nehta

Healthcare Identifiers Implementation Guide

Version 1.1 — 6 June 2011

Final

National E-Health Transition Authority

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

Disclaimer

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

Document Control

This document is maintained in electronic form. The current revision of this document is located on the NEHTA Website. It is the responsibility of the user to verify that this is a copy of the latest revision.

Copyright © 2011 National E-Health Transition Authority Ltd. (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 without the permission of NEHTA. All copies of this document must include the copyright notice and other information contained on this page.

Document version control

Document owner

Document owner
Product and Solutions Development team

Version control

Date	Version	Author	Comments
31 Mar 11	0.01	ICP Team	Initial draft
2 June 11	1.0	ICP Team	Initial limited release
6 June 11	1.1	ICP Team	Update 1.6, Remove formatting marks

Document Status

This document is endorsed for limited release.

Table of contents

Document owner iii
Version control iii
Document Status iii

1 Introduction 1
1.1 Scope 1
1.2 Responsibility 1
1.3 Purpose of the guide 1
1.4 Intended audience 2
1.5 Purpose of the Healthcare Identifiers Service 2
1.6 Definitions 3
1.7 Best practice principles 6
1.8 Acknowledgement 7
1.9 Reference Documents 7
1.10 Regulatory environment 8
1.10.1 Legislation 8
1.10.2 Privacy 8
1.10.3 Healthcare Identifiers 9
1.11 Conformance, Compliance, Accreditation 9
1.12 Change Management 10
1.12.1 Operational changes and impacts 10
1.12.2 Training 12
1.13 Roles and Responsibilities 13
1.13.1 Authorised Employee 13
1.13.2 HI Service Operator 14
1.13.3 CSP Officer 15

2 Healthcare Identifiers 16
2.1 Process of identifying Healthcare Individuals 16
2.1.1 Key benefits 17
2.2 Individual Healthcare Identifiers 18
2.3 IHI state and record statuses 18
2.4 Comparison of IHIs [1] 20
2.5 Healthcare individual search characteristics 22
2.5.1 Processing HI Service requests 22
2.6 Initial bulk uploading of IHIs to a software system for the health sector 22
2.7 Search for IHI 23
2.7.1 IHI search technique 23
2.7.2 Restricted HI Service Search Functionality 24
2.7.3 IHI search rules 24
2.8 General 25
2.8.1 Healthcare Individual and Provider Identifiers 26
2.8.2 Name 27
2.8.3 Contact details 28
2.8.4 Address 28
2.8.5 Electronic communication details 29
2.8.6 Other identifying information 30
2.9 Identification of Healthcare Provider Individual and Organisation 30
2.10 Healthcare Provider Identifier Organisation characteristics 31

2.11 Collection verses exchange 31
2.12 Healthcare Identifier standards and characteristics 31
2.12.1 IHI Creation 31
2.13 Requirements for the national healthcare identification numbering system 34

3 Registration Process 36
3.1 Identification and registration process 36
3.2 Healthcare Individual registration 36
3.2.1 Registering Healthcare Individuals 37
3.3 Healthcare Provider registration 38
3.3.1 Registration via AHPRA 39
3.4 Healthcare Individual registration issues 40
3.5 How to improve IHI validation and registration processes 40
3.6 Data cleansing 42
3.7 General principles of identification & registration of Healthcare Individuals and Providers 42
3.8 Healthcare Individual data collection 43
3.9 New Healthcare Individual registrations 44
3.10 Searching a Healthcare Individual client database 45
3.11 Authenticated sources and existing data 46
3.12 Security management processes 46

4 Data quality management processes 48

5 Healthcare Individual client data linkage 49
5.1 Healthcare Individual client data linkage 49
5.2 Enterprise Healthcare Individual client index 49
5.3 Linking Healthcare Individual client records 50
5.4 Restricted use of identifiers 51
5.5 Data matching 51
5.6 Passive or active mode of data linkage 51
5.7 Process of Healthcare Individual client data linkage 52

6 Pseudonymous and Anonymous data 54
6.1 What is a Pseudonym? 54
6.2 Pseudonymous IHI 54
6.3 Applying for a Pseudonymous IHI 54
6.4 Anonymous IHI 55

7 Healthcare Individual client and provider identification messaging 56
7.1 Obtaining Healthcare Provider Identifiers 56
7.2 Authenticated sources and existing data 57
7.2.1 Searching for HPI-Is in the Healthcare Provider Directory 57
7.2.2 Enable HPI-O Record in Healthcare Provider Directory 57
7.3 Healthcare Individual messaging 57
7.4 Healthcare Provider messaging 58
7.5 Healthcare Individual and Provider standards: 58
7.6 Healthcare Individual standards 58
7.7 Healthcare Provider standards 59
7.8 Messaging – Exchange of data 59

8 Contracted Service Providers 61
8.1 Background 61

8.2 Registering Contracted Service Providers 61
8.3 Functions 61

9 Compliance, Conformance and Accreditation Program 63
9.1 Software Conformance Requirements 63
9.2 The approach to conformance testing 63
9.3 Test laboratory accreditation 64
9.4 Relevant technical requirements 64
9.5 Minimum conformance requirements 64
9.6 Medicare Australia's testing requirements for the HI service interface 65
9.7 Medicare Australia's HI Service vendor environment 65

10 Scenarios 66
10.1 Common healthcare client and provider scenarios 66
10.1.1 Mergers and/or Acquisitions 66
10.1.2 Healthcare provider organisation that is not registered within the HI Service 66
10.1.3 Considerations 67

Appendix A: ICP Business Use Cases 68
Appendix B: Comments Log: 70

This page is intentionally left blank

1 Introduction

1.1 Scope

This implementation guide provides information and guidance about implementing individual and provider identification processes within healthcare facilities and integration with the Healthcare Identifiers Service (HI Service) to obtain national unique healthcare identifiers for individuals, individual healthcare providers and healthcare provider organisations.

