



---

**HI Service**  
**Concept of Operations**

Version 2.0— 8 June 2010

Release – Final

---

**National E-Health Transition Authority Ltd**

Level 25  
56 Pitt Street  
Sydney, NSW, 2000  
Australia.  
<http://www.nehta.gov.au>

**Disclaimer**

NEHTA makes the information and other material ("Information") in this document available in good faith but without any representation or warranty as to its accuracy or completeness. NEHTA cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

**Document Control**

This document is maintained in electronic form. The current revision of this document is located on the NEHTA Document Management System and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is of the latest revision.

**Trademarks**

Company, product, and service names mentioned herein may be trademarks or service marks; such marks are the property of their respective owners.

**Security**

The content of this document is Confidential. The information contained herein must only be used for the purpose for which it is supplied and must not be disclosed other than explicitly agreed in writing with NEHTA.

**Copyright © 2009, NEHTA.**

This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems—without the permission of NEHTA. All copies of this document must include the copyright and other information contained on this page.

National E-Health Transition Authority

## Revision chart

### Document Details

<b>File Name</b>	<b>HI Service Concept of Operations v2.0</b>
Original Author(s)	National Infrastructure Services
Creation Date	22 September 2009
Last Saved	8 June 2010

### Document Sign-off

<b>Name</b>	<b>Role</b>	<b>Signature</b>	<b>Date</b>
Peter Fleming	CEO, NEHTA		

### Revision History

Version	Revision Date	Author(s)	Revision Notes
0.1	12 October 2009	David Cliff, David Halls, Robyn Cooke	Initial draft
0.2	14 October 2009	Robyn Cooke	Updated with additional information and with feedback from IAARG Tiger Team members
0.3	15 October 2009	Robyn Cooke, David Nissen, Bill Bolton	Further updates
0.9	19 October 2009	Robyn Cooke	Further updates
0.95	12 November 2009	Bob Whitehead, Marina Fulcher, Chris Wagner, Nerida Lawrentin, Peter Williams	Updated input from Tiger Team review References to 'Responsible Officer' changed to 'Responsible Officer'
0.96	17 November 2009	Bob Whitehead, Marina Fulcher, Chris Wagner, Nerida Lawrentin, Peter Williams, David Cliff	Additional explanatory text, revisions
0.99	18 November 2009	David Cliff, with input from above	Final revisions
1.00	19 November 2009	David Cliff	Release
1.10	20 April 2010	Bob Whitehead, Marina Fulcher, Robyn Cooke	Editorial updates
2.0	8 June 2010	Joy De Leon following IAARG approval.	Release

# Table of Contents

1	Introduction .....	8
2	Scope .....	9
2.1	Document overview .....	9
2.1.1	Purpose.....	9
2.1.2	Introduction to national e-health.....	9
2.1.3	Audience .....	10
2.1.4	Document Map.....	11
2.2	System overview .....	11
2.2.1	Purpose of the HI Service.....	12
2.2.2	General nature of system.....	13
2.2.3	Project sponsors.....	13
2.2.4	Role of NEHTA .....	14
2.2.5	Users of the HI Service .....	14
2.2.6	Associated Organisations .....	14
2.3	Graphical overview of system.....	14
3	Reference documents .....	17
4	Current Healthcare Identifiers.....	19
4.1	Background.....	19
4.2	Scope of current healthcare identifiers.....	20
4.3	Operational policies and constraints.....	21
4.3.1	Privacy .....	21
4.3.2	Adoption, use or disclosure of Commonwealth Government identifiers .....	21
4.4	Users and other involved personnel .....	22
4.4.1	Other involved personnel .....	22
4.5	Support environment .....	22
4.5.1	Legislation .....	22
4.5.2	Common law duty of confidentiality .....	23
4.5.3	Professional requirements and standards.....	23
4.5.4	Computing infrastructure .....	23
5	Justification for and nature of changes.....	24
5.1	Benefits of a National Approach.....	26
6	Concepts for the proposed system .....	27
6.1	Background and objective.....	27
6.1.1	Background .....	27
6.1.2	Objective.....	27
6.2	Scope of the HI Service .....	27
6.3	Operational policies and constraints.....	27
6.3.1	Governance .....	27
6.3.2	Strategic Oversight .....	28
6.3.3	Management and Operation .....	28
6.3.4	Independent Regulatory Oversight.....	28
6.3.5	Information Security .....	29
6.4	Description of the HI Service.....	31
6.4.1	Components .....	31
6.4.2	Functions.....	32
6.4.3	Structure of the HI Service identifiers.....	32

6.4.4	IHI .....	33
6.4.5	HPI-I .....	35
6.4.6	HPI-O .....	37
6.4.7	HI Provider Directory Service .....	38
6.5	HI Service Channels .....	38
6.5.1	HI Service business offices .....	39
6.5.2	Web service .....	39
6.5.3	Web portal .....	39
6.5.4	Telephone support .....	39
6.6	User Roles .....	40
6.6.1	Support and Operation Roles .....	40
6.7	Support environment .....	41
6.7.1	HI Service Availability .....	42
7	Summary of impacts .....	43
7.1	Organisational impacts .....	43
7.2	Start-Up Impacts for Organisations .....	43
7.3	Operational impacts for Organisations .....	44
8	Analysis of the HI Service .....	45
8.1	Benefits .....	45
8.1.1	Decommissioned capabilities .....	47
8.2	Limitations .....	47
8.3	Alternatives and trade-offs considered .....	47
9	Business Use Cases .....	49
9.1	IHI Business Use Cases .....	49
9.2	HPI-O Business Use Cases .....	50
9.3	HPI-I Business Use Cases .....	52
Appendix A	- Business Use Case .....	53
UC.010	- Presentation at a healthcare facility with a TDS identifier .....	54
UC.011	- Presentation at a healthcare facility without a TDS identifier .....	55
UC.021	- A person enrolls with a Trusted Data Source .....	56
UC.030	- Batch IHI search against HI service for initial IHI load .....	57
UC.031	- Batch IHI search against HI Service for data quality .....	58
UC.040	- Verification (EOI) for an unverified IHI .....	59
UC.060	- Create unverified IHI for newborn .....	60
UC.070	- Unconscious/incapacitated and unknown individual .....	61
UC.081	- Provide pseudonymous IHI for healthcare individual .....	62
UC.083	- Creation of an alternate name .....	63
UC.112	- Maintain an unverified IHI .....	64
UC.130	- Establish seed HPI-O .....	65
UC.131	- Establish Organisation Maintenance Officer .....	66
UC.135	- Establish a networked HPI-O .....	67
UC.136	- Reconfigure HPI-Os (mergers or acquisitions of healthcare provider organisations) .....	68
UC.170	- Maintain HPI-O .....	69
UC.172	- Retire a seed HPI-O .....	70
UC.173	- Retire a networked HPI-O .....	71
UC.180	- New professional registration through a TDS (create HPI-I) .....	72
UC.182	- Create or maintain HPI-I through HI Service .....	73
UC.210	- Link HPI-I with HPI-O in HI Provider Directory Service .....	74

UC.220 – Retire HPI-I .....	75
UC.222 – HPI-I maintains details through web portal access.....	76
UC.224 – Validate HPI-I .....	77
UC.232 – Locate healthcare provider (HPI-I or HPI-O) in HI Provider Directory Service .....	78
Appendix B - Glossary.....	79

## List of figures

Figure 1 – Concept of Operations document relationship .....	11
Figure 2 - Overview of HI Service Components .....	15
Figure 3 - HI Service Solution Overview.....	16
Figure 4 - Structure of the IHI, HPI-I and HPI-O.....	33

# 1 Introduction

The purpose of this Concept of Operations is to provide an overview of the Healthcare Identifiers Service by:

- Describing the current state of healthcare identification
- Describing the Healthcare Identifiers (HI) Service in such a way that key stakeholders can visualise how the HI Service will be used and how it will work
- Documenting key concepts and their usage
- Illustrating the impact on today's situation

The format and contents of this Concept of Operations document are described as follows:

- The general format follows an International Standard (IEEE 1362-1998) for describing the "Concept of Operation" of a software intensive business system
- A Concept of Operations is a user-oriented document that describes system characteristics from a user point of view
- It is used to communicate overall system characteristics to a user, buyer, developer, and other organisational elements (for example, training, facilities, staffing, and maintenance)
- It is used to describe the user organisation(s), mission(s), and organisational objectives from an integrated systems point of view
- The IEEE format has been expanded to include Business Use Cases and other descriptive [material] to provide additional coverage of the application of the Healthcare Identifiers Service within typical for healthcare delivery business processes



## 2 Scope

### 2.1 Document overview

#### 2.1.1 Purpose

The Commonwealth, State and Territory governments have tasked the National E-Health Transition Authority (NEHTA) to identify and foster the design and development of technology to deliver the best e-health system for Australia. A foundation component of this is to deliver a consistent national healthcare identifier service for:

- Recipients of healthcare services – the Individual Healthcare Identifier (IHI)
- Individual providers of healthcare services – the Healthcare Provider Identifier-Individual (HPI-I)
- Healthcare organisations – Healthcare Provider Identifier–Organisation (HPI-O)

This Healthcare Identifiers Service (HI Service) is the subject of this Concept of Operations document. The purpose of the Concept of Operations is to:

- Describe the current state of healthcare identifiers in Australia
- Describe the Healthcare Identifiers Service (HI Service), in such a way that key stakeholders can understand:
  - What the service is
  - Why the service is required (from a high level)
  - How it will work
  - How it will be implemented
- The key privacy/policy underpinnings
- Document key concepts and their usage
- Illustrate key scenarios where healthcare identifiers will be used to highlight any gaps in expectations
- Illustrate the impact relative to today's situation as it relates to the proposed services and solution

#### 2.1.2 Introduction to national e-health

This document provides a comprehensive overview of the HI Service. Readers seeking a more general understanding of the national e-health services are referred to the document "Introduction to National e-Health Services".

That document provides background information on health sector trends, the current use of information technology in the health sector, healthcare identifiers and the benefits of e-health.

The benefits of e-health are illustrated in a simple 'patient journey' that describes how this new technology will work, both diagrammatically and with a table that reflects each step in the journey, in a way that individuals who have any contact with the health sector can relate to.

### **2.1.3 Audience**

This document is specifically intended for the following readers:

- Reference groups and committees who advise or oversee the design and policy framework within which the HI Service operates. This includes:
  - National Health Chief Information Officer Forum (NHCIOF)
  - National Health Information Regulatory Framework (NHIRF) Working Group
  - Identification, Authentication and Access Reference Group (IAARG)
  - Continuity of Care Reference Group (CCRG) Medication Management Reference Group (MMRG)
  - Diagnostic Services Reference Group (DSRG)
  - Clinical Leads Unit
  - Other relevant NEHTA Reference Groups
- It may also be of some value to others in the e-health space who have an interest in the overall e-health program, and may include:
  - Chief Information Officers
  - Program managers
  - Product managers
  - Project managers
  - Business analysts
  - Consultants
  - Software developers
  - Policy officers
  - Standards bodies
  - Clinical representatives

- Healthcare consumer representatives
- Health informaticians
- Professional bodies

While this document may have a broader application, it is not directed at readers outside the community identified above.

For additional background information about e-health in Australia and the NEHTA work, readers are referred to the reference material listed in Section 3.

## 2.1.4 Document Map

Figure 1 represents the relationship between this document and some other HI Service documents.

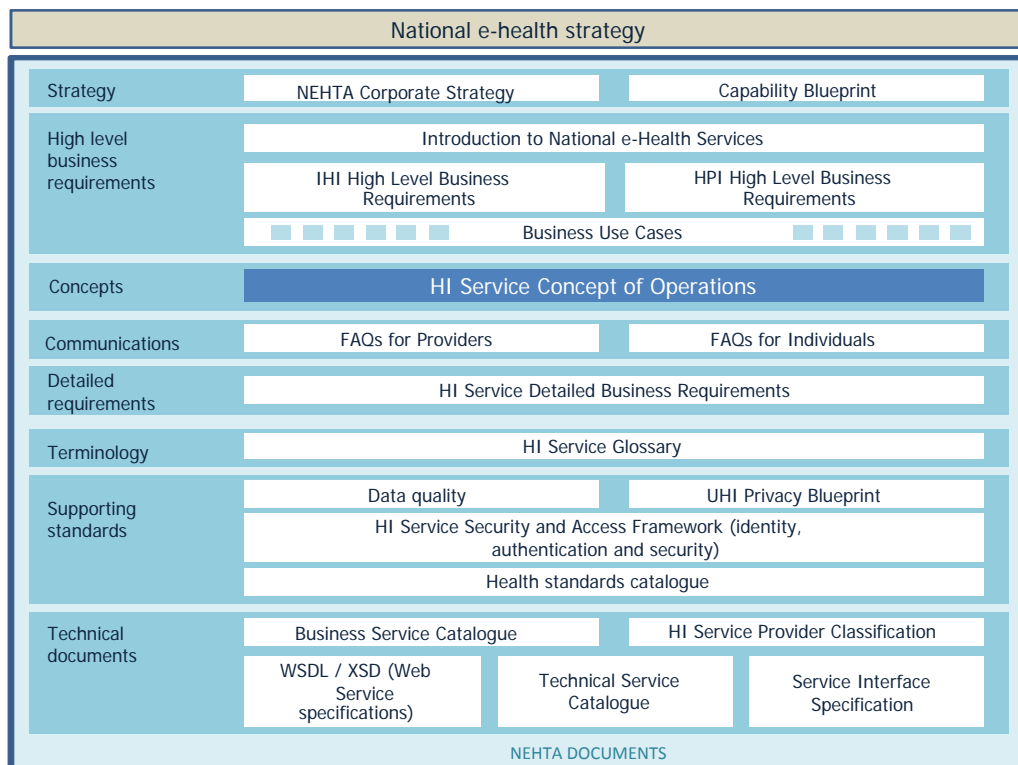


Figure 1 – Concept of Operations document relationship

## 2.2 System overview

The HI Service is a system that provides a consistent set of identifiers for healthcare individuals and healthcare providers (organisations and individuals).

The HI Service:

- Enables healthcare providers to associate health information about a healthcare individual accurately, securely and consistently within a healthcare context. This association

includes use within electronic communications such as discharge summaries, prescriptions and referrals

- Provides a means of managing the relationship between healthcare provider individuals and organisations when accessing the HI Service and, in the future, individual electronic health records

To provide an overview of the system, this document will describe the HI Service in terms of:

- Purpose
- General nature
- Project sponsors
- User agencies
- Certifiers or certifying bodies
- Graphical overview

### 2.2.1 Purpose of the HI Service

The purpose of the Healthcare Identifiers Service is to assign, issue and maintain national healthcare identifiers for consumers and providers. Together with the establishment of robust regulatory arrangements to ensure appropriate safeguards for patient health information, this will encourage participation in e-health initiatives

The regulatory arrangements will limit the use of healthcare identifiers to healthcare management and communication as part of delivering healthcare services, health service management activities and health research.

E-health is the means of ensuring that the right health information is provided to the right person, at the right place and time, in a secure electronic form. It aims to optimise the quality and efficiency of health care delivery.

The National e-health Strategy notes that e-health will<sup>1</sup>:

- Ensure the right consumer health information is electronically made available to the right person at the right place and time to enable informed care and treatment decisions
- Enable the Australian health sector to more effectively operate as an inter-connected system overcoming the current fragmentation and duplication of service delivery
- Provide consumers with electronic access to the information needed to better manage and control their personal health outcomes

---

<sup>1</sup> National e-health Strategy, p.26

- Enable multi-disciplinary teams to electronically communicate and exchange information and provide better coordinated health care across the continuum of care
- Provide consumers with confidence that their personal health information is managed in a secure, confidential and tightly controlled manner
- Enable electronic access to appropriate health care services for consumers within remote, rural and disadvantaged communities
- Facilitate continuous improvement of the health system through more effective reporting and sharing of health outcome information
- Improve the quality, safety and efficiency of clinical practices by giving care providers better access to consumer health information, clinical evidence and clinical decision support tools
- Support more informed policy, investment and research decisions through access to timely, accurate and comprehensive reporting on Australian health care system activities and outcomes.

The HI Service will provide a consistent national healthcare identifier infrastructure for use across the Australian healthcare sector, and will support the Council of Australian Government's (COAG) initiative to accelerate the adoption of e-health technologies in Australia.

### **2.2.2 General nature of system**

The HI Service is more than just business services and technology. It combines technology with enabling legislation, policy and operational services that work together to facilitate consistent use of identifiers for healthcare individuals and providers.

### **2.2.3 Project sponsors**

In 2006, COAG agreed to a national approach to developing, implementing and operating key systems, including for individual and healthcare provider identifiers, as part of accelerating work towards a national electronic health records system.

Through the Australian Health Ministers' Conference (AHMC), the project is sponsored by the Commonwealth, state and territory governments, which have been investing, through NEHTA, in key building blocks for a national e-health system, including the HI Service.

#### **2.2.4 Role of NEHTA**

The role of NEHTA is to project manage the design, development and delivery of e-health enabling technology and services.

The development of the HI Service is a foundation component of NEHTA's work program.

#### **2.2.5 Users of the HI Service**

The HI Service will provide healthcare identifier infrastructure for use across a complex network of public and private healthcare provider individuals and organisations, including:

- public and private sector hospitals
- general practice
- clinical specialist
- community health
- healthcare administrators
- allied health
- aged care settings

#### **2.2.6 Associated Organisations**

The HI Service will work co-operatively with a number of other organisations in the healthcare sector, including:

- Trusted Data Sources
- Development organisations
- Standards bodies
- Professional bodies
- Regulatory bodies

### **2.3 Graphical overview of system**

Figure 2 provides a context for the HI Service within the National e-Health Infrastructure.

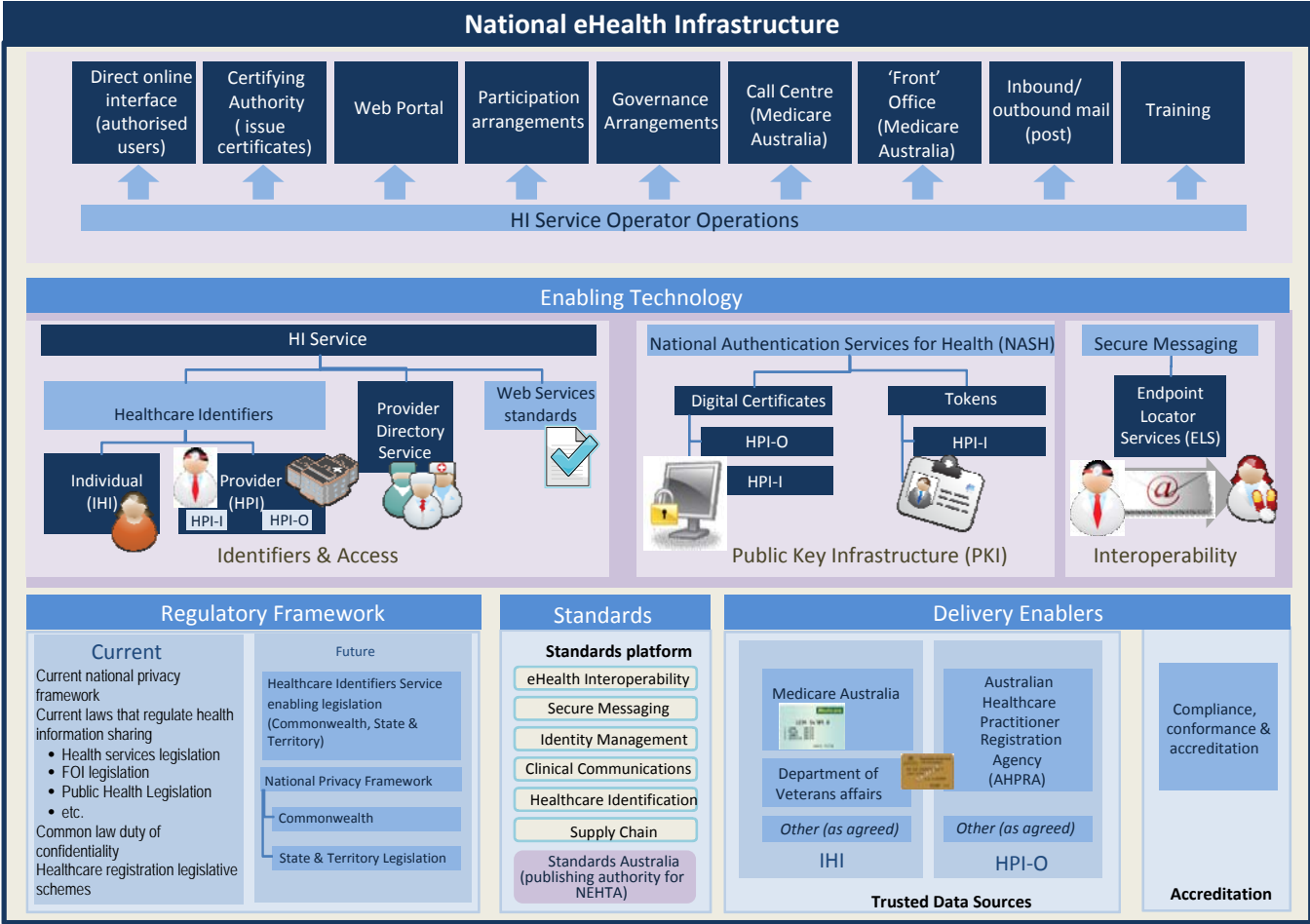


Figure 2 - Overview of HI Service Components

The following solution overview diagram shows the HI Service and its relationship with associated systems and organisations.

