface
{abstract}
+ register()
+ activate()
+ deactivate()
+ getAccessControlView()
+ getIndividualNominatedProvider()
+ deleteNominatedProvider()
+ setAccessControl()
+ setNominatedProvider()
+ setIndividualProfile()
+ setAuthorisedRepresentative()
+ setNominatedRepresentative()
+ acceptRepresentativeNomination()
+ excludeOrganisation()
+ includeOrganisation()
+ doesPCEHRExist()
+ generateTAK()
«interface»
Document Query and Management External Interface
{abstract}
+ retrieveDocument()
+ findDocuments()
+ storeDocument()
+ removeDocument()
+ storeDocumentMetaData()
+ retrieveDocumentMetaData()
+ setDocumentAccessLevel()
+ openPCEHR()
+ closePCEHR()
«interface»
PCEHR View Interface
{abstract}
+ getConsolidatedView()
+ getIndexView()
+ getChangeHistoryView()
+ getConsumerAuditView()
«interface»
Report Interfaces
{abstract}
Business Services Layer
PCEHR Core Services
«flow»
Audit Log
Technical Service Layer
Service Coordination
«interface»
Conformant Repository Document Metadata Retrieval
{abstract}
+ retrieveDocumentMetaData()
+ findDocuments()
«interface»
Conformant Repository Document Retrieval
{abstract}
+ retrieveDocument()
+ removeDocument()
«interface»
Conformat Repository Document Storage
{abstract}
+ storeDocument()
Report Service
«interface»
LO Conformant Repository Interface
{abstract}
National Repository
+ retrieveDocument()
+ storeDocument()
+ removeDocument()
+ retrieveDocumentMetaData()
Foundation Services
HI Service
NASH
TemplateService
NHSPD
CTI
Operational System Layer
Conformant Repository
+ retrieveDocument()
+ removeDocument()
+ retrieveDocumentMetaData()
Medicare Repositories