1.2 Responsibility

Responsibilities for the capture, storage and use of identifying information about individuals and/or healthcare providers, including the implementation of the Australian Standards[1] for identification, should be clearly and unambiguously documented in relevant policies, procedures and work instructions.

1.3 Purpose of the guide

This implementation guide complements the Standards Australia Australian Healthcare Client and Provider Identification Handbook (HB222-2006), and has been developed in conjunction with representatives from the healthcare sector and the operator of the HI Service, Medicare Australia.

The purpose is to provide guidance to support planners and implementers in the adoption of national Healthcare Identifiers issued by the HI Service across the healthcare sector in a consistent and streamlined manner.

This guide provides information to:

- Support standardisation of individual and provider registration processes;
- Support consistent collection of individual and provider identification data; and
- Support the integration of provider software, with the HI Identifiers Service.

Specific benefits to be gained by applying the principles of implementing standardised information processes within a healthcare facility include:

- Improved information systems that facilitate data searching, data associations and individual/provider identification;
- Standardised search processes according to data collection size that will improve, the healthcare facilities ability to find existing healthcare individual/provider information within the computer systems;
- Support of semantic interoperability between data collections in different areas of healthcare, thereby improving comparability of and ease of communication between data sets;
- Improvement of the quality and value of individual/provider identifying data through improved data collection processes;

[1] Australian Healthcare Client and Provider Identification Handbook (HB222-2006)

- Clarification of the issues of healthcare individual identification in Australia in order to support education activities and the development of procedures to suit a computerised information system for employees within a healthcare facility;
- Improve the efficiency of healthcare individual registration and identification processes at all levels of healthcare and promote consistency of practice; and
- Improved awareness of principles of appropriate use of identifying health information and the mechanisms to protect healthcare individuals and service provider's privacy.

Note:

Further analysis may be required for specific local level implementation. Local policies and procedures may need to be developed to provide ongoing reference material for staff and employee training purposes.

1.4 Intended audience

The intended audience for this document is primarily:

- Planners;
- Implementers & Change Managers;
- Software vendors; and
- End users.

1.5 Purpose of the Healthcare Identifiers Service

The purpose of the HI Service is to assign a unique national Healthcare Identifier to each healthcare recipient and healthcare provider to establish and maintain accurate records to support the communication and management of health information.

The HI Service is also the fundamental building block for secure electronic communication of health information between healthcare providers and the creation of a Personally Controlled Electronic Health Record (PCEHR).

Together, with the establishment of robust regulatory arrangements to ensure appropriate safeguards for patient health information, the implementation of unique national Healthcare Identifiers for healthcare recipients and healthcare providers will also encourage the participation of the health sector in various e-health initiatives.

E-health aims to optimise the quality and efficiency of healthcare delivery.

The National e-Health Strategy notes that e-health will[2]:

- 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 healthcare sector to more effectively operate as an inter-connected system overcoming the current fragmentation and duplication of service delivery;

[2] National e-Health Strategy

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

1.6 Definitions

Key definitions provided below:

Authorised Employee	An Authorised Employee is an individual who is engaged and authorised to act on behalf of a Healthcare Provider Organisation (HPI-O), to manage the flow of patient communication and health information within the organisation and is also authorised to access the HI Service. The Authorised Employee is not a healthcare provider and will not be required to have a number assigned by the Healthcare Provider Organisation. The HPI-O must ensure that the HI Service will have available to it, the current names and contact details of those employees authorised to access the HI Service.
Compliance, Conformance and Accreditation (CCA)	The Compliance, Conformance and Accreditation (CCA) process was designed by the E-Health Industry to help Developers of software systems in the implementation of healthcare identifiers to minimise risks to clinical safety, privacy and information security and maximises the benefits associated with their usage. CCA is one of the testing processes required to be granted production access to the HI Service.

Contracted Service Provider (CSP)	A Contracted Service Provider (CSP), is an entity that provides the following services under a contract with a HPI-O: (a) Information technology services relating to the communication of health information; or (b) Health information management services. A CSP will have a unique identification number allocated by the HI Service Operator following successful registration. A CSP cannot access the HI Service without being contracted by a healthcare provider organisation (HPI-O).
Contracted Service Provider (CSP) Officer	A Contracted Service Provider (CSP) Officer is an individual that should be a senior appointment within a Contracted Service Provider and take on the full responsibility for any dealings with the HI Service.
Healthcare Provider	Healthcare provider is a generic term which refers to a healthcare provider individual and/or a healthcare provider organisation.
Healthcare Provider Identifier Individual (HPI-I)	A Healthcare Provider Identifier Individual (HPI-I) is a national unique 16 digit identifying number assigned to health practitioners who provide healthcare services to the general public.
Healthcare Provider Directory	The Healthcare Provider Directory (HPD) is managed by the HI Service Operator. It will contain the professional and business details of the healthcare providers who have consented to those details being included in the HPD.
Healthcare Identifiers (HI) Licensed Material (HILM)	HI Licensed Material means the specifications, artefacts, requirements and other material issued by Medicare Australia and includes all Intellectual Property, media, documents and other property contained in the HI Licensed Material or provided as support during the term of the Licence Agreement and any updates and new releases of HI Licensed Material.
Healthcare Provider Organisation	Healthcare Provider Organisation is an entity, or a part of an entity, that has conducted, conducts, or will conduct, an enterprise that provides healthcare (including healthcare that is provided free of charge), in accordance with the s6(1) Privacy Act 1988. Examples include: A public hospital or a corporation that runs a medical centre or a single GP Practice.
Healthcare Provider Identifier Organisation (HPI-O)	A Healthcare Provider Identifier Organisation (HPI-O) is a national unique 16 digit identifying number assigned to organisations involved in delivering healthcare services.