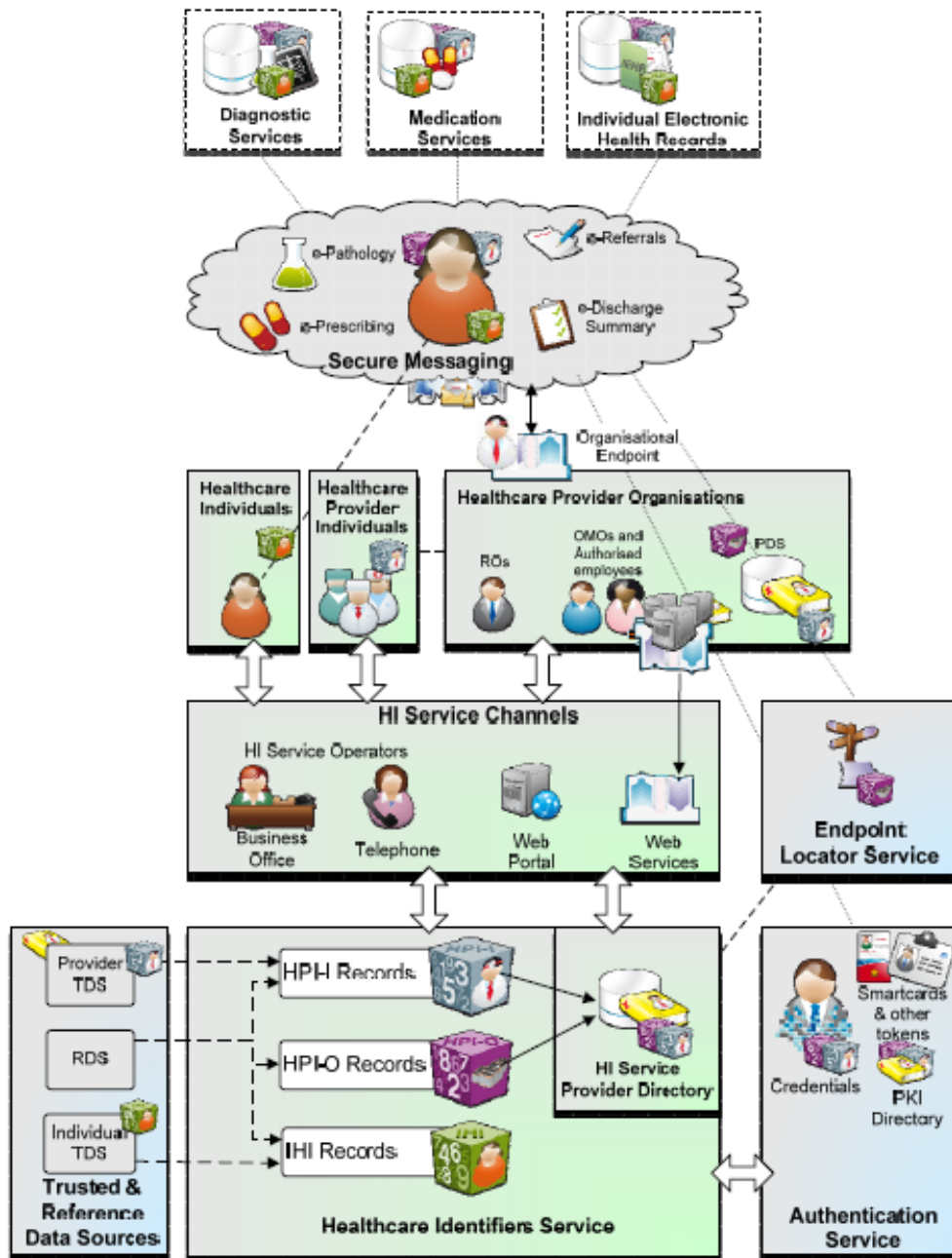


Figure 3 - HI Service Solution Overview



### 3 Reference documents

- AS 3523-1:2008 Australian Standard, Identification Cards-  
Identification of issuers, Part 1: Numbering system, 2008
- AS4846-2006 Healthcare Provider Identification, 2nd edition,  
Australian Standards Association, June 30 2006
- Australian Institute of Health and Welfare, Metadata Online Registry  
(METeOR), 2006
- AS5017-2006 Healthcare Client Identification, Australian Standards  
Association, June 30 2006
- Better Health for all Australians Action Plan Attachment D, Feb 10  
2006,  
[http://coag.gov.au/meetings/100206/attachment\\_d\\_better\\_hea  
lth.pdf](http://coag.gov.au/meetings/100206/attachment_d_better_health.pdf)
- Healthcare identifiers and privacy: Discussion paper on proposals  
for legislative support Australian Health Ministers' Advisory  
Council, July 2009
- IEEE 1362-1998, IEEE Guide for Information Technology - System  
Definition – Concept of Operations (ConOps), Software  
Engineering Standards Committee of the IEEE Computer  
Society, USA, Mar 19 1998
- ISO/PDTS 22220, Healthcare Informatics – Identification of subjects  
of healthcare, International Standards Organisation, Jan 18  
2005
- ISO7812-16/IEC 7812-1:2000(E), Identification Cards –  
Identification of Issuers, International Standards Organisation,  
September 15 2000
- National E-Health Strategy Summary, Australian Health Ministers'  
Conference, December 2008
- NEHTA, Healthcare Provider Classification for the HI Services  
Position Paper, version 1.0, November 19 2009
- NEHTA, HI Service Security and Access Framework, version 1.0,  
November 13 2009
- NEHTA, Healthcare Provider Identifiers Business Requirements,  
version 1.0, October 26 2009
- NEHTA, Individual Healthcare Identifiers Business Requirements,  
version 1.0, November 18 2009

NEHTA, Introduction to National e-Health Services, version 1.0,  
November 1 2009

NEHTA, HI Service Detailed Requirements, version 1.0, November  
19 2007

NEHTA, HI Service Glossary, version 1.0, November 19 2007

## 4 Current Healthcare Identifiers

This section provides an overview of the current approach in place for healthcare identifiers. There is no existing national system for healthcare identifiers.

### 4.1 Background

Healthcare individuals are largely responsible for coordinating their own care delivery, with little access to their own personal health information, as it is stored in multiple, fragmented systems. Healthcare individuals have limited capacity to use current identifiers that may relate to them.

Healthcare has traditionally relied heavily on the healthcare individual keeping track of their own health needs, and on the healthcare provider collecting necessary information from the healthcare individual during the process of providing healthcare services. Individuals are familiar with the need or expectation to identify themselves as part of their interactions with a range of services and organisations, including healthcare services.

Providing continuity of care to a healthcare individual over multiple separate care episodes is often hampered by a lack of consistent identification of the individual.

Additionally, referring a healthcare individual from one provider to another and sharing or exchanging treatment or diagnosis information between healthcare providers has, in the main, been done by using paper.

Currently, healthcare providers have a variety of different processes for identifying both their patients and other providers that they deal with in the healthcare sector.

Healthcare providers, including general practices, pharmacies, pathologists, private and public hospitals all generally have their own individual patient record systems. Additionally, state and territory jurisdictions use their own patient or client identification systems.

The National E-Health Strategy Summary described this situation as follows:

*The Australian health care system is straining to deal with increasing cost and demand pressures and a shortage of skilled health care workers. Given this reality, we need to move to a system where every interaction between consumers and care providers achieves maximum impact on health outcomes and where scarce financial and human resources are deployed as effectively as possible. Most of all we must draw upon the latent capacity in the system represented by consumers*

*themselves playing a more active role in the protection and management of their personal health outcomes.*<sup>2</sup>

E-health systems provide the means to achieve this, but to be effective these need to be supported by consistent healthcare identifiers for individuals and providers.

The document 'Healthcare identifiers and privacy: Discussion paper on proposals for legislative support', describes the situation and need in this way:

*At present, sharing of patient health information in the course of delivering healthcare services is ad hoc and inefficiently based on arrangements between particular stakeholders. There is, for example, no common way to identify individual healthcare consumers or healthcare providers.*<sup>3</sup>

It is within this context that the need for a HI Service has been identified.

## **4.2 Scope of current healthcare identifiers**

Current healthcare identifiers are provided and managed through a combination of manual and technology components, and operate within a complex set of privacy and health information management policies and laws.

The current approach to healthcare identifier systems promotes:

- Public health organisations increasingly establishing jurisdictionally or regionally based identification schemes
- Identifiers, such as Medical Record Numbers (MRNs), being created and maintained for healthcare individuals at a local level
- Healthcare provider identifiers that are only used within the domain of a healthcare facility, and managed by the provider's local directory
- Healthcare provider information being stored across multiple directories, maintained by various registration bodies, private medical imaging, pharmacy and pathology services and public and private hospitals, making it difficult to locate individual providers
- Inconsistent identification of healthcare providers who work for more than one organisation at the same time, making it

---

<sup>2</sup> Australian Health Ministers' Conference, *National E-Health Strategy Summary*, December 2008, p 1

<sup>3</sup> Australian Health Ministers' Advisory Council, *Healthcare identifiers and privacy: Discussion paper on proposals for legislative support*, July 2009, p 9

difficult to send patient information to the right service location

- Lack of clarity between identifiers which are intended for medical and other benefit purposes, and identifiers which are intended for healthcare delivery purposes

### **4.3 Operational policies and constraints**

The use of healthcare identifiers in Australia today is constrained by a number of policies related to privacy, and the adoption and use of identifiers.

#### **4.3.1 Privacy**

Australia's current privacy landscape is complicated and fragmented. Differing privacy schemes apply to health and e-health infrastructure across the Commonwealth, states and territories. This mix of legislation and administrative arrangements has resulted in:

- Increased compliance costs, particularly where business is being conducted across jurisdictional boundaries, or public and private sectors
- Confusion about which regimes regulate particular businesses
- Forum shopping between regulators to exploit differences in regulation
- Uncertainty among consumers about their rights

Changes are currently being considered to the national privacy legislation following the Australian Law Reform Commission review of Australian privacy laws.

#### **4.3.2 Adoption, use or disclosure of Commonwealth Government identifiers**

Unique identifiers can facilitate more seamless and convenient interactions between service organisations and consumers, they can also make it significantly easier to match or link personal information that has been collected in different contexts and for different purposes.

To prevent inappropriate linkage of personal information in ways that individuals may not expect, the Privacy Act (Commonwealth) prevents private sector organisations from adopting identifiers that have been assigned to individuals by a Commonwealth agency, unless they have been authorised to do so by law.

There are also restrictions on using or disclosing Commonwealth identifiers other than to meet the obligations of the issuing agency.

## **4.4 Users and other involved personnel**

Current healthcare identification schemes are primarily used to support the clinical and business processes of healthcare providers. As such, the main users of these health identifier schemes are healthcare providers and healthcare managers.

### **4.4.1 Other involved personnel**

Other individuals or services that currently use healthcare identifier systems include:

- Administrators and clerical staff who work for healthcare providers
- Secure messaging services
- Authentication Services
- Jurisdictional and local service directories
- Other organisations such as research bodies

## **4.5 Support environment**

There are many elements applying to the regulation of health information sharing. These include laws that may prohibit specific information flows, or authorise information flows that would otherwise be a breach of privacy legislation. Key instances of these are:

- Legislation
- Common law duty of confidentiality
- Professional requirements and standards

### **4.5.1 Legislation**

Legislative controls on sharing of health information include:

- Health services legislation
- Freedom of Information (FOI) legislation
- Privacy legislation
- Public health notifications required under law
- Child protection legislation
- HIV AIDS legislation
- Mental health legislation
- Power of attorney and guardianship legislation

#### **4.5.2 Common law duty of confidentiality**

There is a common law duty of confidentiality that healthcare providers owe to patients, when personal information is collected as part of a healthcare interaction.

#### **4.5.3 Professional requirements and standards**

Requirements are imposed on certain healthcare providers under the various healthcare registration schemes. Healthcare and clinical standards are also issued by a range of expert bodies.

#### **4.5.4 Computing infrastructure**

There is a relative lack of maturity of information technology within the Australian healthcare sector, with the inconsistent application of national e-health standards on which to base the development of hardware and software. This is compounded by the lack of national governance over certification and compliance with standards.

## 5 Justification for and nature of changes

This section describes the drivers for developing and implementing the national Healthcare Identifiers Service.

Currently in Australia there is no single method that uniquely and reliably identifies healthcare individuals within the healthcare environment.

The majority of healthcare organisations operate separate identification methods and supporting systems to identify individuals receiving healthcare.

Associating the wrong health information to a patient can risk patient safety, through not being able to correctly associate health information (from a single or multiple episodes of care) to the correct patient. Errors can include:

- Medication errors
- Incorrect surgical interventions
- Diagnostic testing errors

A national approach to establishing healthcare identifiers has been selected to avoid duplicating development costs and efforts and in recognition that identifiers are part of the core infrastructure needed to support secure electronic communication and supporting portability of patient information across the various elements of Australia's healthcare system.

The National E-Health Strategy Summary included identification and authentication as one of the five key national foundations required for e-health:

***Identification and authentication*** - *There is a need to design and implement an identification and authentication regime for health information as soon as possible as this work will be absolutely fundamental to the nation's ability to securely and reliably access and share health information. Australia should seek, as far as possible, to make the allocation of consumer and care provider national identifiers universal and automatic.*<sup>4</sup>

A fundamental shift in the way information is accessed and shared across the health system is required. Healthcare individuals, healthcare providers and healthcare managers need to access and share health information reliably and securely across geographic and health sector boundaries.

---

<sup>4</sup> Australian Health Ministers' Conference, *National E-Health Strategy Summary*, December 2008, p 10



This can only be achieved by implementing a world class e-health capability.

The HI Service is a fundamental building block to achieve this capability and, through the HI Service, identifiers for healthcare individuals, providers and organisations will realise the following aims. To:

- Uniquely and consistently identify healthcare individuals at the point of care
- Consistently associate health information with a healthcare individual within a healthcare context, including all electronic communications (such as discharge summaries and referrals)
- Uniquely, accurately and consistently identify healthcare provider individuals and organisations, and the relationship between a healthcare provider individual and an organisation, by providing high assurance identification and authentication for providers:
  - When accessing national e-health infrastructure
  - In electronic communications between healthcare providers
  - In electronic communications with healthcare individuals
- Support the development and operation of healthcare provider directory services, to facilitate electronic communications within a healthcare context (such as discharge summaries and referrals)<sup>5</sup>
- Support the development and operation of a security and access framework that ensures the appropriate authorisation and authentication of healthcare providers to access national e-health infrastructure

---

<sup>5</sup> A distinction is made between a provider directory that contains essential information required to support e-health communications and healthcare services directories.

The intention of the HI Service is to deliver a provider directory that can be leveraged by healthcare jurisdictions or other authorised organisations for a healthcare services directory.

## 5.1 Benefits of a National Approach

The National E-Health Strategy notes that<sup>6</sup>:

*A nationally coordinated approach to E-Health will [improve] the capacity of the Australian health system to do more with existing resources and by enabling these resources to be deployed against real need.*

The HI Service is a foundation for this coordinated, national approach to e-health.

---

<sup>6</sup> National e-health Strategy Summary, p.23

## **6 Concepts for the proposed system**

The HI Service will provide a set of national healthcare identifiers that support communication of health information more accurately, securely and reliably than is possible in the current environment.

This section articulates a high-level description of the HI Service and explains how it will operate.

### **6.1 Background and objective**

#### **6.1.1 Background**

To build a world class e-health solution, Australia needs frameworks and infrastructure components that can be leveraged at national, state and territory, regional and local levels to deliver solutions that are able to be integrated and share data across geographic and health sector boundaries.

#### **6.1.2 Objective**

The HI Service will provide identifiers that:

- Support healthcare providers' ability to associate health information with a healthcare individual (accurately and consistently) in a healthcare context. This includes all electronic communications such as discharge summaries, prescriptions and referrals;
- Support the management of the relationship between healthcare provider individuals and organisations when accessing the HI Service and, in the future, individual electronic health records; and
- Are based on a set of core standards.

### **6.2 Scope of the HI Service**

The HI Service allocates healthcare identifiers for use within the Australian healthcare system. It is intended for use by all Australian healthcare recipients and eligible providers.

Provision of any electronic health record functionality is out of scope.

### **6.3 Operational policies and constraints**

#### **6.3.1 Governance**

National e-health governance arrangements considered as part of the National E-Health Strategy were endorsed in principle by Health Ministers in December 2008 to guide further development of e-health in Australia. The Strategy identified three key governance functions:

- Strategic oversight
- Management and Operation
- Independent Regulatory Oversight

### **6.3.2 Strategic Oversight**

The body with responsibility for strategic oversight of the HI Service will be determined by COAG, and it is proposed that this will be Health Ministers. Key responsibilities of this body will be to determine national policies and the strategic direction of the HI Service, including its scope and authorised participants, the required regulatory and institutional arrangements and monitoring of those arrangements to ensure they continue to be suitable for purpose.

### **6.3.3 Management and Operation**

In accordance with national policies, priorities and strategic directions, key functions to be undertaken by the HI Service Operator include:

- Managing the issue and assignment of national healthcare identifiers
- Managing access to and use/disclosure of national healthcare identifiers
- Maintaining records of national healthcare identifiers
- Managing relationships with participants and relevant data sources
- Providing advice and information to the strategic oversight body on the performance of the system
- Educating, training and informing healthcare providers and healthcare individuals about how the HI Service operates
- Responding to system/service complaints and enquiries (in the first instance)

### **6.3.4 Independent Regulatory Oversight**

A key element of independent regulation for the establishment and operation of the HI Service and the subsequent handling of healthcare identifiers by health sector participants is privacy regulation.

Key functions of privacy regulators will include:

- Handling of complaints from healthcare individuals and providers in relation to use of healthcare identifiers and associated information

- Monitoring the handling of healthcare identifiers and associated information
- Conducting investigations
- Applying a range of sanctions or penalties commensurate with the seriousness of a breach
- Developing and issuing codes or guidelines in accordance with policy set by strategic governance bodies
- General oversight and advice powers

### **6.3.5 Information Security**

The Security and Access Framework for the HI Service will operate within the context of the overall e-health security and access framework. It covers the principles, policies, processes and tools that are to be used to achieve this aim.

This framework recognises that strong information security will contribute to the success of the HI Service by appropriately safeguarding the personal information required to operate the Service<sup>7</sup>.

A multi-layered approach will safeguard the HI Service, and accordingly the Security and Access Framework incorporates both technical and non-technical controls. These include:

- Smartcards and PKI certificates to facilitate the accurate identification and authentication of individuals accessing the HI Service
- Robust audit trails, and proactive monitoring of access to the HI Service by both internal and external users
- Role-based access control policies
- Rigorous security testing, to be conducted both prior to and after commencement of operation of the HI Service
- Ensuring users of the HI Service are adequately trained, through provision of educational programs and other training mechanisms
- Requirements that healthcare provider individuals and organisations comply with healthcare identifiers specific legislation

The Security and Access Framework for the HI Service will ensure that the privacy, confidentiality, integrity and availability of information within the HI Service are not compromised.

---

<sup>7</sup> Taken from NEHTA's HI Service Security and Access Framework, Version 1.0, Nov 13 2009

Security needs to be operationally realistic for stakeholders, meaning that it must support, rather than hinder, the HI Service. As such, security has been designed to be 'fit for purpose', and to address policy objectives. Appropriate security controls are therefore being implemented in order to meet the HI Service objectives.

The objective of the Security and Access Framework for the HI Service is to:

- Minimise the risk of unauthorised access to the HI Service and the information it contains
- Enable detection of unauthorised information access or modification, and any other breach of information security (including privacy)
- Facilitate appropriate response to, and investigation of, any such breaches
- Assure the continued availability of the HI Service
- Provide a means to continually improve security protections (including protection of privacy, confidentiality, integrity and availability)

The Security and Access Framework will ensure that the privacy, confidentiality, integrity and availability of information within the HI Service are not compromised. As security needs to be operationally realistic for stakeholders, (meaning that it must support, rather than hinder, the HI Service) it has been designed to be 'fit for purpose' and address policy objectives.

#### **6.3.5.1 Breaches of security**

The Security and Access Framework operates within the broader information regulatory framework. Any breach of security may also be a breach of privacy and be subject to further penalties under the appropriate regulatory regime.

#### **6.3.5.2 Risk Management**

A risk management approach has been taken that aligns and complies with the international best practice information security management standard, ISO/IEC 27001.

The Security and Access Framework also recognises Medicare Australia as the initial HI Service Operator. The HI Service Operator is obligated to comply with the Australian Government's Protective Services Manual (PSM) and 'ACSI-33'. This approach will ensure that the HI Service is appropriately protected whilst meeting the needs of the healthcare community.

### **6.3.5.3 Confidentiality**

Confidentiality is paramount to ensure that information held in the HI Service is not made available or disclosed to unauthorised individuals or entities, whether directly or through automated processes. Confidentiality is not limited to, but includes, personal information, as well as commercially sensitive information.

Confidentiality will be assured by restricting access to information in the HI Service only to those users who are authorised to access it, and logging all access, whether successful or unsuccessful.

### **6.3.5.4 Integrity**

Integrity of information is concerned with ensuring that HI Service data is consistent and correct. Safeguarding the accuracy and completeness of information is vital for maintaining the integrity of the HI Service. Data quality management techniques will be used to regularly assess and maintain the quality and integrity of the HI Service information.