Healthcare Identifiers Service (HI Service)	The Healthcare Identifiers Service (HI Service) provides a range of business services that enable the identification, allocation, access control, disclosure, maintenance and retirement of unique national Healthcare Identifiers for healthcare individuals and healthcare providers.
HI Service Operator	The current operator of the HI Service is Medicare Australia.
Individual Healthcare Identifier (IHI)	An Individual Healthcare Identifier (IHI) is a unique national 16 digit identification number assigned to individuals who seek healthcare services in Australia.
Licence Agreement - Use of the Healthcare Identifiers Licensed Material for Notice of Connection	To facilitate communications between participants in the HI Service, Medicare Australia has agreed to license certain Material to software developers for use in obtaining a Notice of Connection (NOC). The NOC does not authorise connection or use of the HI Service, although it is a necessary pre-requisite for connection. The Licence Agreement specifies the terms and conditions for both Medicate Australia and the software developers.
Networked Organisation	A part of a seed organisation, which exists beneath the seed in the organisational hierarchy. A networked organisation may include a location, a clinic or any other logical representation required to support the seed organisation in the delivery of health services or health related services.
Notice of Connection (NOC)	Notice of Connection or NOC means the notification issued to a software developer subsequent to successfully completing the Software Product connection testing process (based on the HI Licensed Material). The NOC verifies only that the version or versions of the Software Product specified in the Notice of Connection are capable of connecting to the HI Service.
Organisation Maintenance Officer (OMO)	An Organisation Maintenance Officer (OMO) is an individual who is authorised by the healthcare organisation to manage the day to day activities with the HI Service. These activities may include maintaining organisational information, manage the security and access controls for all 'Authorised Employees'. The OMO is also responsible for obtaining consent from all healthcare provider individuals seeking to publish their professional and business details in the HI Service Healthcare Provider Directory (HPD).
Provisional IHI	A Provisional IHI is allocated to an individual who has presented at a healthcare facility and is unconscious or incapacitated and unknown to the healthcare facility. It will expire 90 days after the date of last use.

Responsible Officer (RO)	A Responsible Officer (RO) is an individual that should be a senior appointment within a healthcare provider organisation and authorised to act on behalf of the healthcare organisation in it's dealings with the HI Service. The 'Responsible Officer', for example, may be associated with the role of the Executive Officer to a Chief Executive or a senior position in the area of corporate services.
Seed Organisation	A healthcare provider organisation at the top of an organisational hierarchy or structure. A Seed Organisation is a legal entity that employs healthcare practitioners who provide health services. A Seed Organisation will be registered with the HI Service and can establish multiple relationships with Networked Organisations within its hierarchy.
Unverified IHI	An Unverified IHI is allocated to an individual, where the identity of an individual who is seeking healthcare has not been verified using evidence of identity by the HI Service. An Unverified IHI can also be allocated to an individual who is seeking healthcare and would like to remain anonymous.
Verified IHI	A Verified IHI is allocated to an individual, where the identity of an individual who is seeking healthcare and has been verified using evidence of identity by the HI Service Operator.

For further definitions, refer to HI Service Glossary.

1.7 Best practice principles

The following overarching Practice Principles apply to the use of Healthcare Identifiers within a healthcare facility:

- The Healthcare Identifiers Act 2010 governs the assigning, issuing, use and disclosure of Healthcare Identifiers. In addition relevant legislation, especially the Health Records Act and the Federal Privacy Acts, must be complied with;
- The HI Service will not disclose healthcare identifiers to a healthcare provider if the software they use to connect to the HI Service has not passed Compliance, Conformance and Accreditation (CCA) testing;
- All healthcare software systems handling healthcare identifiers are encouraged to comply with the CCA requirements even if they do not access the HI Service directly;
- The provision of healthcare services is not dependent on a healthcare individual having or disclosing their IHI number; and
- The local software system will be the primary location of the IHI. A healthcare facility will use a single master application for allocating a patient identifier and associated patient details. The same application will be used to perform relevant administrative processes such as merges, etc. The master application will broadcast patient details, via HL7, to applications that require this information to be synchronized.

1.8 Acknowledgement

The following is a list, of organisations that have been involved in a stakeholder capacity and consulted either individually or as workshop participants:

- Australian Association of Practice Managers (AAPM);
- Identification, Authentication & Access Reference Group (IAARG);
- Clinical Leads;
- Department of Health and Ageing (DoHA);
- Medical Software Industry Association (MSIA);
- Australian Information Industry Association (AIIA);
- Aged Care IT Vendors Association (ACIVA);
- Department of Health Victoria;
- Northern Territory Department of Health;
- ACT Health;
- Tasmania Department of Health;
- Australian Psychological Society; and
- Medicare Australia.

1.9 Reference Documents

The following references have been used in preparing this document, correct as of April, 2011:

- Australian Health Care Client and Provider Identification Handbook HB222-2006
- AS 5017 Australian Standard - Health Care Client Identification - 2006
- AS 4590 Australian Standard - Interchange of client information – 2006
- AS 4846 Australian Standard – Health care provider identification
- ISO 7812 Identification cards — Identification of issuers
- http://www.aihw.gov.au/data-standards/
- http://meteor.aihw.gov.au/content/index.phtml/itemId/181414
- Healthcare Identifiers Act 2010
- Healthcare Identifiers Regulations 2010
- Privacy Act 1988
- Implementation Collateral Use Case Catalogue
- HI Service Concept of Operations V 2.0
- HI Service Glossary v1.0
- HPI-I Provider Type Classification Reference Guide v5.0
- HPI-O Organisation Type Classification Reference Guide
- Medicare Australia Healthcare Identifiers Licensed Material
- Best Practice Guide for implementing Individual Healthcare Identifiers in Victorian Hospitals and Health Services V0.6

- Implementation Collateral Business Use Cases v1.0
- Implementation Collateral Use Case Catalogue v1.0

1.10 Regulatory environment

There are many elements that apply to the regulation of health information sharing, identification of individual and security of information. These include laws, principles and administrative policies that set out how information may be collected, shared and stored, prohibit specific information flows, or legally authorise information flows that would otherwise be a breach of privacy legislation.

1.10.1 Legislation

Legislative controls on the sharing of healthcare identifiers and health information include:

- Healthcare Identifiers Act 2010 and Healthcare Identifiers Regulations 2010
- Health Records legislation;
- Privacy legislation;
- Freedom of Information (FOI) legislation;
- Public health notifications required under law;
- Child protection legislation;
- HIV AIDS legislation;
- Mental health legislation;
- Power of attorney and guardianship legislation;
- Common law duty of confidentiality;
- Professional requirements and standards; and
- Other legislation, guidelines and standards.

1.10.2 Privacy

Australia's information privacy legislation gives individuals some control over the collection and handling of their personal information. It attempts to strike a balance between competing interests; that is, between the individual's right to privacy and the benefits of the free flow of information. Finding an appropriate balance between these interests is fundamental to the development of e-health in Australia.

Information privacy protection in Australia is legislated under various Commonwealth and State/Territory statutes which overlap but are not identical.

The Privacy Act 1988 regulates Commonwealth agencies, including the Australian Capital Territory public sector agencies, and private sector organisations such as healthcare service providers in the collection, use, storage, and disclosure of personal information. The Act gives individuals the right to know why an organisation is collecting their personal information, what information it holds about them, how it will use the information, who else will receive or access the information, and it provides individuals the right to access the information held on them, as well as the right to correct the information if it is incorrect. Generally, personal information may only be collected by an organisation with the consent of

the individual (or as otherwise permitted by specific privacy principles or laws). The collection of the information must also be necessary for one or more of the functions of the organisation.

1.10.3 Healthcare Identifiers

Healthcare Identifiers in Australia are governed by a regulatory framework which is set out in the Healthcare Identifiers Act 2010 and Healthcare Identifiers Regulations 2010.

This legislation addresses the assignment, use and disclosure of healthcare identifiers as well as setting out a number of unauthorised uses of these identifiers.

The legislation does not provide authority for the use or disclosure of any health information with which the healthcare identifiers may be associated. Any use or disclosure of the health information must be undertaken in accordance with applicable privacy and health information regulatory arrangements.

1.11 Conformance, Compliance, Accreditation[3]

NEHTA in consultation with the health sector including Medicare Australia, the Department of Health and Ageing, the Medical Software Industry Association (MSIA), the Australian Information Industry Association (AIIA), the Aged Care IT Vendors Association (ACIVA), state and territory health departments, has developed conformance requirements and an assessment process to support the safe use of healthcare identifiers by health software systems. These are detailed in the NEHTA publications listed below. Section 9 of this document provides additional details on the CCA requirements and assessment process applicable to HI implementations.

- Healthcare Identifiers Software, Conformance Assessment Scheme, Version 3.0, NEHTA, 3 May 2011; and
- Use of Healthcare Identifiers in Health Software Systems, Software Conformance Requirements, Version 1.4, NEHTA, 3 May 2011.

Software systems requiring direct access to the HI Service must complete both HI conformance testing (as documented in this HI Conformance Assessment Scheme) and Medicare Australia's Notice of Connection (NOC) testing process. The conformance testing described in the Healthcare Identifiers (HI) Software Conformance Assessment Scheme are often referred to as the 'CCA' tests. The CCA tests are performed to assure the safe use of healthcare identifiers by a health software system and the NOC tests are performed to determine that the software can connect to the HI Service.

This first phase of the healthcare identifiers conformance requirements apply to software systems that directly access the healthcare identifiers (HI) Service. For software systems that do not directly access the HI Service, but manage and use local copies of healthcare identifiers, it is strongly recommended that these systems still undergo HI conformance testing in order to support the correct handling of identifiers.

The HI Software Conformance Assessment Scheme and associated test specifications aim to define consistent testing of health software systems that provides a sufficient assurance of conformance to the software requirements for use of healthcare identifiers.

[3] Software Conformance Requirements for Use of HI

Correct handling and use of healthcare identifiers by software systems will improve efficiency and quality of healthcare and reduce errors in managing patient information. Conversely, clinical safety risks may arise from incorrect or inappropriate use of healthcare identifiers.

Due to the significance of these risks, health software systems are to be assessed for conformance to requirements for the use of healthcare identifiers. The health software sector and the Department of Health and Ageing have agreed independent testing is to be mandated for new or significantly changed compliant systems to assure safe use of identifiers.