### **6.3.5.5 Availability**

The HI Service must be readily available and usable upon demand by any user who is appropriately authorised, including individuals accessing information about themselves. Healthcare events which lead to a need to access the HI Service may occur at any time. High operational availability must be assured by using a highly resilient production platform which includes geographically diverse components.

## **6.4 Description of the HI Service**

This section describes the major components of the HI Service, the range of functions provided and the channels used to access those functions.

### **6.4.1 Components**

The HI Service has three primary core service components:

- Individual Healthcare Identifier (IHI)
- Healthcare Provider Identifier-Individual (HPI-I)
- Healthcare Provider Identifier-Organisation (HPI-O)

A further component of the HI Service is the HI Provider Directory Service (HI PDS), available only to healthcare providers.

Healthcare providers issued with HPI-Is or HPI-Os will have the option of being included in the HI PDS. The HI PDS will enable the search and location of healthcare providers and supports communication and information exchange between them, such as referrals, test orders and results.

### 6.4.2 Functions

The HI Service functions include:

- Allocating IHIs, HPI-Is and HPI-Os
- Enabling users who are appropriately authorised to search, retrieve or validate IHIs, HPI-Is and HPI-Os
- Maintaining data associated with IHIs, HPI-Is and HPI-Os
- Enabling users who are appropriately authorised to maintain and publish selected data associated with HPI-Is and HPI-Os
- Facilitating the provision of digital certificates for accessing the HI Service and e-health communications
- Retiring IHIs, HPI-Is and HPI-Os

### 6.4.3 Structure of the HI Service identifiers

The IHI, HPI-I and HPI-O are persistent and unique 16 digit reference numbers that are designed to be read by individuals and machines. They are intended for use on tokens, medical documents, patient wrist bands and other media as appropriate.

The identifiers:

- Adhere to the International Standard [ISO7812: AS 3523.1&2-2008]
- Are visually distinguishable to ensure clinical safety as all three identifiers may be present side by side in healthcare documents
- Are intended to be displayed on documentation, reports, etc
- Are the same length (16 digits)
- Will never be re-used
- Can store enough unique numbers to ensure current and future population coverage
- Do not contain any information about a person or organisation such as age, location or field of practice
- Have built in integrity (IIN and Check digit)
- Support issue of identifiable numbers for testing and pilot purposes

Figure 4 provides a graphical representation of the numbering system.



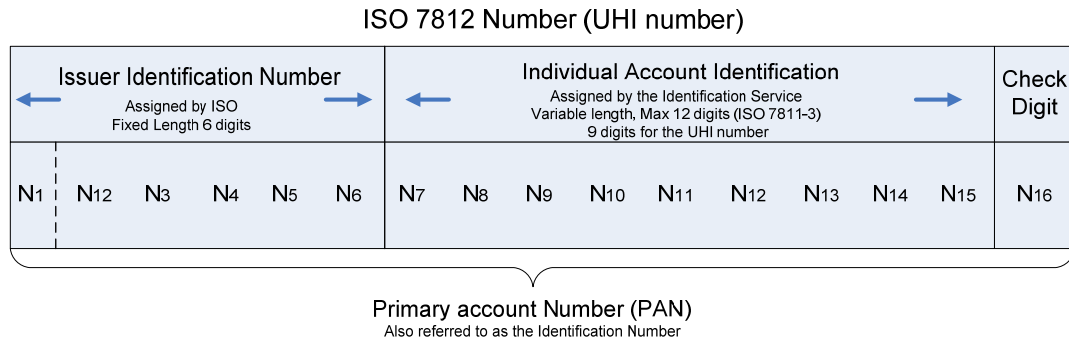


Figure 4 - Structure of the IHI, HPI-I and HPI-O

Each of the identifiers is made up of three components: issuer identification number, individual account identification number and the check digit.

- The issuer identification number is the first 6 digits of the identifier. This is a constant for each identifier as follows:
  - For all identifiers, the first 5 digits will be '80036'<sup>8</sup>
  - The 6<sup>th</sup> digit (N<sub>6</sub>) will be
    - '0' for an IHI
    - '1' for an HPI-I; or
    - '2' for an HPI-O
- The individual account identification number is the unique reference number.
- The check digit will be calculated using all components of the issuer and individual identification numbers. The check digit is computed using the Luhn formula modulus 10 "double-add-double" check digit [ISO7812].

#### 6.4.4 IHI

An IHI may be assigned to any person who receives healthcare.

To uniquely assign the IHI, a limited amount of identifying information will be used. This will include<sup>9</sup>:

- Name
- Date of birth (DOB)
- Date of birth accuracy indicator
- Sex

<sup>8</sup> Where '80' refers to health and '036' is Australia – consistent with the international and Australian standard

<sup>9</sup> Information associated with the IHI is compliant with AS5017 compliant – Health Care Client Identification

and may include:

- Address (verified IHIs will always include an address)
- Birth plurality (where relevant, and for a designated period)
- Birth order (where relevant, and for a designated period)
- Date of death (if applicable)
- Date of death accuracy indicator
- Alias/s
- Trusted Data Source<sup>10</sup> (TDS) identifier for the healthcare individual

IHIs will be automatically allocated against demographic information provided by Trusted Data Sources (TDS) and maintained through a one-way update from the TDS. Medicare Australia and Department of Veterans' Affairs (DVA) have been identified as initial TDSs.

Where an individual's IHI has been allocated through a TDS, the TDS will be responsible for storing and maintaining address information for the individual.

Individuals who are not automatically allocated an IHI, or who cannot be easily identified in the HI Service when presenting for healthcare services, will be able to have an interim number generated at the point of care (i.e. provisional IHI or unverified IHI).

#### **6.4.4.1 IHI Classification**

An IHI can be classified as 'verified', 'unverified', 'provisional', 'deceased' or 'retired'.

Additionally, for records management, the HI Service will support classifications to indicate that an IHI is a suspected or confirmed duplicate or replicate.

A verified IHI indicates that the information associated with that IHI has been confirmed through an Evidence of Identity (EOI) process that has been completed, either through the TDS that provided the initial information for the IHI, or through the HI Service.

An unverified IHI means that the information associated with the IHI has not been through an EOI process.

---

<sup>10</sup> A TDS is a managed repository of valid or trusted data that is recognised as an authoritative external source of data that meets an appropriate set of criteria and contains a set of attributes that covers the requirements of another business system. Leveraging existing data from an approved TDS occurs through technical processes, always ensuring that personal information is safeguarded.

A provisional IHI will be allocated to an individual who has presented at a healthcare facility and is unconscious or incapacitated, and unknown to the healthcare facility. Provisional IHIs will expire after 90 days unless the status has changed.

An IHI that has a status of deceased indicates that the HI Service has been notified of the death of a healthcare individual associated with that IHI.

An IHI that has a status of retired indicates that an IHI with a deceased status has been inactive for a period of 90 days and Fact of Death Data has been received from a Registrar of Births Deaths and Marriages..

#### **6.4.4.2 Verifying IHIs**

An individual will be able to verify their unverified IHI by completing an EOI process through the HI Service Operator or by enrolling with a Trusted Data Source.

#### **6.4.4.3 Retrieving IHIs**

IHIs will be able to be:

- Accurately and seamlessly retrieved by healthcare providers by the use of an individual's accredited/authorised TDS identifier. Retrieval of an individual's IHI will be based on an exact match using the TDS identifier plus the individual's name and date of birth
- Retrieved by healthcare providers via a demographic search where no TDS identifier is available. The demographic search will be based on an exact match using name and date of birth. In some situations, details of address and sex may need to be used to obtain an exact match

#### **6.4.4.4 IHI Tokens**

The HI Service will issue tokens directly to individuals who do not have one issued through a TDS.

#### **6.4.5 HPI-I**

An HPI-I may be allocated to a healthcare provider individual. It is associated with a limited amount of identifying personal and professional information required to uniquely identify the healthcare provider individual in the HI Service.

This will include for all HPI-I's:

- Name
- Address for registration
- Sex

- Date of birth (DOB)
- Provider individual type/s<sup>11</sup>

For HPI-Is allocated through a TDS it may include:

- Provider individual specialty/s<sup>12</sup>
- TDS identifier/s<sup>13</sup>
- Registration status/s

For all HPI-Is it may include:

- Business name (that is, the healthcare provider organisation name at which the healthcare provider individual is employed or practices)
- Electronic communication details
- Provider individual specialisation<sup>14</sup>
- Professional registration start date
- Professional registration end date
- Date of death (if applicable)

HPI-Is will be:

- Issued to any individual involved in providing healthcare who requires one
- Allocated to a healthcare provider individual through their professional or registration body where one exists, or other TDS, and maintained through a one-way synchronisation from the TDS

---

<sup>11</sup> Healthcare Provider Individual Type is a broad classification of healthcare provider individuals engaged in the provision of healthcare services consistent with AS4846 and ANZSCO 12200\_2006 – for further information see “Healthcare Provider Classification for the HI Services - Position Paper”

<sup>12</sup> Healthcare Provider Individual Specialty complies with AS4846 and ANZSCO 12200\_2006. It describes a healthcare provider individual’s field of practice (the skill or knowledge in a particular area practised by that provider).

This is further qualified by the Healthcare Provider Individual Specialisation which is the lower level of specialty that a healthcare provider individual identifies as being their specialised field of practice i.e. the skill or knowledge in a more specific practised by that provider. – for further information see “Healthcare Provider Classification for the HI Services - Position Paper”

<sup>13</sup> The TDS identifier is the number assigned for the individual by the TDS. For the initial release of the HI Service, this will be an individual’s AHPRA number or reference

<sup>14</sup> As per footnote 12

HPI-Is may be:

- Issued to a healthcare provider individual by the HI Service where the individual is not eligible for registration with a TDS but is eligible for an HPI-I under the healthcare identifiers legislation
- Used to identify the healthcare provider individual associated with accessing health information
- Used in electronic health information transactions and communications

#### **6.4.6 HPI-O**

An HPI-O may be allocated to a healthcare provider organisation and is associated with a set of identifying information.

This will include:

- ABN (Australian Business Number) and associated name, ACN (Australian Company Number) and associated company name or other accepted organisation identifier<sup>15</sup>
- Organisation Name (name under which the organisation operates)
- Address<sup>16</sup>
- Service Type<sup>17</sup>
- Electronic communication details
- Responsible Officer (RO) – individual with authority to act on behalf of the organisation
  - Name, DOB, address, electronic communication details (the last is optional)
- Organisation Maintenance Officer (OMO) - individual appointed to administer HI Service functions for HPI-O
  - Name, DOB, address, electronic communication details (this last is optional)

It may also include:

- Service unit<sup>18</sup>

---

<sup>15</sup> For further information on these information elements, refer to "Healthcare Provider Classification for the HI Services - Position Paper"

<sup>16</sup> The Address complies AS 4846 - Healthcare Provider Identification, 2nd edition

<sup>17</sup> The Australian Institute of Health and Welfare (METeOR) defines a Healthcare Provider Organisation Service Type as the specialities provided by Healthcare Providers in private or group practices in their own offices (e.g., centres, clinics) or in the facilities of others, such as hospitals or health maintenance type medical centres

- Registered Business Name
- Reference information to the Endpoint Locator Service (ELS) for the HPI-O

#### **6.4.6.1 HPI-O Classification**

HPI-Os will have one of two classifications:

- Seed HPI-O - This is the initial HPI-O allocated for the healthcare provider organisation and is the top level of an organisation's structure or hierarchy
- Network HPI-O - Network HPI-Os are allocated in a hierarchical structure under a seed HPI-O

#### **6.4.7 HI Provider Directory Service**

The HI Provider Directory Service (HI PDS) facilitates communication and information exchange between providers.

Healthcare providers have an option to publish information in the HI PDS, which users who are appropriately authorised can search, browse and download into their local address book. The HI PDS may contain:

- HPI-I, HPI-I status and selected demographic details
- HPI-O, HPI-O status and selected organisational details
- HPI-O association with HPI-I(s) (where the HPI-I has consented)
- Specialties
- Contact information
- Electronic communication details

The Organisation Maintenance Officer (OMO) for a HPI-O can choose the organisation information and associations with healthcare provider individuals, with the consent of the healthcare provider individual, to publish in the PDS.

A healthcare provider individual will be able to remove an existing association with an HPI-O at any time.

### **6.5 HI Service Channels**

Healthcare individuals and providers can access the HI Service through a number of channels. The service that is required will

---

<sup>18</sup> The Australian Institute of Health and Welfare (METeOR) defines Healthcare Provider Organisation Services Units as the nature of service provided by an organisational unit or organisational arrangement, which a healthcare provider organisation provides.

determine the particular range of channels through which it can be delivered.

#### **6.5.1 HI Service business offices**

A physical location where a healthcare individual, provider or authorised organisation representative can interact with a HI Service officer, to perform any tasks relating to their participation in the HI Service.

#### **6.5.2 Web service**

This is a system-to-system interface for HI Service transactions such as locating and retrieving an individual's IHI. It is often referred to as a business-to-business (B2B) interface.

This interface connects local healthcare business systems to the HI Service. Typical healthcare business systems that are expected to use this interface would include general practice systems, patient administration systems, emergency department systems, directory services etc.

#### **6.5.3 Web portal**

This is a website where healthcare individuals are able to view the information attached to their IHI, as well as the audit log of any events associated with the record. A healthcare individual is able to contact a HI Service officer to obtain further information about specific events. Healthcare individuals will need to register for access to the portal.

Healthcare providers are able to use a web portal to perform a range of HI Service interactions related to their provider information<sup>19</sup>.

#### **6.5.4 Telephone support**

HI Service officers can assist healthcare individuals or providers by way of the telephone.

The available telephone support channels are:

- A common Call Centre channel for IHIs, HPI-Is and HPI-Os. This channel will service requests for business transactions and accept reports of technical problems with the HI Service.
- An Online Technical Support desk for implementers (software vendors etc) which manages the test environment and provides software support documentation.

---

<sup>19</sup> Currently provided by Healthcare Provider Online Service (HPOS)

## 6.6 User Roles

There are a number of core business roles identified within the HI Service:

- Healthcare individuals
- Healthcare provider individuals
- Healthcare provider organisations
  - Authorised employees
  - Responsible Officers
  - Organisation Maintenance Officers
- HI Service Operator
  - HI Service officers
  - System administrators

Refer to the Business Use Cases in [Appendix A](#) for further detail on how these roles interact with the HI Service.

### 6.6.1 Support and Operation Roles

The HI Service Operator is responsible for the effective operation of the system.

#### 6.6.1.1 Roles of other organisations and services

There are a number of other organisations and services that are essential to the overall functioning of the HI Service.

- Trusted Data Sources
- Authorised HI Service Agents
- Authentication Service
- Reference Data Sources

#### 6.6.1.2 Trusted Data Sources

Trusted Data Sources are accredited and authorised to provide demographic and professional data to populate the IHI and HPI-I records.

Data that is provided to the HI Service by TDSs will be maintained through a one-way synchronisation of data from the TDS. TDSs will be the authoritative source for data they supply for HPI-Is, and will be the only party able to modify such data.

The TDSs currently identified are:

- Medicare Australia, as a source of verified healthcare individual data



- Department of Veteran Affairs (DVA), as a source of verified healthcare individual data
- Australian Health Practitioner Regulation Agency (AHPRA), as a source of individual healthcare provider data for an initially identified set of ten registered healthcare professions<sup>20</sup>

#### **6.6.1.3 Authorised HI Service Agents**

To assist management of the HI Service and enable distributed management of the HI Service, approved organisations may be given authority to act as agents of the HI Service.

#### **6.6.1.4 Authentication Service**

The HI Service will use the National Authentication Service for Health (NASH) to provide security credentials for healthcare provider individuals and organisations. These credentials will be used for:

- Accessing the HI Service
- Asserting their identity when participating in e-health

#### **6.6.1.5 Reference Data Sources**

Reference data sources may be used, where appropriate, to validate particular data fields in the HI Service records; for example, postcodes.

### **6.7 Support environment**

The initial HI Service Operator will be Medicare Australia, whose existing information and service infrastructure is being leveraged, where appropriate, and extended, to establish the HI Service.

Healthcare consumer and provider confidence is supported by the experience and trusted status of Medicare Australia, in delivering national health related services.

Implementation of healthcare identifiers will be supported by a legislative framework to underpin the governance, privacy and agreed uses for national healthcare identifier reference numbers.

Specifically, it is intended that the legislative framework will:

---

<sup>20</sup> "Ten national boards have been established under the Health Practitioner Regulation (Administrative Arrangements) National Law Act 2008. These boards are: Chiropractic Board of Australia, Dental Board of Australia (includes the professions of dentist, dental therapist, dental hygienist or dental prosthetist), Medical Board of Australia, Nursing and Midwifery Board of Australia, Optometry Board of Australia, Osteopathy Board of Australia, Pharmacy Board of Australia, Physiotherapy Board of Australia, Podiatry Board of Australia, and Psychology Board of Australia." (Source: <http://www.ahpra.gov.au/>)

- Establish arrangements for operating the HI Service, initially by providing Medicare Australia with the function to operate the HI Service
- Set out limits for the use of healthcare identifiers to healthcare information management and communications purposes, as part of delivering healthcare services, and appropriate other uses of healthcare identifiers for related purposes, including for management of health services and health research, as well as any other authorised or required by law exceptions
- Establish the process for eligibility and participation
- Establish processes for inquiry and complaint
- Establish penalties for the misuse of healthcare identifiers
- Describe how privacy laws will apply to the use of healthcare identifiers
- Provide for review of the framework within a defined period

Support for healthcare software developers will be provided. This will include:

- On-line technical support
- Support documentation
- Test environment
- Compliance, certification and accreditation

### **6.7.1 HI Service Availability**

The HI Service will be available through the Service Channels (described in Section 6.5) as follows:

- Web Services and Web Portal access to the HI Service will be available 24 hours a day, 7 days a week subject to agreed service levels
- Call centres and phone support will be available within business hours on all business days where:
  - Business days are any day other than a Saturday, Sunday or public holiday (including public service holidays) throughout Australia, promulgated in the Commonwealth of Australia Gazette.
  - Business Hours are 8.30 AM to 6:00 PM in any Australian time zone on a Business Day.

## 7 Summary of impacts

The HI Service is a new, national identifier service which does not replace an existing national identifier service. The impacts therefore are primarily associated with the introduction and use of the HI Service within the healthcare sector.

The impact on, and extent of change management required by, healthcare provider organisations and provider individuals will vary depending on a number of factors, including:

- Type of healthcare services provided
- Organisation size
- Existing e-health capability
- Level of participation

This section describes the expected operational and organisational impacts that are likely to arise from participation in the HI Service by healthcare organisations.

There are three main areas of impact:

- Organisation
- Start-Up
- Operation

### 7.1 Organisational impacts

Some of the considerations for an organisation in terms of roles and responsibilities in relation to the HI Service are:

- Changes in roles or positions
- Skill upgrades
- Business process changes
- Change management processes
- Ensuring compliance with relevant regulations

### 7.2 Start-Up Impacts for Organisations

Some of the considerations for an organisation when preparing to participate in the HI Service are:

- Patient and Provider Identifiers
  - Develop strategy for handling new and existing identifiers
  - Implement business system changes
- Changes to Computer system
  - Acquire computer system if required

- Upgrade or obtain new software
  - Obtain reliable internet access
  - Manage the migration process
- Authentication
  - Request NASH certificates
  - Configure systems
- Organisational Maintenance
  - Create seed HPI-O
  - Validate associated HPI-Is
  - Create static link with HPI-Is if desired
  - Populate HI PDS record if desired
- Education and Training
  - Computer Systems
  - Business Processes

### **7.3 Operational impacts for Organisations**

Some of the considerations for an organisation when preparing for 'business as usual' operation with the HI Service are:

- Business processes
  - Use of the HI Service and national identifiers
  - Alternative processes developed for operation when access to the HI Service is not available
- Computer system
  - Keep system up to date with any HI Service and NASH changes
  - Authentication
  - Maintain certificates as appropriate
- Organisational Maintenance
  - Maintain HPI-O network hierarchy if appropriate
  - Maintain associated HPI-Is if appropriate
  - Maintain static link with HPI-Is if desired
  - Maintain Provider Directory Service entry if desired
  - Maintain seed organisation status with HI Service
- Education and Training
  - Provide training as required
  - Patient communication about IHIs and the HI Service

## 8 Analysis of the HI Service

This section provides an analysis of the benefits, new and enhanced capabilities, limitations and trade-offs that have been considered in the design and development of the HI Service.