This testing is to be conducted by test laboratories that have been accredited by the National Association of Testing Authorities (NATA) to perform HI testing. These laboratories are independent organisations that understand the risks associated with incorrect use of healthcare identifiers and perform tests to reduce these risks. Test laboratories can perform testing at the premises of a software developer and can also perform testing in their own test environment.

The healthcare identifiers conformance test specifications contain a set of conformance test cases derived from conformance requirements for the use of healthcare identifiers. Test cases are grouped by business use case. Conformance test specifications have both positive and negative functional test cases, to detect incorrect behaviour and ensure wrong data is handled correctly.

The HI Service Licensed Material may be obtained from the Medicare Australia website after accepting the Licence Agreement – Use of the Healthcare Identifiers Licensed Material for Notice of Connection.

1.12 Change Management

1.12.1 Operational changes and impacts

Changes will be required to IT software systems and business processes to achieve successful integration and adoption of Healthcare Identifiers within a healthcare facility.

Local business processes and the existing capabilities of a vendor's software system developed for the healthcare sector will require further analysis, to determine the extent of changes that may be required. The following changes may be required:

- Business processes:
  - Develop processes for interaction with the HI Service and the use of national healthcare identifiers;
  - Develop alternative processes for operation when access to the HI Service is not available;
- Computer system:
  - Keep system up to date with any HI Service changes;
  - Ensure authentication requirements are met;
  - Maintain authentication certificates as appropriate;
- Organisation Maintenance:
  - Develop and maintain HPI-O network hierarchy if appropriate;
  - Maintain associated HPI-Is if appropriate;
  - Maintain static link with HPI-Is if desired;

- Maintain HI Service Healthcare Provider Directory entry if desired;
- Maintain seed organisation status within the HI Service;

- Education and Training:
  - Provide training as required about using healthcare identifiers; and/or
  - Patient communication about IHIs and the HI Service.

The variation in the processes undertaken by healthcare facilities does not allow for a common approach to implementation of e-health solutions and healthcare identifiers. Further analysis, will be required to develop local implementation requirements and plans.

The following is a representative list of questions, which should be addressed by a healthcare facility for local implementation[4]:

- Under which circumstances should the healthcare organisation create a Provisional or Unverified IHI?

  For example:

  - Provisional or Unverified IHIs are never created;
  - Provisional or Unverified IHIs are always created; or
  - Creation of Provisional or Unverified IHIs is a matter of local policy.

- Under, which circumstances should the healthcare organisation associate an IHI with a patient record?

  For example:

  - Automatically when a Verified or Unverified IHI is returned from the HI Service, or after manual verification.

- What processes need to be followed as a result of an exception process, such as the identification of a duplicate or replica IHI?

  For example:

  - Verify with the patient if present, and/or contact the HI Service operator after investigating local records.

The options for the software system process include:

- Suspend the use of Healthcare Identifiers from active use if a potential duplicate/replica found for both (or more records);
- Remove the Healthcare Identifiers from the patient record and retain history in the system log;
- Merge patient health records after investigation in the local system; and/or
- How frequent should a batch search be undertaken to check the currency of local patient records with IHIs against the HI Service?

Healthcare facilities should consider the impact on their service and businesses processes, and decide the best implementation plan to suit their circumstances.

Things to consider may include:

- Organisational Structure:

[4] Best Practice Guide for implementing Individual Healthcare Identifiers in Victorian Hospitals and Health Services

- Should the Healthcare Provide Organisation (HPI-O) be established as a Seed or Network?
- What information is gathered and published in relation to the Healthcare Provider Organisation (HPI-O) and the linked Healthcare Providers (individuals and organisations)?

- Training:
  - Are employees who are authorised to act on behalf of a healthcare provider organisation, trained in the use of their in- house software system to access and manage identifier data?
  - Are the correct check-lists/practices in place to enable employees who are authorised to act on behalf of a healthcare provider organisation, to correctly identify the patient?
  - Is there sufficient time in the interaction between the employees who are authorised to act on behalf of a healthcare provider organisation and the patient to correctly identify the patient?
  - Do employees who are authorised to act on behalf of a healthcare provider organisation have the time and system functionality to be sure the required record does not exist?
  - Are employees who are authorised to act on behalf of a healthcare provider organisation, aware of the consequences of creating duplicates or proliferating Unverified IHIs where an eligible patient IHI should be found?
  - Are employees who are authorised to act on behalf of a healthcare provider organisation to perform back office functions, trained in best practice on how to effectively search and or interact with the HI Service?
- Data Quality
  - Has the healthcare facility undertaken a rigorous exercise pre-implementation to ensure data integrity and quality on key HI search fields?

    <u>For example:</u>
  - Medicare Australia/DVA card coverage, accurate name, DOB, sex, address details.
  - Are there adequate processes in place to resolve data quality issues resulting from the allocation of an IHI?
  - Are employees who are authorised to act on behalf of a healthcare provider organisation to perform back office functions, aware of the various HI Service channels available for assistance?,
  - Are authorised employees cognisant of the application of the HI service channels to work effectively with them to resolve local and national data quality issues?
  - Do employees who are authorised to act on behalf of a healthcare provider organisation who perform referrals/intakes know how to interact with the HI Service, for resolution of IHI issues?

1.12.2 Training

All employees responsible for registering new healthcare individuals or providers or updating existing registration details should receive training that highlights the

nature, importance, business and the healthcare benefits associated with accurate identification.