### 8.1 Benefits

Implementation of e-health across the Australian healthcare sector will deliver a safer, more sustainable health system through<sup>21</sup>:

- More secure, convenient and coordinated interactions across the many different parts of the health system
- Better consumer access to health information
- More informed and efficient care and treatment decision-making by healthcare providers
- Better understanding of what is happening in the health system and more informed population health surveillance, policy development, service planning and management
- Improved healthcare provider access to decision support tools, such as up-to-date consumer information and knowledge sources, at the point of care

The HI Service supports this by:

- National healthcare identifiers for consistently identifying healthcare individuals and providers, and enabling an association between identifiers and the related medical records
- Healthcare identifiers that are consistent across traditional federal/state/local boundaries and cross-sector boundaries will make it easier to exchange information with a greater level of confidence and reliability in identifying a healthcare individual or provider (individual and organisation)
- Use of authorised/accredited tokens such as Medicare cards, to assist healthcare providers to search reliably for and retrieve IHIs
- Provisional or unverified IHIs may be created under certain circumstances

Providing opportunities to improve patient privacy and accountability for information management The HI Service will:

---

<sup>21</sup> For a more comprehensive discussion on this, please refer to the National E-Health Strategy Summary

- Minimise the likelihood of health information being sent to the wrong healthcare provider or being associated with the wrong healthcare individual
- Minimise the administrative processes for participation by healthcare provider individuals and organisations
- Maximise the possibility that health information about a healthcare individual can be assembled from multiple providers and locations
- Maximise the effective use of health information for automated clinical decision support
- Reduce duplication of investigations and diagnostic tests, as a result of information being more readily available and easier to find
- Reduce errors and increase efficiency in handling health information

Additionally, the HI Service will enable:

- Unique and consistent identification of healthcare individuals at the point of care
- Consistent association of health information to a healthcare individual within a healthcare context, including electronic communications (such as discharge summaries and referrals)
- The development and implementation of processes to support use of information for statistical and reporting purposes
- Administrative efficiencies by reducing the need to capture the same information numerous times
- Improved decision support for healthcare providers and healthcare individuals, and improved patient information leading to a potential reduction in adverse events and improved treatment effectiveness
- Improved communication between healthcare providers during an individual's treatment
- More efficient record keeping
- Significant improvement for healthcare individuals in the volume, quality and granularity of health information available for better managing their health
- Reduction in time that consumers and care providers spend manually booking appointments, ordering treatments, and repeating/sharing information across the health sector

### **8.1.1 Decommissioned capabilities**

The HI Service provides an opportunity to decommission or improve the maintenance of existing individual health consumer and provider index systems. These systems are managed by hospitals, community healthcare providers, community imaging and laboratory services, pharmacies and jurisdictional health departments. Substantial investment is currently required by these organisations to maintain the integrity of these systems.

## **8.2 Limitations**

The National E-Health Strategy Summary highlights the issue of establishing realistic planning horizons for the steps in the journey to a pervasive e-health system for Australia. The HI Service is part of the first planning horizon, to establish the foundations for e-health.

As the first major foundational service component to be delivered, there have been many expectations that the HI Service will deliver capabilities which are not achievable without other e-health services, systems and components being available. The scope of the HI Service has been limited to delivering the essential identifier capabilities to provide a good foundation for further development of the overall e-health environment in Australia.

A roadmap approach has been adopted for further development of the HI Service capabilities. The roadmap will involve further phases of requirements' gathering and consultation, and this will provide the opportunity to address aspects of the HI Service which may be considered limiting as the e-health environment evolves.

## **8.3 Alternatives and trade-offs considered**

The policy setting for the initial design for the individual healthcare identifier was for participation to be on a voluntary basis. Through consultation with jurisdictional and key healthcare provider stakeholders on refining the original design of the HI Service, it became apparent that the policy setting for voluntary participation for healthcare individuals in the HI Service posed clear impediments to the widespread adoption of IHIs as a primary identifier.

The efficiency gains for healthcare providers, and the quality and safety benefits for consumers, are dependent on the widespread adoption of IHIs.

The original policy setting of voluntary participation by healthcare individuals meant that healthcare individuals had the option of withdrawing participation at any time. This had the effect of preventing the adoption of the IHI as a primary identifier by healthcare providers, as the status of an IHI could change from active to inactive at any time.

The inability to adopt the IHI as a primary identifier would reduce the reliability of matching the right person with the right health information and impede the development of automated processes to manage the communication of health information between healthcare providers.

The Australian Health Ministers' Advisory Council (AHMAC) considered advice from the National E-Health and Information Principle Committee, including advice from NEHTA, the NHCIOF and the NHIRF working group, and agreed that the policy settings should be changed to ensure widespread uptake of the IHI.

In November 2008, following advice received from AHMC, COAG re-affirmed its support for a national approach to healthcare identifiers and agreed to the assignment of an IHI as a universal unique identifier assigned to all individuals receiving healthcare in Australia, rather than uptake of IHIs on a voluntary participation basis.



## 9 Business Use Cases

Appendix A presents a set of Business Use Cases that illustrate the expected use of the HI Service by healthcare individuals, healthcare provider individuals and healthcare provider organisations.

This section describes a representative set of Business Use Cases for the HI Service.

They are focused on business activities that occur in relation to the HI Service. Business Use Cases that illustrate and describe the use of identifiers in e-health solutions are outside the scope of this document.

### 9.1 IHI Business Use Cases

#### **UC.010 - Presentation at a healthcare facility with a TDS identifier**

Where an individual presents at a healthcare facility with a TDS identifier, the identifier can be used to locate their IHI. This process would be used for:

1. A new patient; or
2. A known patient where no IHI has been associated with their patient record.

#### **UC.011 – Presentation at a healthcare facility without providing a TDS identifier**

Where an individual presents at a healthcare facility without providing a TDS identifier, the IHI can be located using identifying information. This process would be used for:

1. A new patient; or
2. A known patient where no IHI has been associated with their patient record.

#### **UC.021 – A person enrolls with a Trusted Data source**

When an individual enrolls with a TDS they will automatically be allocated a verified IHI.

#### **UC.030 – Batch IHI search against HI Service for initial IHI load**

A healthcare facility initiates a batch search against records held by the HI Service, in order to initially populate a healthcare facility's patient index with matching verified IHIs for patients known to the healthcare facility.

**UC.031 – Batch IHI search against HI Service for IHI data quality**

A healthcare facility initiates a batch search against records held by the HI Service in order to:

- locate IHIs for patients known to the healthcare facility; and/or
- validate IHIs stored in their local system

This will assist with maintenance of locally stored information.

**UC.040 – Verification (EOI) for an unverified IHI**

A healthcare individual may request that an unverified IHI record created for him/her be verified via a HI Service officer.

**UC.060 – Create unverified IHI for newborn**

An IHI can be created for a newborn.

**UC.070 – Unconscious/incapacitated and unknown individual**

When an individual who is unknown to a healthcare facility presents in an unconscious or incapacitated state (without any form of identification), the healthcare facility can create a provisional IHI to be associated with the patient record.

**UC.081 – Provide pseudonymous IHI for healthcare individual**

A healthcare individual who believes they may have reason(s) to protect their identity in healthcare settings can request a pseudonymous IHI from the HI Service.

**UC.083 – Creation of an alternate name**

Healthcare individuals may request that an alternate name (alias) be associated with their verified IHI.

**UC.112 – Maintain an unverified IHI**

At the request of the healthcare individual, a healthcare facility can update information associated with unverified IHIs.

**9.2 HPI-O Business Use Cases****UC.130 - Establish seed HPI-O**

A 'seed' HPI-O is the overarching organisational identifier issued to an eligible healthcare provider organisation, from which additional 'networked' HPI-Os may be created for those parts of the organisation.

**UC.131 – Establish Organisation Maintenance Officer**

A Healthcare Provider Organisation needs to establish one or more OMO.

The role is established by the RO or another OMO with authority to establish additional OMOs, through the HI Service.

An RO may also take on the role of OMO.

**UC.135 – Establish a networked HPI-O**

A seed HPI-O may have a hierarchy of associated network HPI-Os.

**UC.136 – Reconfigure HPI-Os (mergers or acquisitions of healthcare provider organisations)**

After the merger or acquisition of a healthcare provider organisation, the RO of the primary HPI-O may request a merging of the HPI-Os for those organisations affected by the merger or acquisition.

**UC.170 – Maintain HPI-O**

An OMO with appropriate authority maintains information associated to a HPI-O. They may:

- Update information associated with the HPI-O and, where appropriate, display the updated information in the HI Provider Directory Service
- Show or not show HPI-O information in the HI Provider Directory Service
- Enable/Disable access to electronic address for the HPI-O

Change (update) parent HPI-O An OMO may be assigned all privileges for maintenance of an HPI-O.

**UC.172 – Retire a seed HPI-O**

The RO of a healthcare provider organisation may request the retirement of the seed HPI-O of the organisation through the HI Service officer.

**UC.173 – Retire a networked HPI-O**

The OMO of a healthcare provider organisation may request the retirement of a networked HPI-O(s) for which they have authority.

The retirement of a networked HPI-O will involve the retirement of HPI-O(s) that are subordinate to the HPI-O being retired.

### **9.3 HPI-I Business Use Cases**

#### **UC-180 – New professional registration through a Trusted Data Source (TDS)**

Eligible healthcare provider individuals can be allocated an HPI-I through an associated TDS.

Any changes to healthcare provider individual details that have been supplied by the TDS are also updated by the TDS.

#### **UC.182 – Create or maintain HPI-I through the HI Service**

Eligible healthcare provider individuals who are not allocated a HPI-I through a TDS can be allocated a HPI-I by the HI Service.

HPI-Is allocated by the HI Service are maintained through the HI Service.

#### **UC.210 – Link HPI-I with HPI-O in HI Provider Directory Service**

With the agreement of a healthcare provider individual, an OMO may create a link in the HI PDS between the HPI-I and an HPI-O for which they are responsible.

#### **UC.220 – Retire HPI-I**

A HPI-I is retired when the HI Service receives notification that a healthcare provider individual is deceased.

#### **UC.222 – HPI-I maintains details through web portal access**

A healthcare provider individual is able to view their HPI-I record, and update limited information associated with their HPI-I via a web portal.

#### **UC.224 – Validate HPI-I and status**

When a healthcare provider organisation needs to validate an HPI-I associated with their organisation, they can access the information from the HI Service.

#### **UC.232 – Locate provider (HPI-I or HPI-O) in HI Provider Directory Service**

Users who are appropriately authorised may search or browse the HI PDS for HPI-I(s) or HPI-O(s) and associated information.

## Appendix A - Business Use Case

This appendix contains the expanded versions of the Business Use Cases listed in Section 9. The Business Use Cases provided are listed in the following table.

IHI Business Use Cases	HPI-O Business Use Cases	HPI-I Business Use Cases
UC.010 – Presentation at a healthcare facility with a TDS identifier	UC.130 – Establish seed HPI-O	UC.180 – New professional registration through a TDS (create HPI-I)
UC.011 – Presentation at a healthcare facility without a TDS identifier	UC.131 – Establish Organisation Maintenance Officer	UC.182 – Create or maintain HPI-I through the HI Service
UC.021 – A person enrolls with a Trusted Data source	UC.135 – Establish a networked HPI-O	UC.210 – Link HPI-I with HPI-O in HI Provider Directory Service
UC.030 – Batch IHI search against HI Service for initial IHI load	UC.136 – Reconfigure HPI-Os (mergers or acquisitions of healthcare provider organisations)	UC.220 – Retire HPI-I
UC.031 – Batch IHI search against HI Service for data quality	UC.170 – Maintain HPI-O	UC.222 – HPI-I maintains details through web portal access
UC.040 – Verification (EOI) for an unverified IHI	UC.172 – Retire a seed HPI-O	UC.224 – Validate HPI-I and status
UC.060 – Create unverified IHI for newborn	UC.173 – Retire a networked HPI-O	UC.232 – Locate healthcare provider (HPI-I or HPI-O) in HI Provider Directory Service
UC.070 – Unconscious/incapacitated and unknown patient		
UC.081 – Provide pseudonymous IHI for healthcare individual		
UC.083 – Creation of an alternate name		
UC.112 – Maintain an unverified IHI		

## UC.010 - Presentation at a healthcare facility with a TDS identifier

### Description

Where an individual presents at a healthcare facility with a TDS identifier, the identifier can be used to locate their IHI. This process would be used for:

1. A new patient; or
2. A known patient where no IHI has been associated with their patient record.

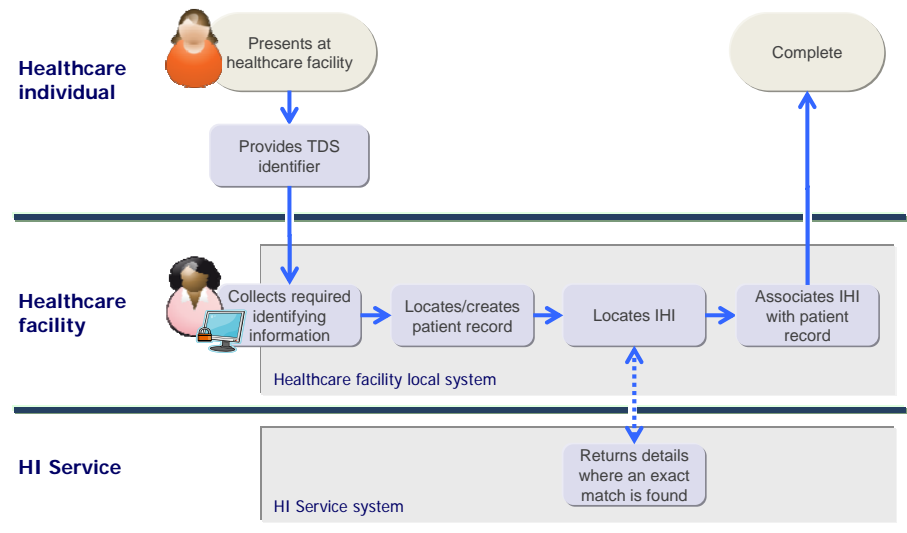
### Participants

Healthcare individual, Healthcare facility, HI Service

### Process Overview

An individual attends a healthcare facility and provides identifying information required to locate or create a patient record.

Where there is no IHI associated with the patient record and the individual has provided an identifier allocated to them by a TDS, the identifier combined with the individual's name and date of birth is used to locate their IHI. The retrieved IHI is then associated with the patient record.



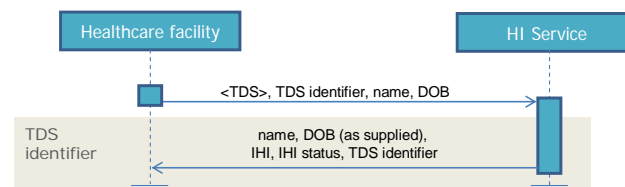
### Operational Policy

The status of the IHI located using the TDS identifier will be 'verified'.

### Relevant High Level IHI Business Requirements

BR.2009.08.200 Facilitate consistent and efficient identification of healthcare individuals at the point of care via the use of a Trusted Data Source identifier.

### Interaction with HI Service



### Accredited/authorised token

Tokens issued by TDS are defined as accredited/authorised tokens for the HI Service.

The TDS identifier that has been allocated to the healthcare individual may be accessible through the number on these tokens.

### Possibility of not locating an IHI with a TDS identifier

It is possible that an IHI will not be located in response to a search using a TDS identifier if incorrect information is entered.

In these circumstances, after first checking the accuracy of the TDS identifier and other search criteria, the standard search parameters as identified in UC.011 may be followed to locate the IHI for the individual. The HI Service officer should be contacted before creating an unverified IHI where a TDS identifier has been provided.

## UC.011 – Presentation at a healthcare facility without a TDS identifier

### Description

Where an individual presents at the healthcare facility without providing a TDS identifier, the IHI can be located using identifying information. This process would be used for:

1. A new patient; or
2. A known patient where no IHI has been associated with their patient record.

### Participants

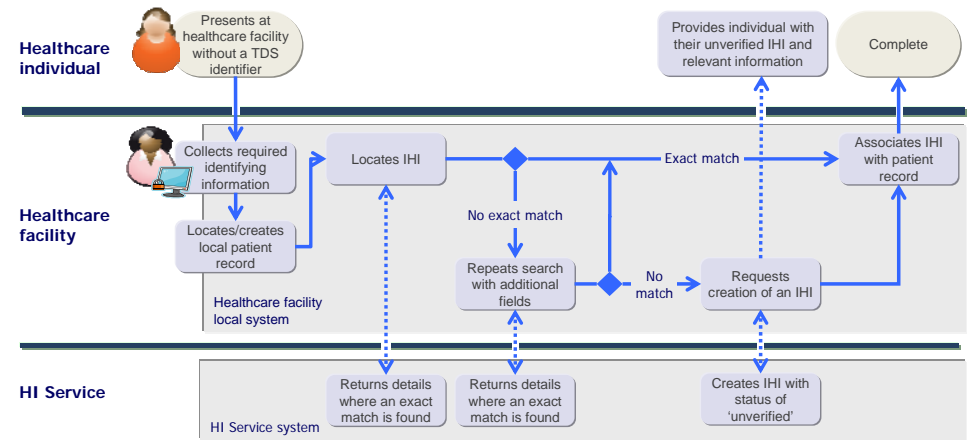
Healthcare individual, Healthcare facility, HI Service

### Process Overview

An individual attends a healthcare facility and provides identifying information required to locate or create a patient record.

Where there is no IHI associated with the patient record, identifying information provided by the individual can be used to locate their IHI. The retrieved IHI is then associated with their patient record.

Where the search for an individual's IHI is unsuccessful, the healthcare facility can create an unverified IHI for the individual.



### Search methodology

Using identifying information to locate an individual's IHI may be conducted as follows:

1. An initial attempt to locate the IHI is conducted using the supplied name, DOB information
2. If no match is returned, a further search may be conducted providing the individual's address and/or sex in addition to their name and DOB

Where no match is returned, an unverified IHI can be created.

The HI Service will only return identifying information provided by the healthcare facility

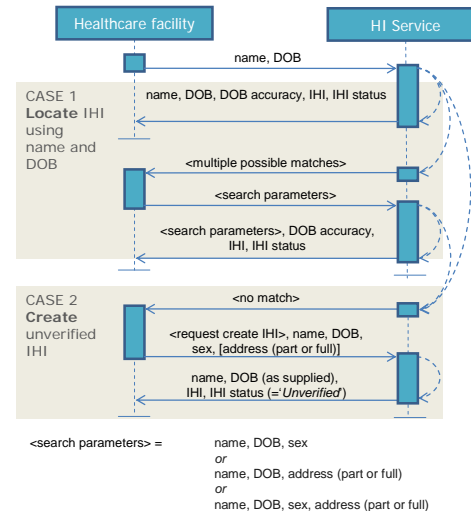
### Relevant High Level IHI Business Requirements

BR.2009.08.190 Enable authorised users to create a new IHI and associated record at the point of care

BR.2009.08.205 Enable a healthcare individual to be allocated an IHI without providing assurances of their identity at the point of care

BR.2009.08.265 Support authorised healthcare providers to retrieve an IHI and associated status via a demographic search in the absence of Trusted Data Source identifier

### Interaction with HI Service



## UC.021 – A person enrolls with a Trusted Data Source

### Description

When an individual enrolls with a TDS they will automatically be allocated a verified IHI.

### Participants

Healthcare individual, TDS, HI Service

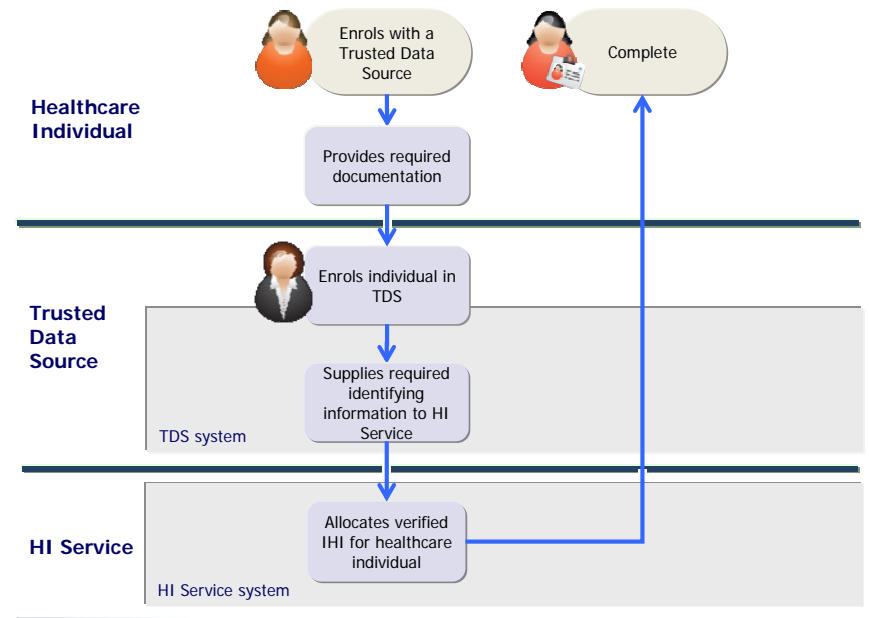
### Process Overview

An individual enrolls with a TDS.

The individual's identifying information is provided to the HI Service which automatically allocates a verified IHI.

The individual's TDS identifier is associated with the IHI to support searching for the IHI by healthcare facilities.

A TDS may provide identifying information on new enrolments to the HI Service in a regular batch process.



### Policy

The HI Service recognises TDSs as a source of verified identifying information for the purpose of creating IHIs.

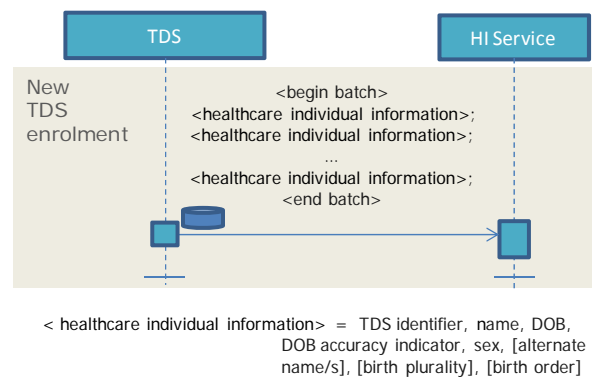
Individuals who enrol with TDSs will automatically be allocated a verified IHI.