The training provided to employees should include information regarding:

- The flow and uses of identifying information;
- The purpose and objectives of searching data;
- Principles and standardised procedures for searching on existing registrations;
- Principles and standardised procedures for registration, including local policies, related to identification and anonymity requirements;
- Quality control feedback and processes; and
- Appropriate use of identifying information and the need to protect individual privacy (e.g. familiarisation with National Privacy Principles).

Some of the considerations for a healthcare provider organisation, in terms of roles and responsibilities in relation to the HI Service include:

Changes in roles or positions;

- Skill upgrades;
- Business process changes;
- Change management processes; and
- Ensuring compliance with relevant regulations.

1.13 Roles and Responsibilities

A number of responsibilities are required to be undertaken whilst interacting with the HI Service. These responsibilities can be performed by existing employees, or within new roles as described below.

1.13.1 Authorised Employee

An 'Authorised Employee' is an individual that will act on behalf of the healthcare provider organisation and have the responsibility for managing interactions with the HI Service to assist with patient administration as well as interactions which includes information management functions with Contracted Service Providers (CSPs).

The status of 'Authorised Employee' may be associated with different types of roles within the healthcare provider organisation. For example, an 'Authorised Employee' may be an outpatient clerk and have contact with the public or an administrative role ensuring data quality in records management.

Types of Authorised Employees may also include:

- Responsible Officer (RO);
- Organisation Maintenance Officer (OMO); or
- Healthcare Provider Individual (HPI-I).

A healthcare provider organisation is responsible for the ongoing management of an 'Authorised Employee's' access and security controls.

Healthcare provider organisations have a responsibility for managing 'Authorised Employees' in accordance with the HI Act 2010.

1.13.1.1 Responsible Officer

A Responsible Officer (RO) is an individual that should be a senior appointment within a healthcare provider organisation and authorised to act on behalf of the healthcare organisation in its dealings with the HI Service. For example, the 'Responsible Officer' may be associated with the role of the Executive Officer to a Chief Executive or a senior position in the area of corporate services. The 'Responsible Officer' should have oversight and authorisation over any changes that might occur within the healthcare provider organisation to enable her/him to fulfil this role effectively.

1.13.1.2 Organisation Maintenance Officer

An Organisation Maintenance Officer (OMO) is an individual, who is authorised by the healthcare organisation to manage the day to day activities with the HI Service. These activities may include maintaining organisational information, manage the security and access controls for all 'Authorised Employees'.

The 'Organisation Maintenance Officer', role may be associated with a position within the Human Resources department of a healthcare provider organisation or a practice manager in a small practice and could form part of the induction of new healthcare providers and management of any restructures and changes to employee positions and responsibilities.

Depending, on the size and service provision of a healthcare provider organisation the 'Organisation Maintenance Officer' may need to inform the HI Service of any additional Organisation Maintenance Officers for a healthcare provider organisation at a 'Network' level.

1.13.1.3 Healthcare Provider Identifier Individual (HPI-I)

A Healthcare Provider Identifier Individual (HPI-I) is a unique identifying number assigned to healthcare practitioners who provide healthcare services and who are eligible under the HI Act 2010. The Australian Health Practitioner Regulation Agency (AHPRA) is responsible for the largest proportion of healthcare practitioners within Australia (approximately 500,000). AHPRA is responsible for their registration and accreditation which is required to enable a practitioner to practice within Australia and is underpinned by the Health Practitioner Regulation Agency National Law Act 2009. Those practitioners who fall outside the responsibilities of AHPRA may apply to the HI Service for a HPI-I if they meet the threshold requirements of the legislation.

The HI legislation defines eligibility in terms of:

- Healthcare practitioner is a member of a professional association[5]; and
- The association must have admission requirements, including qualifications, national membership, standards for practice and ethical conduct, requirements for continuing education, rules and sanctions, representative membership practicing in healthcare.

1.13.2 HI Service Operator

Currently, Medicare Australia is the HI Service Operator as prescribed by the *HI Act 2010*. Section 5 of the *HI Act 2010* defines the HI Service Operator to mean the Chief Executive Officer of Medicare Australia. This is a Commonwealth statutory agency.

[5] *s5 Professional Association HI Act 2010*

The HI Service leverages the existing Medicare Australia infrastructure and utilises its trusted national dataset. This dataset provides the necessary personal information needed to assign a unique national healthcare, and individual healthcare identifier (IHI) to every individual receiving healthcare in Australia. Each individual assigned a unique healthcare identifier has been verified by an evidence of identity process.

Medicare Australia has also designed and built business processes and database to support the assignment of Healthcare Identifiers to healthcare provider's individuals (HPI-I) and organisations (HPI-O).

Elements of Medicare Australia's existing infrastructure have been incorporated into the HI Service design including information policies and customer services such as shop front and online services.

1.13.3 CSP Officer

A Contracted Service Provider (CSP) Officer is an individual that should be a senior appointment within a Contracted Service Provider organisation who is authorised to take responsibility for managing information technology services relating to the communication of health information on behalf of the healthcare organisation in its dealings with the HI Service.

2 Healthcare Identifiers

2.1 Process of identifying Healthcare Individuals[6]

In one form or another, all healthcare providers, as well as users of health data, would ordinarily rely on individuals being identified uniquely and consistently within the healthcare facility in which they work. Most healthcare facilities register their healthcare individuals in a client index (often referred to as a Patient Master Index (PMI) or Master Patient Index (MPI)). Due to complex legal and functional structures of healthcare facilities, some organisations' health data is shared across many physically distant healthcare provider organisations. These client indices enable data held about healthcare individuals to be made available to authorised healthcare providers within an organisation, and enable all data held regarding that individual to be associated with the correct healthcare individual and no other individual. Information systems should also enable healthcare individual information to be held securely in respect of the individual's wishes and rights to privacy and confidentiality, and to ensure compliance with relevant privacy laws.