### Relevant High Level IHI Business Requirements

BR.2009.08.200 Facilitate consistent and efficient identification of healthcare individuals at the point of care via the use of a Trusted Data Source identifier

BR.2009.08.210 Automatically allocate an IHI to a healthcare individual enrolling for the first time with a Trusted Data Source

### Interaction with HI Service



### Multiple Enrolments

Where an individual has previously been allocated a verified IHI, their TDS identifier will be added to their existing verified IHI.

The HI Service will not attempt to resolve any potential duplicates where an individual appears to have already been allocated an unverified IHI unless the healthcare individual requests resolution.



UC.030 – Batch IHI search against HI service for initial IHI load

Description

A healthcare facility initiates a batch search against records held by the HI Service, in order to initially populate a healthcare facility's patient index with matching verified IHIs for patients already known to the healthcare facility.

Participants

Healthcare facility, HI Service

Process Overview

A healthcare facility collates a list of patient records from its local patient index for cross checking, formats the information required and initiates the batch search process.

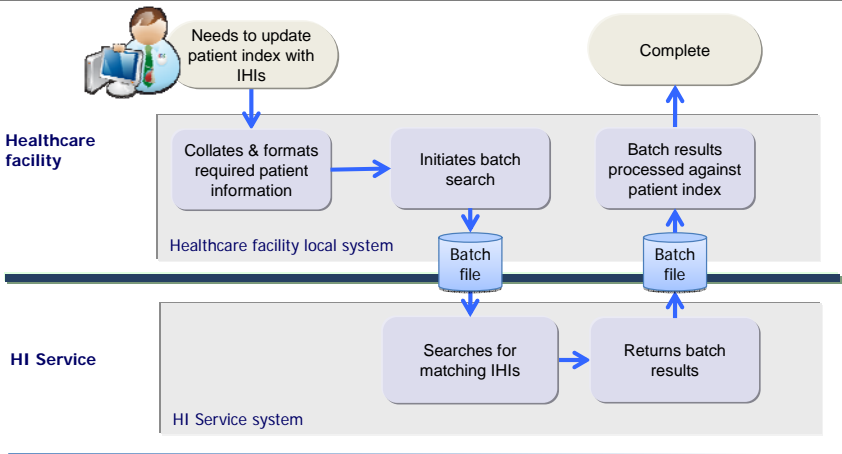
The batch file provided to the HI Service will contain either:

- TDS identifier, name, DOB; and/or
- TDS identifier, name, DOB, sex; and/or
- Name, DOB, sex, address (part or full)

The HI Service will attempt to locate an IHI for each set of search criteria contained in the batch.

If an exact match is found, the HI Service will return the IHI, IHI status and a DOB accuracy indicator in addition to the information supplied for the search.

Where the information cannot be matched, the HI Service will return an error message indicating the type of error. This could include either no match or multiple possible matches.



Operational Policy

Batch searches may only be conducted in relation to individuals known to the healthcare facility.

Quality of Service

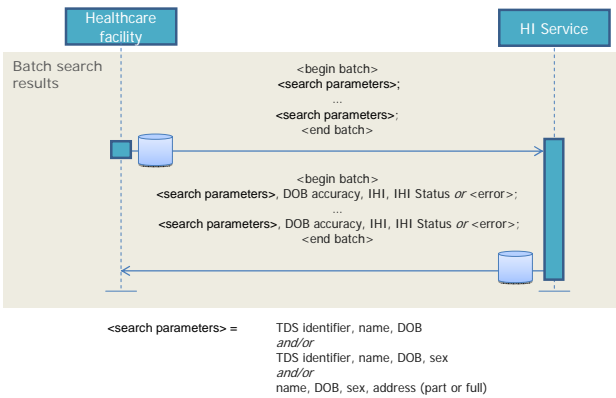
Executing a batch search will be subject to defined parameters set out in participation arrangements, including permissible timing, frequency and size of batch searches, to ensure that the conduct of batch searches does not adversely impact the performance of the HI Service.

Relevant High Level IHI Business Requirements

BR.2009.08.100 Support the healthcare sector by providing healthcare identifier services which are highly available

BR.2009.08.260 Support batch searches by healthcare provider organisations returning IHIs and associated status

Interaction with HI Service



Standards

The data elements used to conduct the batch search will be compliant with Australian and International Standards [AS5017, ISO/PDTS 22220].

UC.031 – Batch IHI search against HI Service for data quality

Description

A healthcare facility initiates a batch search against records held by the HI Service in order to:

- locate IHIs for patients known to the healthcare facility; and/or
- validate IHIs stored in their local system

This will assist with maintenance of locally stored information.

Participants

Healthcare facility, HI Service

Process Overview

A healthcare facility collates a list of patient records from its local patient index for cross checking, formats the information and initiates the batch search process.

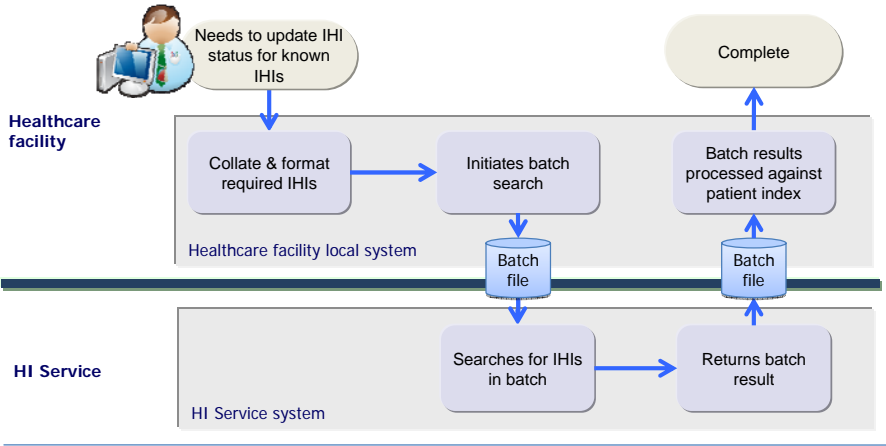
The batch file provided to the HI Service will contain either:

- TDS identifier, name, DOB; and/or
- TDS identifier, name, DOB, sex; and/or
- Name, DOB, sex, address (part or full); and/or
- IHI, name, DOB

The HI Service will attempt to locate an IHI for each set of search criteria contained in the batch.

If an exact match is found, the HI Service will return the IHI, IHI Status and a DOB accuracy indicator, in addition to the information supplied for the search.

Where the information cannot be matched, the HI Service will return an error message indicating the type of error. This could include either no match or multiple possible matches.



Operational Policy

Batch searches may only be conducted in relation to individuals known to the healthcare facility.

Quality of Service

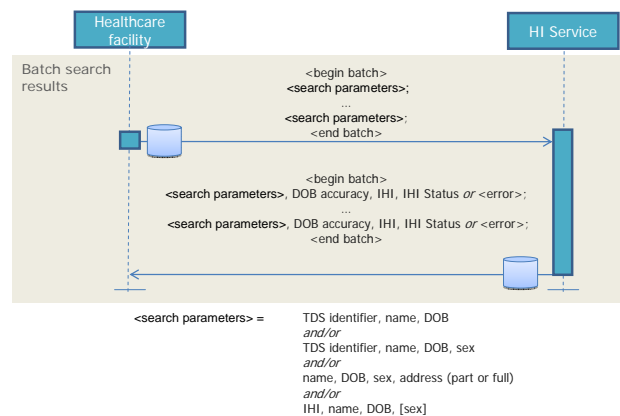
Executing a batch search will be subject to defined parameters set out in participation arrangements, including permissible timing, frequency and size of batch searches, to ensure that the conduct of batch searches does not adversely impact the performance of the HI Service.

Relevant High Level IHI Business Requirements

BR.2009.08.100 Support the healthcare sector by providing healthcare identifier services which are highly available

BR.2009.08.260 Support batch searches by healthcare provider organisations returning IHIs and associated status

Interaction with HI Service



Standards

The data elements used to conduct the batch search will be compliant with Australian and International Standards [AS5017, ISO/PDTS 22220].

IHI and status

IHIs provided may be verified or unverified, and where an IHI is provided that has been confirmed as duplicate or replica, an appropriate error message, and the correct IHI, will be returned.

## UC.040 – Verification (EOI) for an unverified IHI

### Description

. A healthcare individual may request that an unverified IHI created for him/her be verified via a HI Service officer.

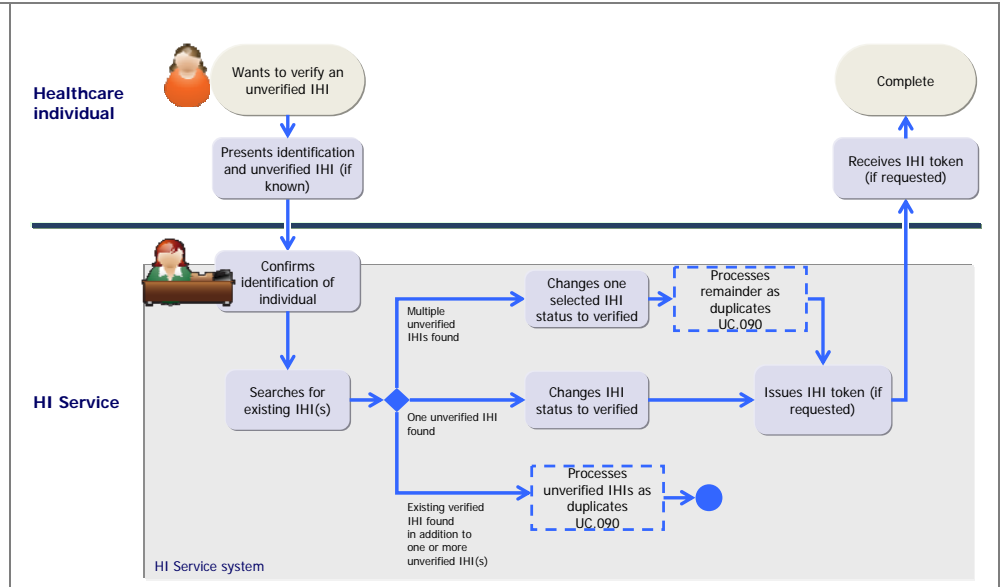
### Participants

Healthcare individual, HI Service

### Process Overview

An individual presents to a HI Service officer to verify an unverified IHI. The healthcare individual is identified and the HI Service officer searches for existing IHIs. Three possibilities are identified:

- If only a single unverified IHI is found the status will be changed to 'verified', and a HI Service token will be issued if required.
- If multiple unverified IHIs are found the status of one unverified IHI will be changed to 'verified' and the remaining unverified IHIs will be treated as duplicates.
- If an existing verified IHI is found in addition to one or more unverified IHIs the unverified IHIs will be treated as duplicates.



### Policy

The primary purpose of the IHI is the consistent identification of all healthcare individuals.

The ability to consistently identify an individual is improved by establishing verified IHIs.

Verification improves the level of confidence with which information associated with an IHI can be used.

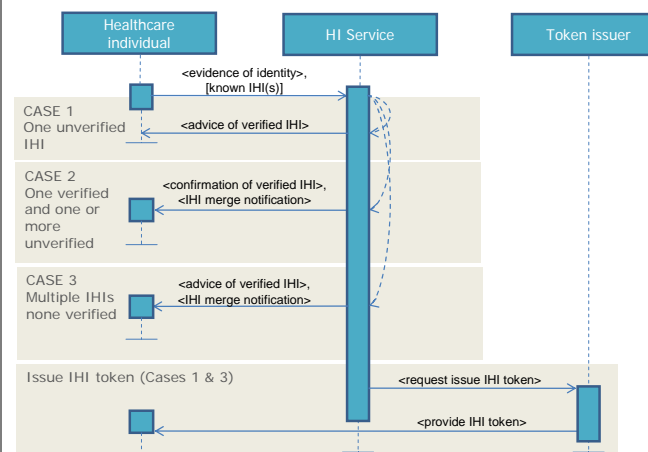
### Relevant High Level IHI Business Requirements

BR.2009.08.025 Enable consistent and accurate communications with healthcare individuals and healthcare providers

BR.2009.08.185 Allocate a unique identifier to all eligible healthcare individuals receiving health services in Australia

BR.2009.08.240 Develop and implement a national system, processes and services associated with the management of verified and unverified IHIs (including but not limited to collection, disclosure, access, use, maintenance and retirement)

### Interaction with HI Service



### Operational Note

The HI Service officer will have access to advanced search capabilities, including probabilistic and phonetic searching.

The HI Service officer will also locate any unverified IHIs that may also be assigned to the individual and resolve these as part of the verification process so that the individual has a single verified IHI.

## UC.060 – Create unverified IHI for newborn

### Description

An IHI can be created for a newborn.

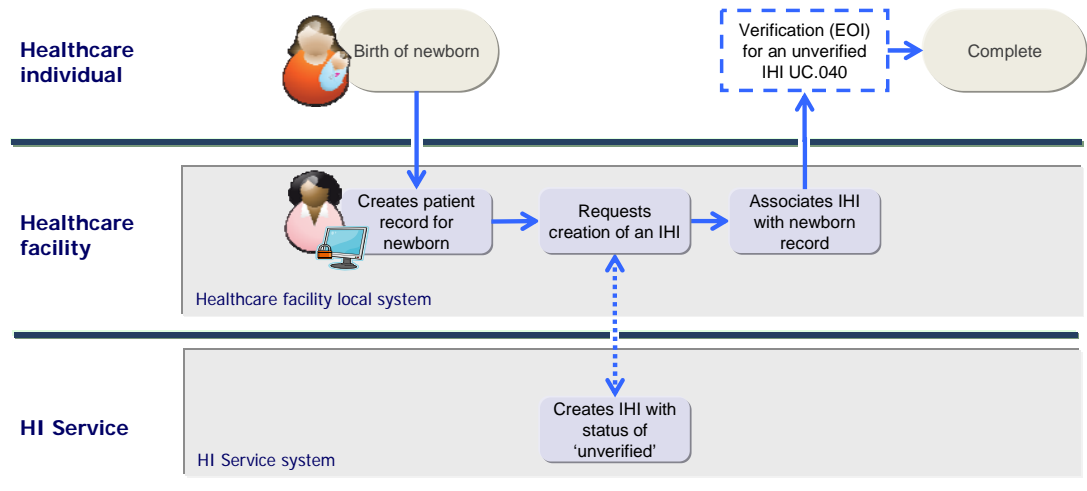
### Participants

Healthcare individual, Healthcare facility, HI Service

### Process Overview

Following the birth of a child, healthcare facility staff can create an unverified IHI to be associated with the newborn's patient record.

At a later time the parents or guardians can verify the unverified IHI, as per UC.040.

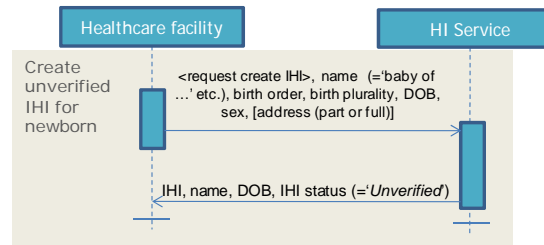


### Relevant High Level IHI Business Requirements

BR.2009.08.190 Enable authorised users to create a new IHI and associated record at the point of care

BR.2009.08.205 Enable a healthcare individual to be allocated an IHI without providing assurances of their identity at the point of care

### Interaction with HI Service



### Operational Note

Newborns can receive a verified IHI through their enrolment in a TDS, such as Medicare. This is discussed in UC.021.

## UC.070 – Unconscious/incapacitated and unknown individual

### Description

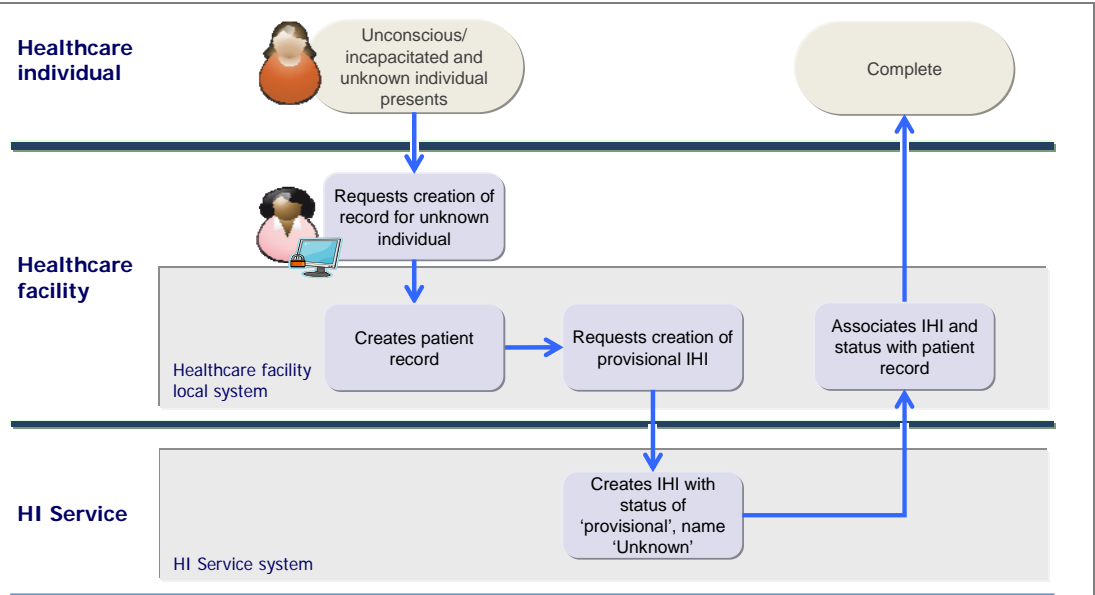
When an individual who is unknown to a healthcare facility presents in an unconscious or incapacitated state (without any form of identification), the healthcare facility can create a provisional IHI to be associated with the patient record.

### Participants

Healthcare individual, Healthcare facility, HI Service

### Process Overview

Healthcare facility staff can request the creation of a provisional IHI to be associated with the unknown patient's record.



### Operational Policy

IHI with status of provisional is intended for emergency situations where the individual is unknown to the facility and unable to communicate, and there is no identifying information available.

The status of a provisional IHI can be changed to unverified once a healthcare facility has sufficient information to identify the individual.

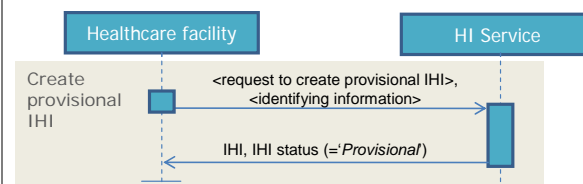
A provisional IHI may also be verified or merged with an existing IHI by the HI Service.

If the provisional IHI has not been merged, verified or become unverified within 90 days of issue, it will be retired.

### Relevant High Level IHI Business Requirements

BR.2009.08.230 Support the creation and maintenance of provisional IHIs by authorised healthcare providers

### Interaction with HI Service



### Naming Convention

AS5017 specifies that the name information stored with an unknown patient's record should be 'unknown'

## UC.081 – Provide pseudonymous IHI for healthcare individual

### Description

A healthcare individual who believes they may have reason(s) to protect their identity in healthcare settings can request a pseudonymous IHI from the HI Service.

### Participants

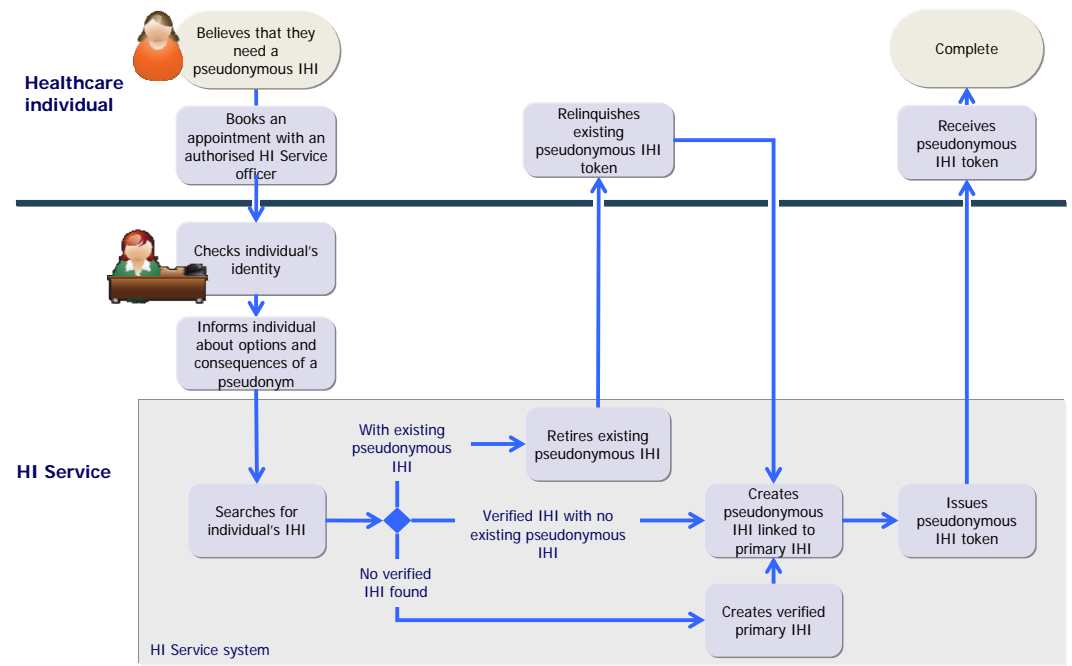
Healthcare individual, HI Service

### Process Overview

A healthcare individual makes a booking to meet with an HI Service officer who has authorisation to approve requests for a pseudonymous IHI.

The HI Service officer confirms that the healthcare individual has been informed about the options available and consequences of obtaining a pseudonymous IHI. The HI Service officer searches for any existing IHIs associated with the healthcare individual and where an existing pseudonymous IHI is located, it is retired and any existing pseudonymous IHI token is relinquished, before a new pseudonymous IHI is created.

The HI Service officer creates a pseudonymous IHI and links it to the healthcare individual's primary IHI.



### Operational Policy

The pseudonymous IHI will be linked to the healthcare individual's primary IHI through a confidential link which can only be accessed by a HI Service officer with the necessary privileges.

In cases where a healthcare individual feels that there is no longer a need for a pseudonymous IHI, they can revert to using their primary IHI. This requires the pseudonymous IHI to be retired.

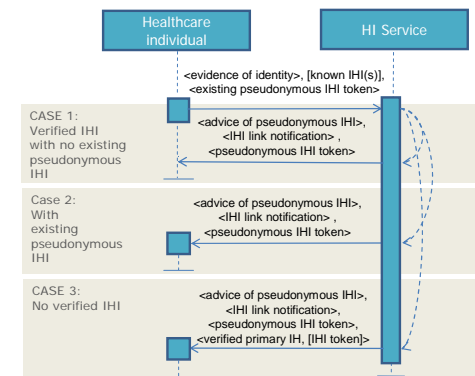
A healthcare individual may also choose to merge their pseudonymous IHI with their primary IHI.

The HI Service officer will provide appropriate information to the healthcare individual about the implications of creating and relinquishing a pseudonymous IHI.

### Relevant High Level IHI Business Requirements

BR.2009.08.250 Support the issuing of a new IHI and association of that new IHI with a pseudonym and other demographic information to be securely linked to an individual's primary IHI

### Interaction with HI Service



## UC.083 – Creation of an alternate name

### Description

A healthcare individual may request that an alternate name (alias) be associated with their verified IHI.

### Participants

Healthcare individual, HI Service

### Process Overview

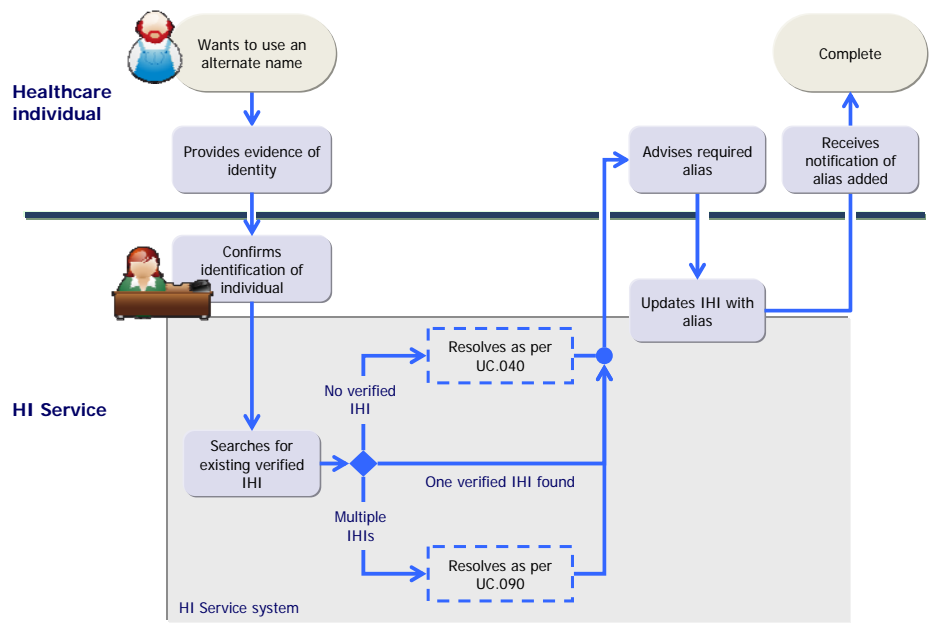
A healthcare individual attends a HI Service office and provides identifying information to locate their IHI.

After the HI Service officer has located the verified IHI, the healthcare individual advises the required alias.

The HI Service officer will associate the alias with the IHI and notify the healthcare individual.

During this process, the HI Service officer may:

- Verify an existing unverified IHI for the individual as per UC.040; or
- Resolve any duplicate IHIs as per UC.090



### Aliases

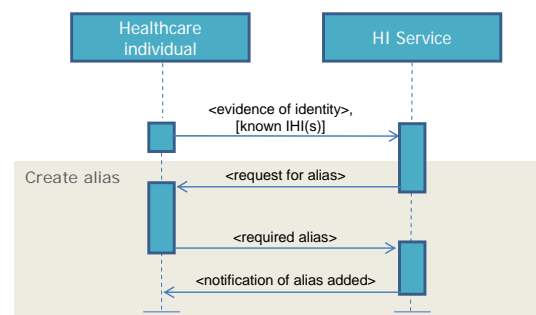
Aliases can only be associated with verified IHIs.

Aliases associated with an IHI can be used for searching IHIs.

### Relevant High Level IHI Business Requirements

BR.2009.09.290 The HI Service will provide a facility for healthcare individuals wishing to use alternate names.

### Interaction with HI Service



### Operational Notes

A verified IHI may have up to 9 aliases associated with it.

If an alias is used to locate a verified IHI, the HI Service will return identifying information without revealing other names or aliases associated with that IHI.

## UC.112 – Maintain an unverified IHI

### Description

At the request of the healthcare individual, a healthcare facility can update information associated with unverified IHIs.

### Participants

Healthcare individual, Healthcare facility, HI Service

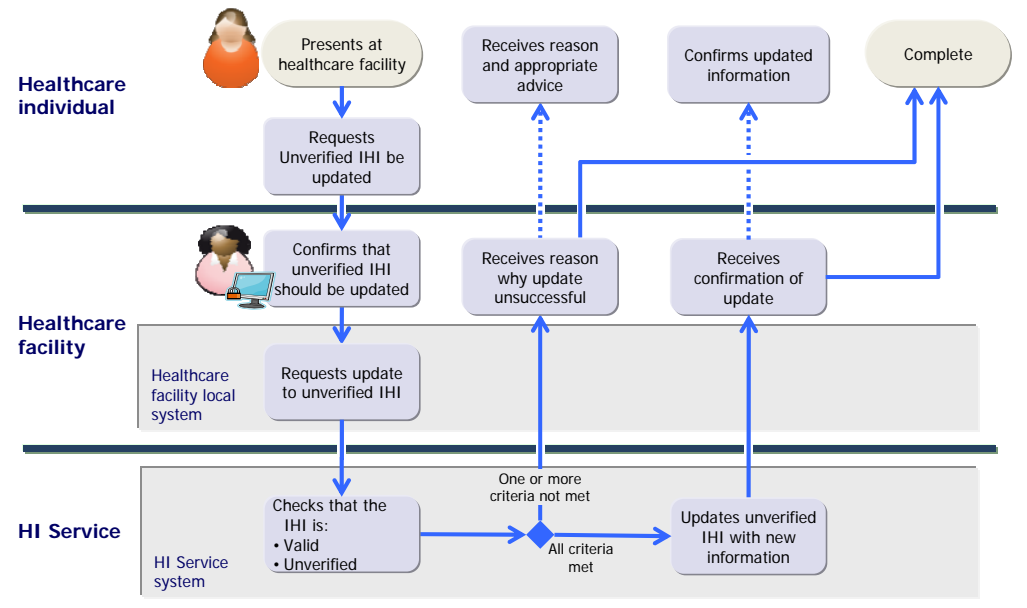
### Process Overview

The healthcare facility provides the unverified IHI, together with name and DOB details, plus the new information.

The HI Service will check that the IHI:

- Is valid, i.e. the IHI, name and DOB provided match the existing record in the HI Service; and
- Is unverified.

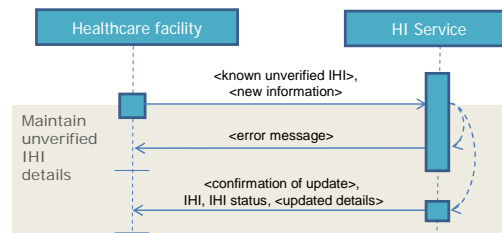
Where these conditions are met the IHI record will be updated. Where any one or more of these conditions are not met, the HI Service will return an error message.



### Relevant High Level IHI Business Requirements

BR.2009.08.225 Support authorised healthcare provider organisations to update unverified IHI records

### Interaction with HI Service



### IHI information that may be maintained

Through this process, a healthcare facility is able to maintain:

- Family Name\*
- Other Name details
- DOB\*
- Sex
- Address

\* = mandatory

Audit of changes to IHI

All changes to IHI information will be recorded in an audit log that may be accessed by the healthcare individual.



## UC.130 – Establish seed HPI -O

### Description

A 'seed' HPI-O is the overarching organisational identifier issued to an eligible healthcare provider organisation, from which additional 'networked' HPI-Os may be created for other parts of the organisation.

### Participants

Healthcare provider organisation (RO) , HI Service

### Process Overview

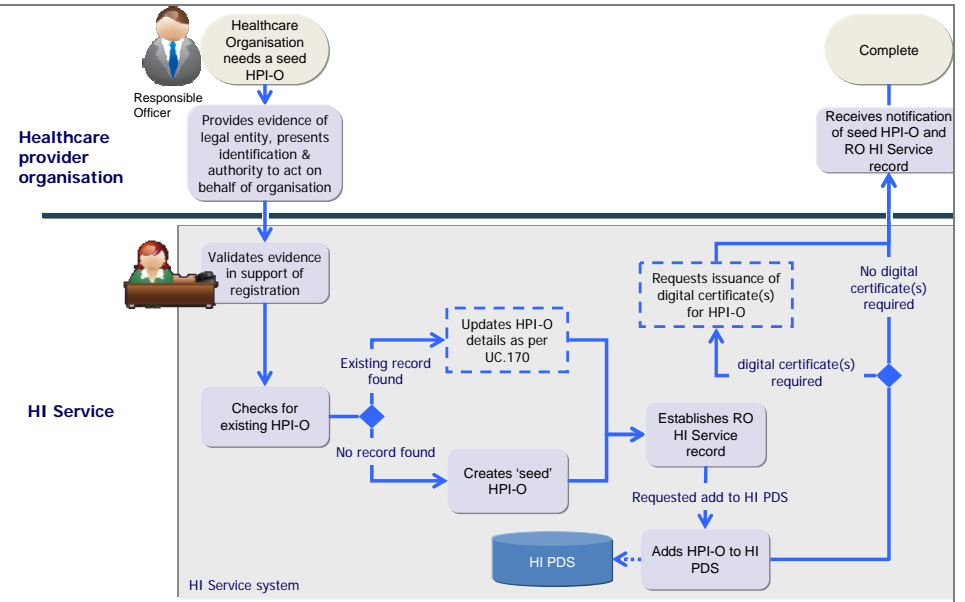
A nominated RO provides the HI Service with the required documentation in support of the request for a HPI-O. Two possibilities are identified:

- If no record is found, a new HPI-O with the classification of seed will be created.
- If an existing active seed HPI-O is found, the HPI-O details will be updated if needed.

The newly created HPI-O may be added to the HI PDS at the request of the RO. The RO may request HPI-O digital certificate(s).

### Note

While this process requires presentation of documentation, it will be supported through a number of channels.



### Operational Policy

A healthcare provider organisation will need to apply for a HPI-O and provide evidence supporting their eligibility and be required to comply with legislative requirements for participation in the HI Service.

A healthcare provider organisation will need to nominate individuals as their RO and OMO (may be the same individual). The nominated RO will need to supply the HI Service evidence of their identity and that they are empowered to act on behalf of the organisation.

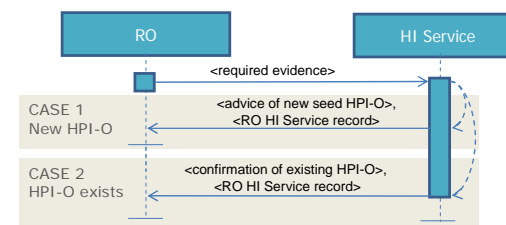
### Relevant High Level HPI Business Requirements

BR.2009.08.140 Create new HPI-Is and HPI-Os, and populate HPI-Is and HPI-Os with associated (and permitted) data; update and maintain existing HPI-Is and HPI-Os and their associated attributes; and retire HPI-Is and HPI-Os

BR.2009.08.045 At the point of issue of an HPI-I or HPI-O, accurately identify healthcare provider individuals and organisations

BR.2009.08.050 Allocate a unique identifier to all eligible healthcare provider individuals and organisations that require one

### Interaction with HI Service



Note: Case 2 represents situations where an active seed HPI-O already exists.

### Digital Certificate(s)

When a new seed HPI-O is created, digital certificate(s) may be requested.

Individuals or systems interacting online with the HI Service must have appropriate digital certificate(s)

## UC.131 – Establish Organisation Maintenance Officer

### Description

A Healthcare Provider Organisation needs to establish one or more OMO.

The role is established by the RO, or another OMO with authority to establish additional OMOs, through the HI Service.

A RO may also take on the role of OMO.

### Participants

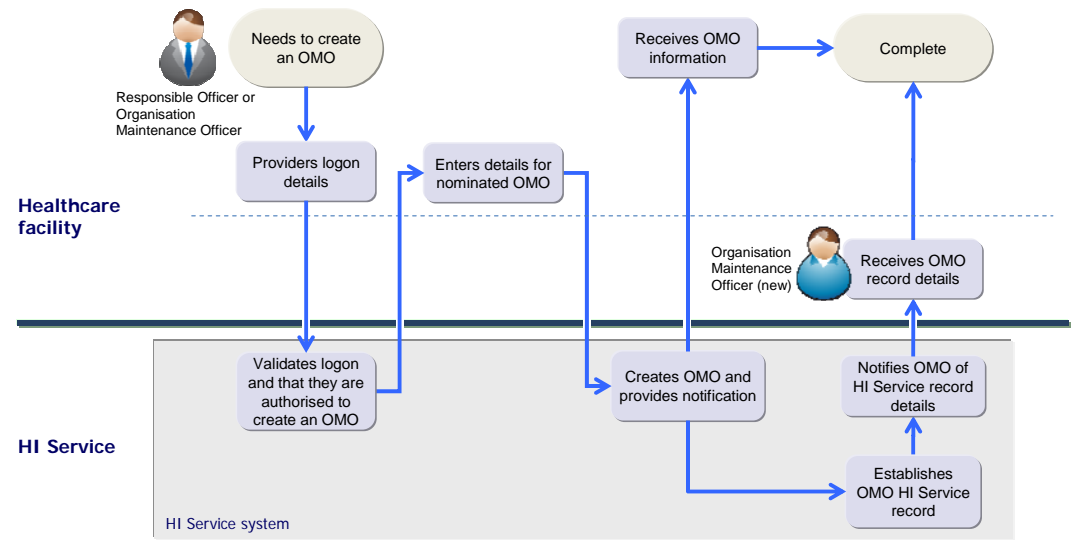
Healthcare facility (RO or OMO) , HI Service

### Process Overview

An existing RO or OMO with authority to establish additional OMOs logs on to the HI Service and enters the details for the new OMO.

The HI Service establishes the identified individual as an OMO and creates an HI Service record for them.

The requesting RO or OMO receives confirmation and the new OMO is notified of their HI Service record details.



### Operational Policy

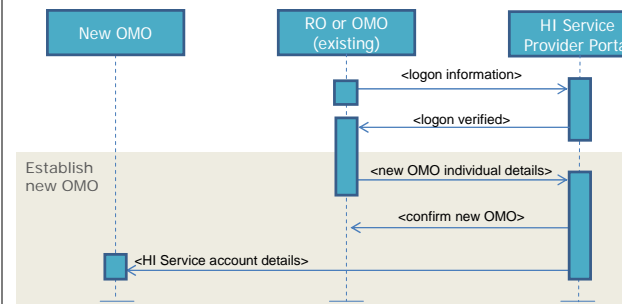
An OMO with the appropriate authority can maintain information associated with an HPI-O. They may

- Create new networked HPI-Os
- Update information associated with the HPI-Os and where appropriate, display the updated information in the HI PDS
- Nominate other OMOs and set their privileges
- Retire a networked HPI-O
- Remove the link of a (subordinate) OMO from HPI-Os
- Maintain links between the provider organisation and provider individuals in the HI PDS with the consent of the provider individuals as per UC210.

### High Level Business Requirements

BR.2009.08.075 Deliver an online service to facilitate healthcare provider individuals and organisations to access and maintain their HPI-I and HPI-O records

### Interaction with HI Service



### OMO for 'seed' HPI-O

During establishment of the 'seed' HPI-O (UC.130), the RO may nominate an OMO or establish themselves in this role.

## UC.135 – Establish a networked HPI-O

### Description

A seed HPI-O may have a hierarchy of associated network HPI-Os. This process describes the creation of a single networked organisation through the HI Service web portal.

### Participants

Healthcare facility (OMO), HI Service

### Process Overview

An OMO logs on to the HI Service web portal and is presented with a map of HPI-Os.

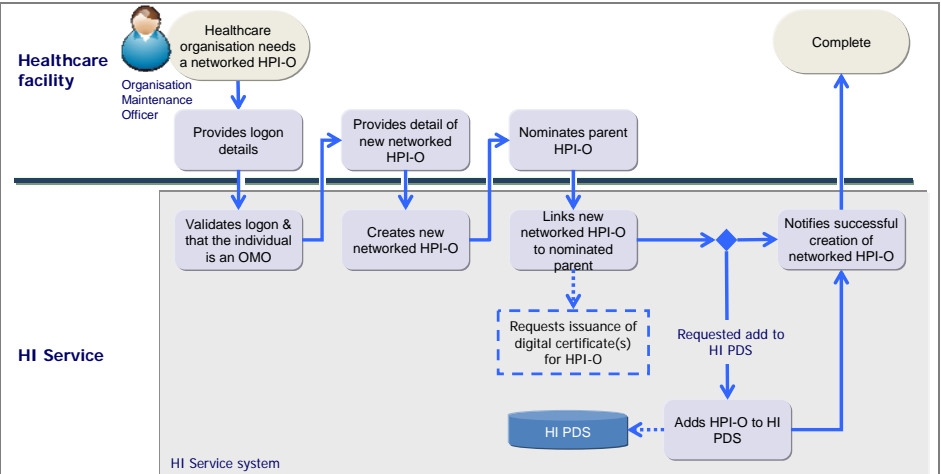
The OMO selects from the map an HPI-O for which they have appropriate authority.

They provide information for the new HPI-O.

The HI Service checks the information for duplicate HPI-Os, creates the new networked HPI-O and links it under the selected parent HPI-O.

The OMO may also publish details of the networked HPI-O with the HI PDS. Where the new HPI-O is required to interact with the HI Service, the OMO will also request delivery of the HPI-O's digital certificate.

The OMO receives notification from the HI Service that the networked HPI-O has been successfully created.



### Operational Policy

Networked HPI-Os are always associated, directly or through other networked HPI-Os, with one seed HPI-O

Every networked HPI-O is required to have an OMO designated to maintain its associated information. An OMO may be responsible for multiple HPI-Os.

### High Level Business Requirements

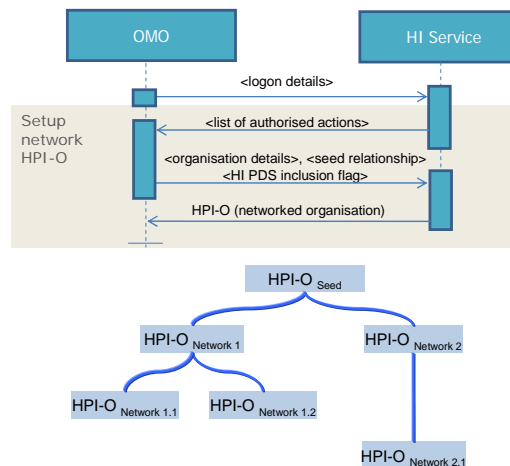
BR.2009.08.140 Create new HPI-Is and HPI-Os, and populate HPI-Is and HPI-Os with associated (and permitted) data; update and maintain existing HPI-Is and HPI-Os and their associated attributes; and retire HPI-Is and HPI-Os

BR.2009.08.096 Promote and communicate the requirements and processes for healthcare provider participation including assignment, collection, disclosure, access, use, maintenance and retirement of HPI-Is and HPI-Os and associated information

BR.2009.08.095 Develop and implement a national system, processes and services associated with the management of HPI-Is and HPI-Os (including but not limited to collection, disclosure, access, use, maintenance and retirement)

BR.2009.08.085 Develop and implement business services to monitor and maintain the integrity and quality of information used, stored and disclosed by the HI Service

### Interaction with HI Service



### HI PDS

Healthcare providers issued with HPI-Os will have the option of being included in a national HI PDS. The HI PDS will enable the search and location of healthcare providers and facilitate communication and information exchange between them, such as referrals, test orders and results.

### Digital Certificates

When a new networked HPI-O is created, digital certificate(s) may be requested.

### A network of HPI-Os

A network of HPI-Os is hierarchical under a single seed HPI-O.

## UC.136 – Reconfigure HPI-Os (mergers or acquisitions of healthcare provider organisations)

### Description

After the merger or acquisition of healthcare provider organisation(s), the RO of the primary HPI-O may request a change to the hierarchy of the organisation to incorporate the acquired HPI-O(s).