PMIs or MPIs are a permanent listing or register of individuals on which health information is held by an organisation; that is, healthcare individuals who have received or are scheduled to receive services. The index provides a single reliable source of healthcare individual identifying information, and is central to being able to correctly identify each healthcare individual. The index allows for the retrieval of health information, and provides a key identifier by which all information can be linked to the healthcare individual to whom it relates. PMIs contain demographic and identification information including the healthcare individuals full name (and any other names by which they are known), contact details such as addresses (current and previous), telephone numbers, other contact details, date of birth, hospital unit record (or medical record) number, and generally the name of the healthcare facility.

An Enterprise Master Patient Index (EMPI) is a form of Customer Data Integration (CDI) specific to the healthcare industry. Healthcare organisations or groups of them will implement an EMPI to identify, match, merge, de-duplicate, and cleanse patient records to create a master index that may be used to obtain a complete and single view of a patient. The EMPI will create a unique identifier for each patient and maintain a mapping to the identifiers used in each record's respective system.

An EMPI will typically provide Application Programming Interfaces (APIs) for searching and querying the index to find patients and the pointers to their identifiers and records in the respective systems. It may also store some subset of the attributes for the patient so that it may be queried as an authoritative source of the "single best record" for the patient. Registration or other practice management applications may interact with the index when admitting new patients to have the single best record from the start, or may have the records indexed at a later time.

An EMPI may additionally work with or include Enterprise Application Integration (EAI) or Enterprise Service Bus (ESB) capabilities to update the originating source systems of the patient records with the cleansed and authoritative data.

A key component of an EMPI is the match engine. A match engine may be deterministic or probabilistic. The match engine must be configured and tuned for

[6] Australian Health Care Client and Provider Identification Handbook HB222-2006

each implementation to minimize the false matches and unmatched. The accuracy and performance of the match engine are a big factor in determining the value and return on investment for an EMPI solution.

The attributes a match engine is configured to use will typically include name, date of birth, sex, , address and more. The match engine must be able to give consideration to typos, misspellings, transpositions, aliases, and more.

Even the best tuned EMPI will not be 100% accurate. Thus, an EMPI will provide a data stewardship interface for reviewing the match engine results, handling records for which the engine does not definitively determine a match or not. This interface will provide for performing search, merge, unmerge, edit and numerous other operations. This interface may also be used to monitor the performance of the match engine and perform periodic audits on the quality of the data.

Organisations that would use an EMPI include hospitals, medical centres, outpatient clinics, physician offices, rehabilitation facilities, etc.

2.1.1 Key benefits

By correctly matching healthcare individual records from disparate systems and different organisations, a complete view of a patient may be obtained. With this complete view, numerous benefits may be realised including:

- Better patient care can be provided;
- Improved customer service can be offered;
- In emergency or other critical care situations, medical staff can be more confident that they know medical conditions or other information that would be critical to providing proper care; and
- Historical care related information can be obtained from across organisations.

The HI Service allocates three types of Healthcare Identifiers:

- Individual Healthcare Identifier (IHI)—is a national unique 16 digit identifying number assigned to individuals enrolled in the Medicare program or those who are issued with a Department of Veterans' Affairs (DVA) treatment card and others who seek healthcare in Australia;
- Healthcare Provider Identifier – Individual (HPI-I) — is a national unique 16 digit identifying number assigned to health practitioners who provide healthcare services to the general public; and
- Healthcare Provider Identifier – Organisation (HPI-O) — is a national unique 16 digit identifying number assigned to organisations involved in delivering healthcare services. A healthcare provider organisation is defined as an entity, or a part of an entity, that has conducted, conducts, or will conduct, an enterprise that provides healthcare (including healthcare that is provided free of charge). Examples include: A public hospital or a corporation that runs a medical centre.

In addition to healthcare identifiers a:

- Contract Service Provider (CSP) will also be allocated a national unique 16 digit number following successful registration with the HI Service Operator. This identifier will only be activated when a CSP is authorised by an active healthcare provider organisation (HPI-O).
- A CSP is an entity that provides the following services, under contract to a healthcare organisation identified with an HPI-O:

(a) Information technology services relating to the communication of health information; or

(b) Health information management services.

2.2 Individual Healthcare Identifiers

An Individual Healthcare Identifier (IHI) is a national unique 16 digit identifying number assigned to every Australian resident receiving healthcare. This includes including Medicare enrolees, DVA Card holders the members of the Department of Defence.

The information held by the HI Service is limited to demographic information (such as the individual's name, date of birth and sex) which is required to uniquely identify the individual and their healthcare providers.

Healthcare Identifiers do not replace Medicare Australia or DVA numbers and do not affect the way medical benefits are claimed.

Healthcare Identifiers are an important building block to enable the Personally Controlled Electronic Health Record (PCEHR) system.

Under the Healthcare Identifiers Act 2010, an IHI can be allocated to an individual and used by a healthcare provider without the individual's consent in the communication of health information. Strict privacy laws governing how these unique national healthcare identifiers can be used.

2.3 IHI state and record statuses

This section provides an explanation around the individual record statuses (types) and the status variation in the IHI, as supplied by the operators of the HI Service, Medicare Australia:

There are three record statuses of Individual Healthcare Identifier (IHI).