This process will move the acquired organisation HPI-O hierarchy under the seed HPI-O of the primary organisation. Once this is complete, the OMO(s) of the primary organisation can restructure the HPI-O hierarchy as appropriate using HPI-O maintenance functions as per UC.170.

### Participants

Healthcare provider organisation (RO), HI Service

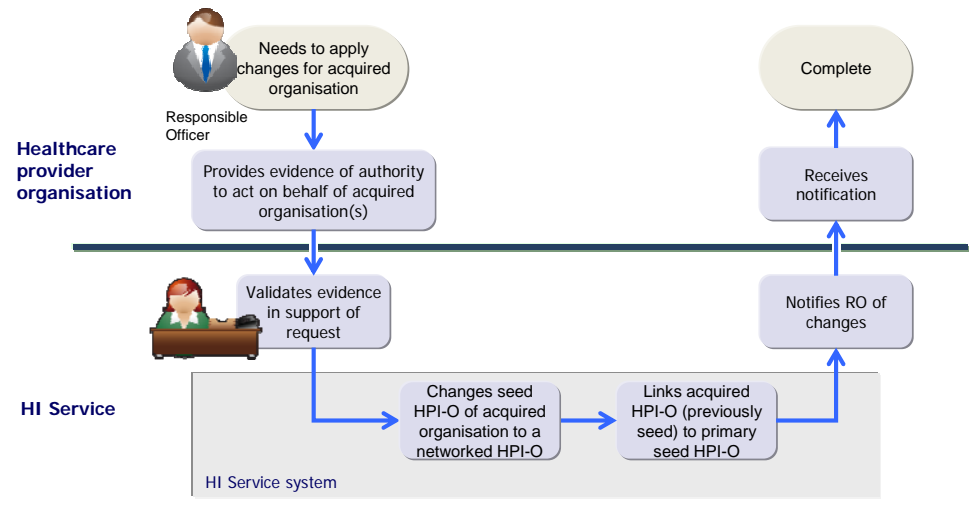
### Process Overview

The RO of the primary HPI-O requests a change to the HPI-O hierarchy. After verification of identity and authority to act on behalf of all affected organisations, the RO will provide supporting evidence about the merged or acquired HPI-O.

The HI Service officer will:

- Change the acquired seed HPI-O to a networked HPI-O;
- Disable access for the RO of the acquired organisation; and
- Link that HPI-O to the primary seed HPI-O

A notification of the changes is provided to the RO of the primary HPI-O.

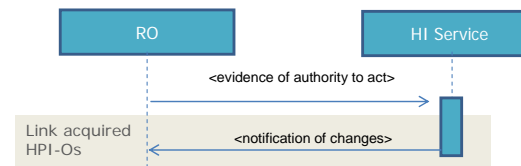


### Relevant High Level HPI Business Requirements

BR.2009.08.096 Promote and communicate the requirements and processes for healthcare provider participation including assignment, collection, disclosure, access, use, maintenance and retirement of HPI-Is and HPI-Os and associated information

BR.2009.08.140 Create new HPI-Is and HPI-Os, and populate HPI-Is and HPI-Os with associated (and permitted) data; update and maintain existing HPI-Is and HPI-Os and their associated attributes; and retire HPI-Is and HPI-Os

### Interaction with HI Service



### Primary and acquired organisations

The term 'primary' is used to define the 'buying' organisation in a merger.

The term 'acquired' is used to define the 'transferring' organisation.

### Operational Note

An OMO must be established in line with UC.131 and UC.135.

## UC.170 – Maintain HPI-O

### Description

An OMO with appropriate authority maintains information associated with an HPI-O. They may:

- Update information associated with the HPI-Os and where appropriate, display the updated information in the HI PDS
- Show or not show HPI-O information in the HI PDS
- Enable/Disable access to electronic address for the HPI-O
- Change (update) parent HPI-O parent

An OMR may be assigned all privileges for the maintenance of an HPI-O

### Participants

Healthcare facility (OMO), HI Service

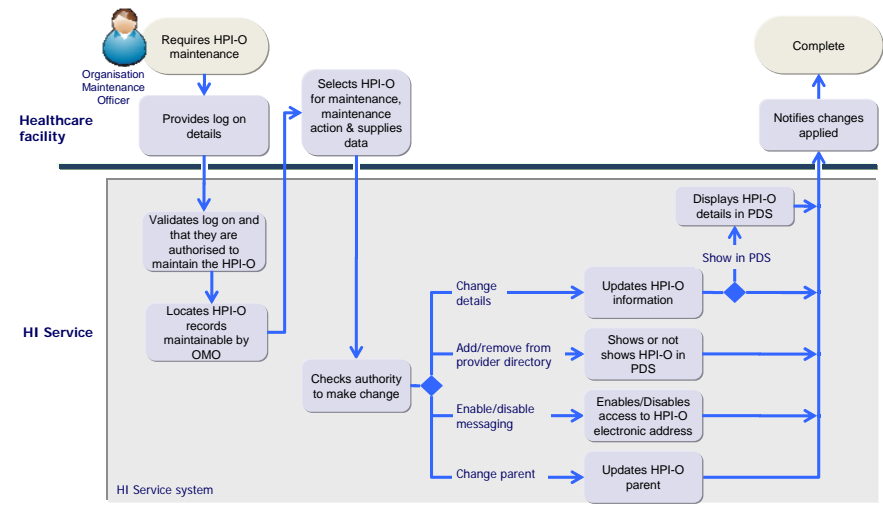
### Process Overview

An OMO logs on to the HI Service web portal. The HI Service provides a map of HPI-Os in their organisation.

The OMO selects the HPI-O requiring maintenance and the required maintenance action.

The HI Service verifies their authority to maintain the selected HPI-Os and applies the requested changes.

The OMO is notified of the outcome.



### Relevant High Level HPI Business Requirements

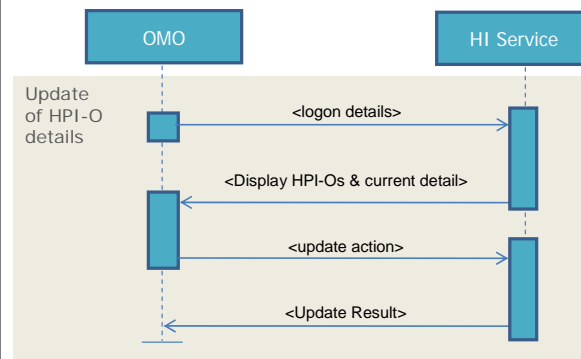
BR.2009.08.075 Deliver an online service to facilitate healthcare provider individuals and organisations to access and maintain their HPI-I and HPI-O records

BR.2009.08.140 Create new HPI-Is and HPI-Os, and populate HPI-Is and HPI-Os with associated (and permitted) data; update and maintain existing HPI-Is and HPI-Os and their associated attributes; and retire HPI-Is and HPI-Os

BR.2009.08.135 Provide a service and associated infrastructure to support authorised users

BR.2009.08.096 Promote and communicate the requirements and processes for healthcare provider participation including assignment, collection, disclosure, access, use, maintenance and retirement of HPI-Is and HPI-Os and associated information

### Interaction with HI Service



### Update HPI-O details

An OMO may maintain the following HPI-O details:

- ABN, ACN or other accepted organisation identifier
- Organisation name
- Address
- Service type
- Service unit
- Electronic communication details
- OMO's name, DOB, address, electronic communication details
- Reference to the Endpoint Locator Service (ELS) for the HPI-O

## UC.172 – Retire a seed HPI-O

### Description

The RO of a healthcare provider organisation may request the retirement of the seed HPI-O of the organisation through the HI Service officer.

### Participants

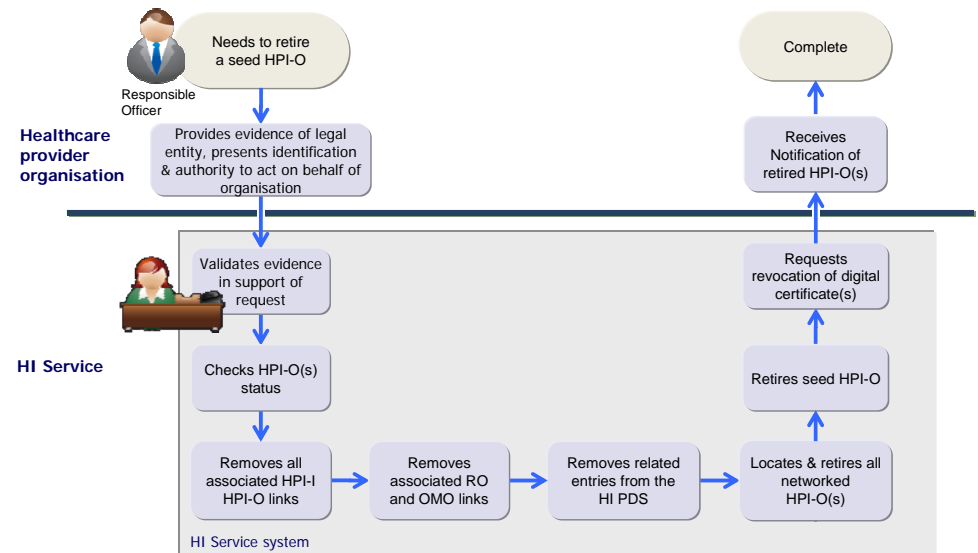
Healthcare provider organisation (RO), HI Service

### Process Overview

The RO presents at a HI Service office and provides evidence of identity and authority to act. The retirement process for a seed HPI-O will automatically:

- Remove associated HPI-I to HPI-O links
- Remove associated RO and OMO()links
- Retire all related entries from the HI PDS
- Retire the seed HPI-O
- Revoke digital certificate(s)

A notification will be provided to conclude the retirement process.



### Operational Policy

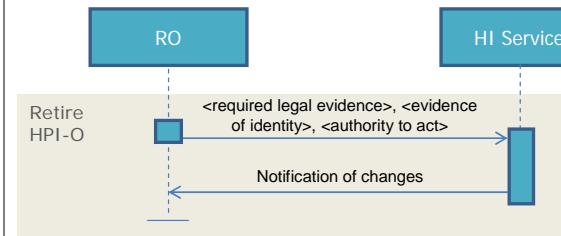
Digital certificates may need to remain active for a period after a seed HPI-O has been retired to enable all business transactions pending to be completed.

### High Level Business Requirements

BR.2009.08.096 Promote and communicate the requirements and processes for healthcare provider participation including assignment, collection, disclosure, access, use, maintenance and retirement of HPI-Is and HPI-Os and associated information

BR.2009.08.140 Create new HPI-Is and HPI-Os, and populate HPI-Is and HPI-Os with associated (and permitted) data; update and maintain existing HPI-Is and HPI-Os and their associated attributes; and retire HPI-Is and HPI-Os

### Interaction with HI Service



## UC.173 – Retire a networked HPI-O

### Description

The OMO of a healthcare provider organisation may request the retirement of networked HPI-O(s) for which they have authority.

The retirement of a networked HPI-O will involve the retirement of HPI-O(s) that are subordinate to the HPI-O being retired.

### Participants

Healthcare facility (OMO)

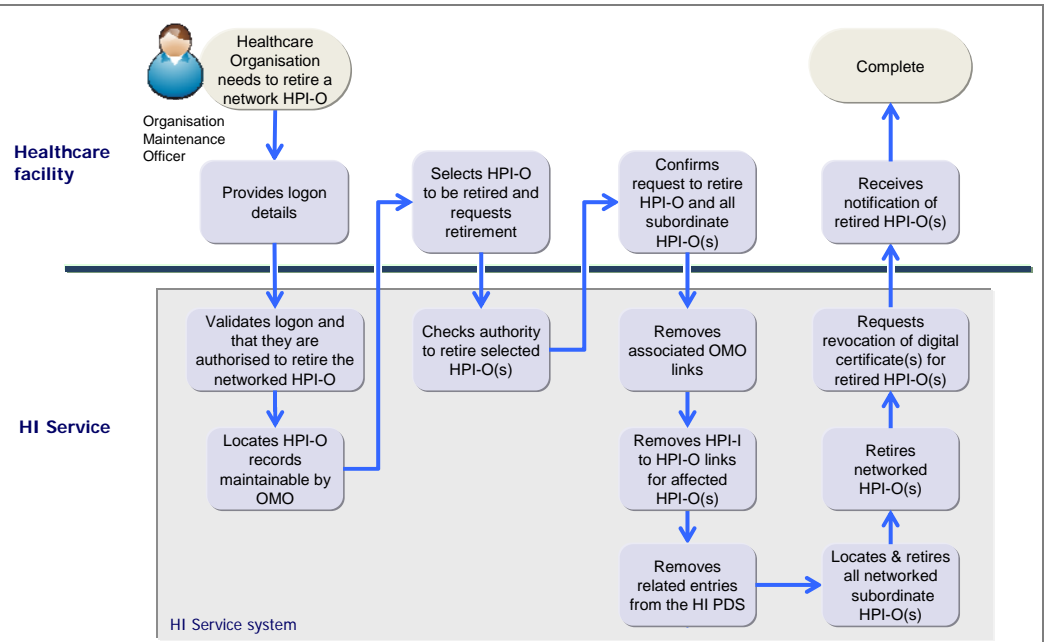
### Process Overview

An OMO logs on to the HI Service web portal. The HI Service verifies their authority to maintain selected HPI-Os.

The OMO selects the HPI-O to be retired and requests retirement. After confirmation, the following actions are carried out for HPI-O(s) to be retired:

- Remove associated HPI-I to HPI-O links
- Remove associated OMO links
- Remove all related entries from the HI PDS
- Retire all subordinate HPI-O(s)
- Retire the selected networked HPI-O
- Revoke digital certificate(s)

A notification will be provided to conclude the retirement process.



### Operational Policy

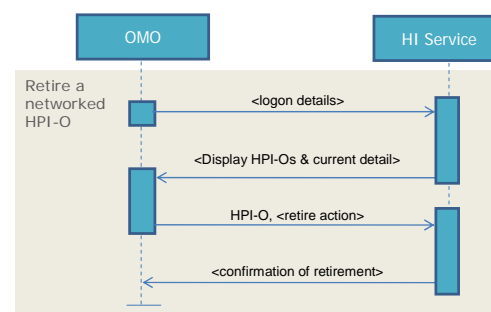
Digital certificates may need to remain active for a period after a networked HPI-O has been retired to enable all business transactions to be completed.

### Relevant High Level HPI Business Requirements

BR.2009.08.096 Promote and communicate the requirements and processes for healthcare provider participation including assignment, collection, disclosure, access, use, maintenance and retirement of HPI-Is and HPI-Os and associated information

BR.2009.08.140 Create new HPI-Is and HPI-Os, and populate HPI-Is and HPI-Os with associated (and permitted) data; update and maintain existing HPI-Is and HPI-Os and their associated attributes; and retire HPI-Is and HPI-Os

### Interaction with HI Service



### Operational Notes

Subordinate HPI-O(s) not intended for retirement should have their parent HPI-O changed prior to the retirement process.

## UC.180 – New professional registration through a TDS (create HPI-I)

### Description

Eligible healthcare provider individuals can be allocated an HPI-I through an associated TDS.

Any changes to healthcare provider individual details that have been supplied by the TDS can only be updated by the TDS.

### Participants

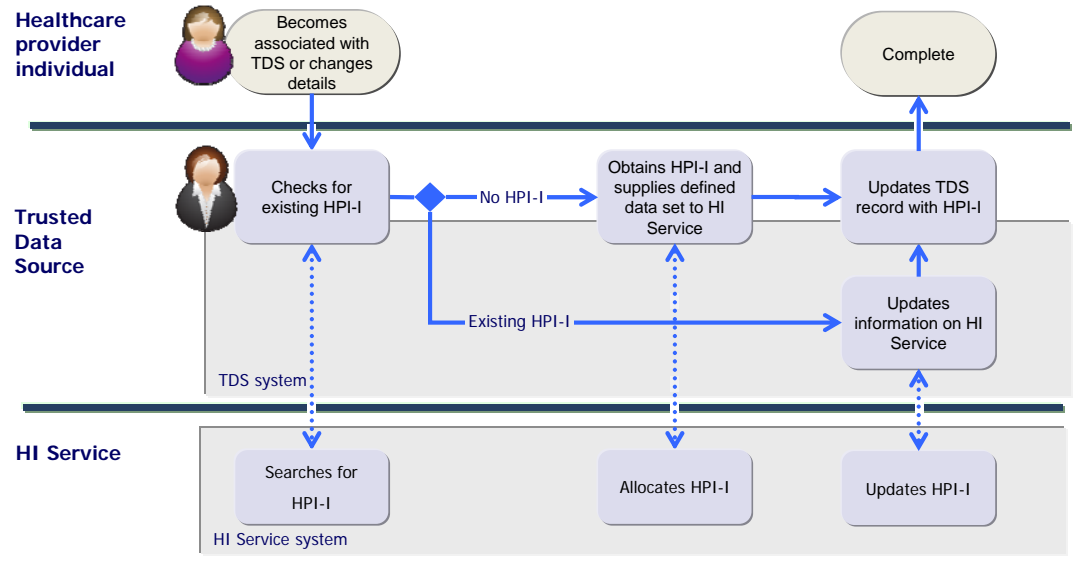
Healthcare provider individual, TDS

### Process Overview

The TDS manages the allocation and maintenance processes of HPI-Is within its area of responsibility.

When a healthcare provider individual becomes associated with a TDS, the TDS will either:

- Update the individual's HPI-I record; or
- Obtain a new HPI-I for the individual



### Policy

The HI Service recognises TDSs as a source of verified identification information for the purpose of creating HPI-Is.

TDSs will be the authoritative source for data they supply to the HI Service and will be the only party able to modify that data.

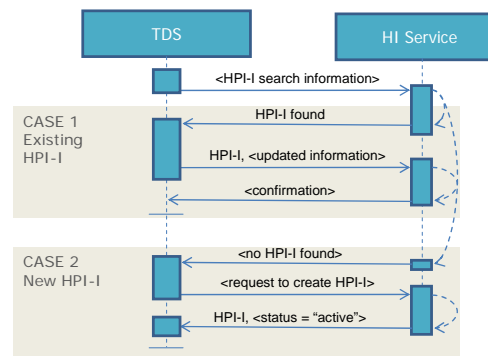
### Relevant High Level HPI Business Requirements

BR.2009.09.071 Automatically allocate an HPI-I to a healthcare provider individual enrolled with a Trusted Data Source

BR.2009.08.050 Allocate a unique identifier to all eligible healthcare provider individuals and organisations that require one

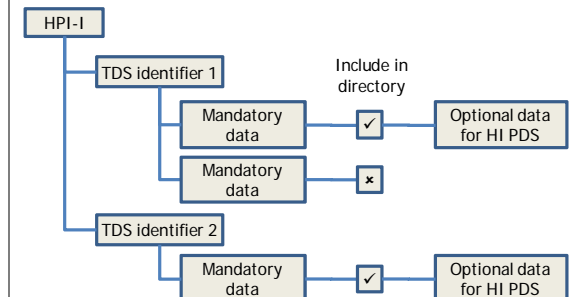
BR.2009.08.060 Comply with national and international standards for healthcare provider identifiers

### Interaction with HI Service



### Operational Notes

The TDS is required to advise the healthcare provider individual of their HPI-I when allocated. Where the healthcare provider individual has multiple specialities which are managed through different TDSs, the data associated with those specialities will be separately stored as shown in the following.





## UC.182 – Create or maintain HPI-I through HI Service

### Description

Eligible healthcare provider individuals who are not allocated a HPI-I through a TDS can be allocated a HPI-I by the HI Service.

HPI-Is allocated by the HI Service are maintained through the HI Service.

### Participants

Healthcare provider individuals, HI Service

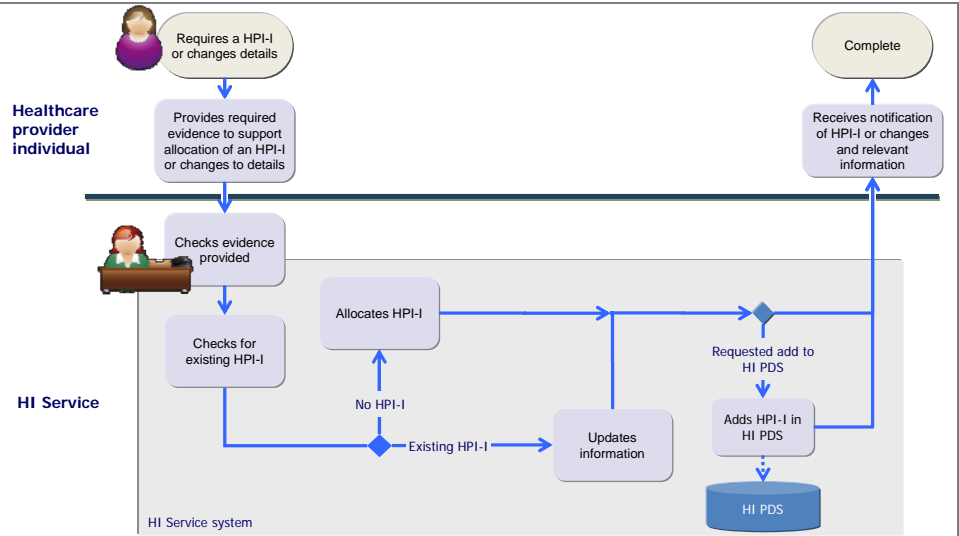
### Process Overview

The healthcare provider individual provides the HI Service officer with evidence to support allocation of an HPI-I.

The healthcare provider individual may also authorise publication of information in the HI PDS. The HI Service officer checks the evidence provided and:

- where no HPI-I has previously been allocated, one may be requested; or
- where an HPI-I has already been created, the HPI-I may be updated.

The requesting individual will receive a notification.



### Policy

A healthcare provider individual seeking allocation of a HPI-I, will be required to provide:

1. Evidence of identity;
2. Evidence of his/her eligibility; and
3. A completed HPI-I application.

### HPI-I obligations

The healthcare provider individual will receive information that advises them of their responsibilities for ensuring that the HPI-I information is accurate, up-to-date and complete.

### Relevant High Level HPI Business Requirements

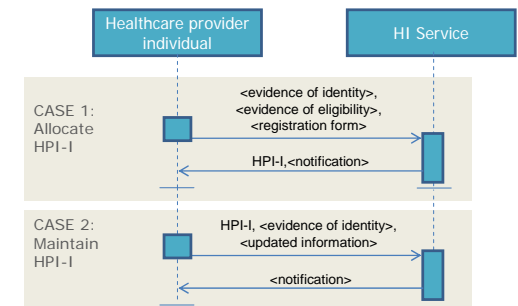
BR.2009.08.045 At the point of issue of an HPI-I or HPI-O, accurately identify healthcare provider individuals and organisations

BR.2009.08.050 Allocate a unique identifier to all eligible healthcare provider individuals and organisations that require one

BR.2009.08.075 Deliver an online service to facilitate healthcare provider individuals and organisations to access and maintain their HPI-I and HPI-O records

BR.2009.08.140 Create new HPI-Is and HPI-Os, and populate HPI-Is and HPI-Os with associated (and permitted) data; update and maintain existing HPI-Is and HPI-Os and their associated attributes; and retire HPI-Is and HPI-Os

### Interaction with HI Service



## UC.210 – Link HPI-I with HPI-O in HI Provider Directory Service

### Description

With the agreement of a healthcare provider individual, an OMO may create a link in the HI PDS between the HPI-I and an HPI-O for which they are responsible.

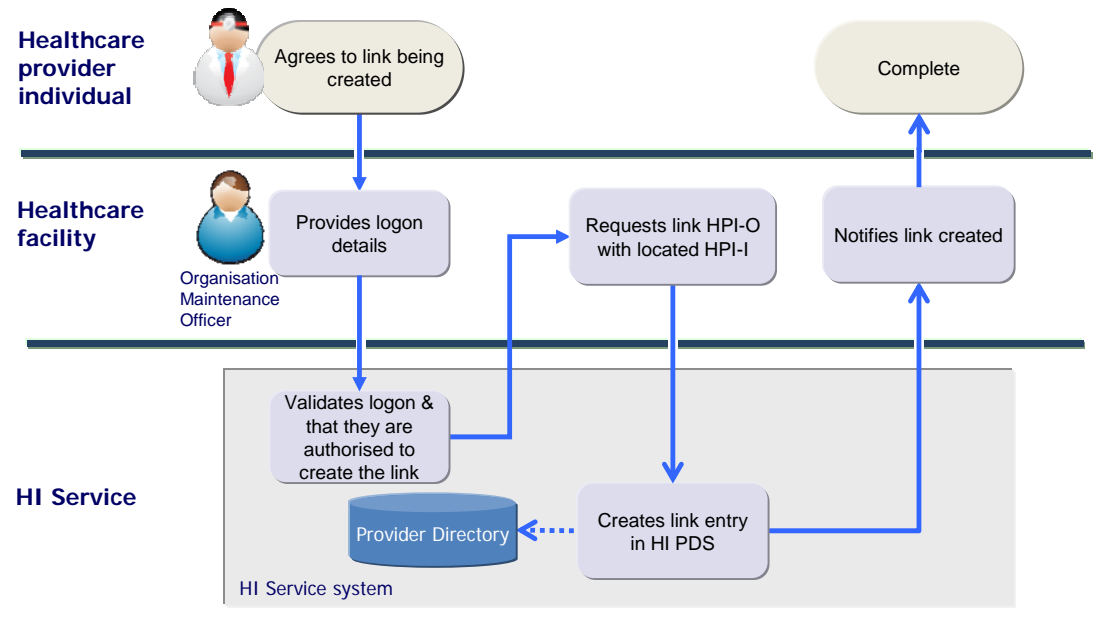
### Participants

Healthcare provider individual, Healthcare facility (OMO), HI Service

### Process Overview

The healthcare provider individual agrees to have their HPI-I linked with the HPI-O in the HI PDS.

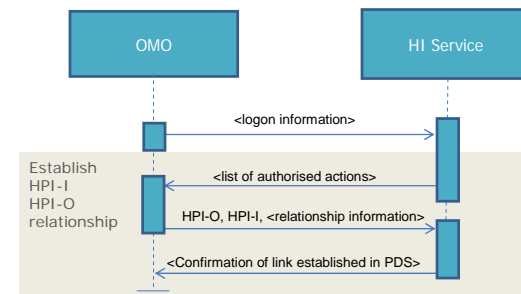
The OMO logs on to the HI Service and requests the establishment of a link between the HPI-I and the HPI-O.



### Relevant High Level HPI Business Requirements

BR.2009.08.035 Support the development and operation of healthcare provider directory services

### Interaction with the HI Service



## UC.220 – Retire HPI-I

### Description

A HPI-I will be retired when the HI Service receives notification that a healthcare provider individual is deceased. This notification could come from a TDS.

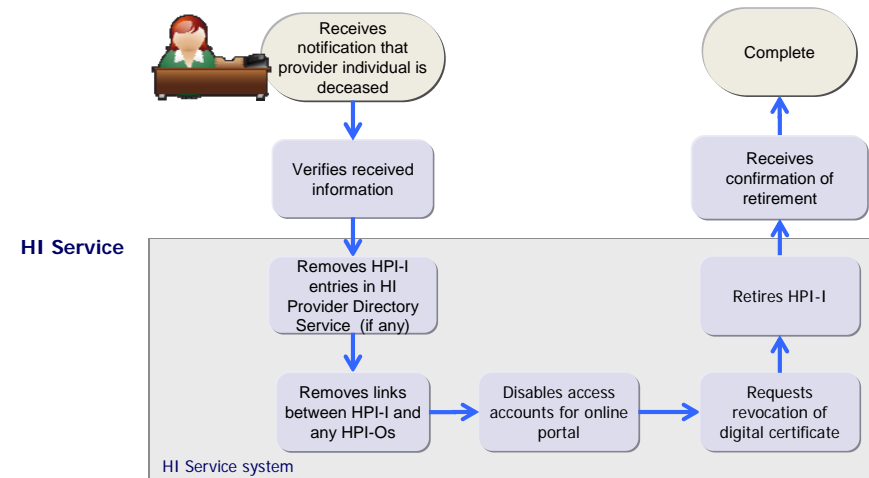
### Participants

Trusted Data Source

### Process Overview

The HI Service receives notification that a healthcare provider individual is deceased. The HI Service retires the HPI-I which involves:

- Removal of the HPI-I from the HI Provider Directory Service
- Removal of links between the HPI-I and any HPI-Os
- Disabling of access accounts to the HI Service provider portal
- Changing HPI-I status to 'retired'
- Requesting revocation of the digital certificate(s) and all related tokens
- Confirmation of retirement back to TDS(s)



### Operational Policy

A TDS is responsible for maintaining links with births, deaths and marriages and notifying the HI Service of the death of healthcare provider individuals.

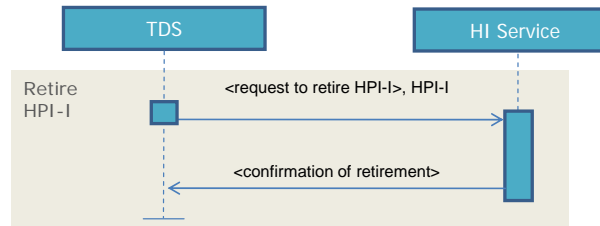
### Relevant High Level HPI Business Requirements

BR.2009.08.080 Source and utilise reference data sources to verify, validate and update HPI-Is, HPI-Os and associated information

BR.2009.08.095 Develop and implement a national system, processes and services associated with the management of HPI-Is and HPI-Os (including but not limited to collection, disclosure, access, use, maintenance and retirement)

BR.2009.08.140 Create new HPI-Is and HPI-Os, and populate HPI-Is and HPI-Os with associated (and permitted) data; update and maintain existing HPI-Is and HPI-Os and their associated attributes; deactivate and retire HPI-Is; and retire HPI-Os

### Interaction with HI Service



## UC.222 – HPI-I maintains details through web portal access

### Description

A healthcare provider individual is able to view their HPI-I record, and update limited information associated with their HPI-I via a web portal.

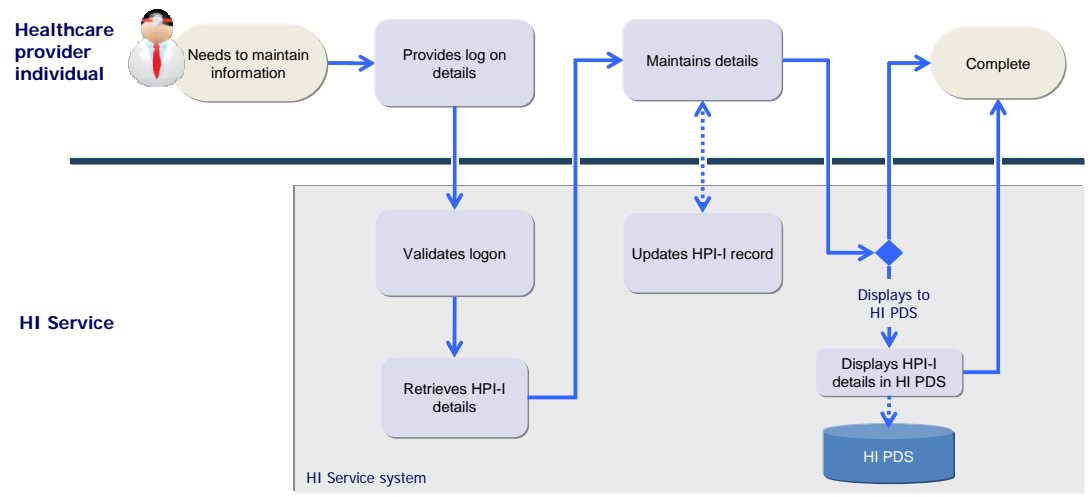
### Participants

Healthcare provider individual

### Process Overview

A healthcare provider individual logs on to the HI Service web portal and accesses their HPI-I record and associated data. The healthcare provider individual is able to:

- Update contact information
- Update information about them to be displayed in the HI PDS
- Choose whether or not to display their information in the HI PDS
- View established links between their HPI-I and HPI-Os within the HI PDS and if required, choose not to publish the link



### Update Restrictions

The healthcare provider individual can only update certain details via the web portal.

Any changes to healthcare provider individual details that have been supplied by the TDS can only be updated by the TDS.

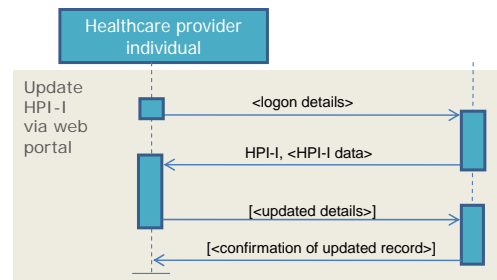
### Relevant High Level HPI Business Requirements

BR.2009.08.075 Deliver an online service to facilitate healthcare provider individuals and organisations to access and maintain their HPI-I and HPI-O records

BR.2009.08.100 Support the healthcare sector by providing identifier services which are highly available

BR.2009.08.135 Provide a service and associated infrastructure to support authorised users

### Interaction with HI Service



# UC.224 – Validate HPI-I

## Description

When a healthcare provider organisation needs to validate an HPI-I associated with their organisation, they can access the information from the HI Service.

## Participants

Healthcare facility (OMO)

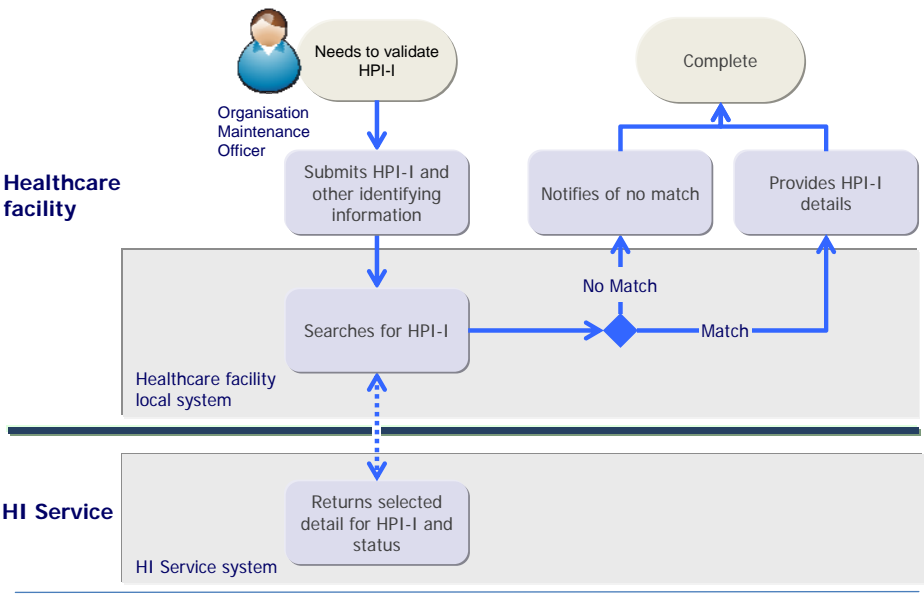
## Process Overview

The authorised user searches for the HPI-I in the HI Service using information provided by the healthcare provider individual. This information must include:

- HPI-I
- Name
- DOB

The search would return selected information associated with the HPI-I and its status. This information will include:

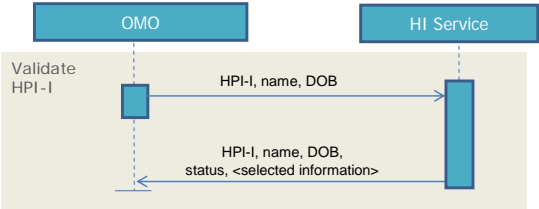
- HPI-I
- Name
- DOB
- Sex
- Provider individual type



## Relevant High Level HPI Business Requirements

BR.2009.08.055 Enable accurate association of a healthcare provider individual by a healthcare provider organisation

## Interaction with HI Service



## UC.232 – Locate healthcare provider (HPI-I or HPI-O) in HI Provider Directory Service

### Description

Users who are appropriately authorised may search or browse the HI PDS for HPI-I(s) or HPI-O(s) and limited associated information.

### Participants

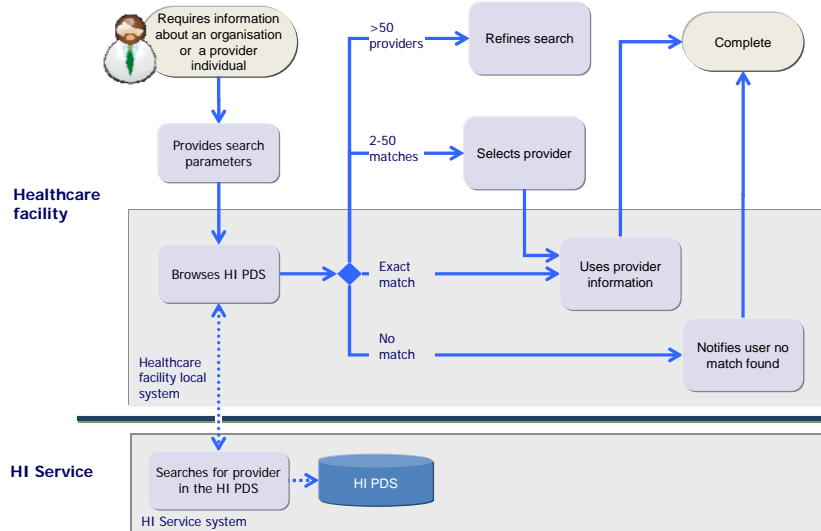
Healthcare facility

### Process Overview

A user who is appropriately authorised accesses the HI PDS and provides the search parameters necessary to locate healthcare organisation or provider information.

The service will return either:

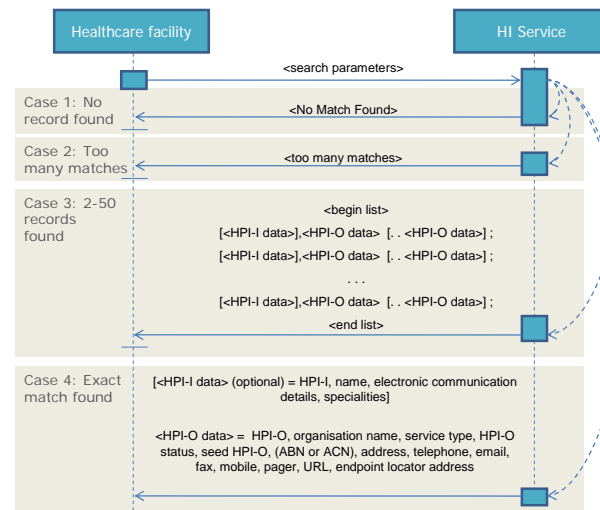
- An exact match;
- No match;
- 2 to 50 possible matches against which the user may browse and select; or
- Too many possible matches (>50) – refine search.



### Relevant High Level HPI Business Requirements

BR.2009.08.035 Support the development and operation of healthcare provider directory services

### Interaction with HI Service



### Search Options

The HI PDS may be searched using any of the following:

- Organisation name
- Organisation service type
- Provider individual name
- Provider individual speciality
- Address (part or full)

### Batch download of HI PDS

Information contained in the HI PDS may be downloaded to provider directories maintained by healthcare facilities subject to appropriate consent.

## Appendix B - Glossary

Term	Definition
AHMAC	Australian Health Ministers' Advisory Council
AHMC	Australian Health Ministers' Conference
AHPRA	Australian Health Practitioner Regulation Agency
Allocation	The process of assigning an IHI to a healthcare individual; a HPI-I to a healthcare individual provider; a HPI-O to a healthcare provider organisation
Authorised employees	An employee of an identified healthcare provider, if that identified healthcare provider has, by notice to the HI Service Operator, authorised the employee to act on behalf of that identified healthcare provider
Batch Upload	Enables the clinical system of a healthcare facility to match a large existing set of healthcare individuals' details, known to the healthcare facility, against IHI data in the HI Service, to download matched IHIs into the clinical system. This process is typically undertaken as a background search.
Business Day	Means any day other than a Saturday, Sunday or public holiday (including public service holidays) throughout Australia, promulgated in the Commonwealth of Australia Gazette.
Business Hours	8.30 AM to 6:00 PM in any Australian time zone on a Business Day.
COAG	Council of Australian Governments
Concept of Operations	Is a user-oriented document that describes system characteristics from a user point of view
Digital Certificate	An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply
E-Health	Is the process of employing the combined use of electronic communication and information technology in the health sector
Evidence of Identity	A set of documents that authenticate the evidence of identity of an individual
HPI-I	The Healthcare Provider Identifier-Individual for individual healthcare providers (HPI-I) is a 16 digit unique reference number used to identify individuals who deliver Australian healthcare
HPI-O	The Healthcare Provider Identifier-Organisation (HPI-O) is a 16 digit unique reference number used to identify healthcare organisations who deliver Australian healthcare
HI Service	The Healthcare Identifiers Service (HI Service) is a range of business services that enable the identification, allocation, access control, disclosure, maintenance and retirement of national healthcare identifiers for healthcare individuals and providers
IEHR	An Individual Electronic Health Record (IEHR) is a secure, private electronic record of an individual's key health history and care information which may in future leverage the HI Service
IHI	The Individual Healthcare Identifier (IHI) is a 16 digit unique reference number used to identify recipients of Australian healthcare services
IHI Record	A limited amount of personal information associated with an individual's IHI. It will include IHI, name(s), date of birth, and may include address and sex
Jurisdiction	Refers to the Australian public health departments at federal, state and territory levels
NEHTA	National E-Health Transition Authority
NASH	National Authentication Service for Health enables the authentication, authorisation and auditing of access to the HI Service
NEHIPC	National E-Health and Information Principal Committee
NRAS	National Registration Accreditation Scheme is a national scheme for the registration and accreditation of health practitioners
Probabilistic Matching	A method which uses statistics and algorithms to determine whether information attached to a record refers to the same individual.

Provisional IHI	A provisional IHI will be allocated to an individual who has presented at a healthcare facility and is unconscious or incapacitated, and unknown to the healthcare facility and will expire 90 days after issue
Retirement	The process of decommissioning an IHI, a HPI-I or a HPI-O
Smartcard	A smartcard is a plastic card about the size of a credit card, with an embedded microchip that can be loaded with data
Trusted Data Source	A TDS is a managed repository of valid or trusted data that is recognised as an authoritative external source of data that meets an appropriate set of criteria and contains a set of attributes that covers the requirements of another business system. Leveraging existing data from an approved TDS occurs through technical processes, always ensuring that personal information is safeguarded
Unverified IHI	Is an IHI created without the evidence of identity process being conducted
Verified IHI	Is an IHI created with the evidence of identity process being conducted