A Verified IHI – is allocated to an individual that is a known customer of Medicare Australia, DVA or Department of Defence or has provided evidence of identity information that has been recorded in the HI Service by the HI Service Operator to establish the identity of the healthcare individual.

An Unverified IHI –is allocated to an individual, where the identity of an individual who is seeking healthcare and has not contacted the HI Service Operator to verify the IHI by providing evidence of identity.

An Unverified IHI can be merged to another Unverified or Verified IHI record. Unverified IHIs are generally reserved for non Medicare Australia eligible individuals (overseas visitors/diplomats, newborns not yet registered with Medicare Australia) or individuals who are seeking healthcare and would like to remain anonymous.

A Provisional IHI – is created and allocated to an individual at a healthcare facility if they are unconscious or incapacitated and unknown to the healthcare facility. Provisional IHIs are able to be updated to an Unverified IHI record or merged with an existing (Unverified or Verified) IHI via a healthcare facility or updated to a Verified IHI via the HI Service Operator by providing evidence of identity. Provisional IHIs will expire 90 days after the last date of use.

There are five IHI statuses of Individual Healthcare Identifier:

Active IHI – An IHI is considered "Active" in the HI Services when:

- It is either Verified, Unverified or Provisional;

- It does not have a Date of Death;
- Age is not greater than 130 years;
- It is not expired.

Deceased IHI – An IHI has a status of "Deceased" when it is:

- Either Verified, Unverified or Provisional;
- There is a Date of Death present in the record;
- Has not yet been matched with Fact of Death Data (FoDD) from Births, Deaths and Marriages Registries;
- Has not yet reached 130 years; or
- Is less then 90 days of no activity (for Provisional IHIs only).

Retired IHI – An IHI has a status of "Retired" when it is:

- Verified or Unverified;
- There is a Date of Death present in the record and either;
- Has been matched with Fact of Death Data (FoDD) from Births, Deaths and Marriages Registries and has had no activity for 90 days; or
- Has reached an age of 130 years (Verified IHIs only).

Expired IHI – An IHI has a status of "Expired" when it is either:

- Provisional IHI and there has been no activity on the record for 90 days; or
- Unverified IHI and has reached an age of 130 years.

Resolved IHI – An IHI has a status of "Resolved" when it is:

- Either Verified, Unverified or Provisional;
- Linked with another record as part of resolving a Provisional IHI or resolving a Duplicate IHI; or
- End dated as part of the replica resolution process.

The lifecycle of an IHI is represented in Figure 1 below:

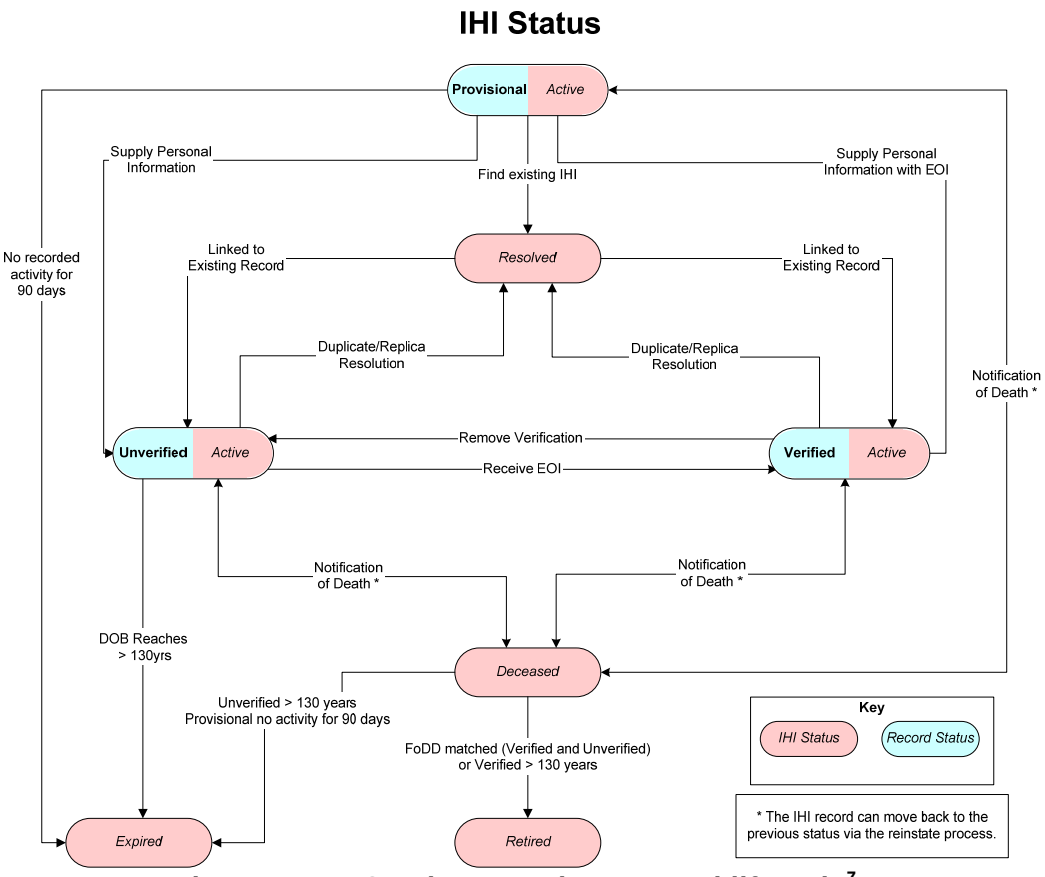


Figure 1 - HI Service record states and lifecycle[7]

2.4 Comparison of IHIs [1]

Upon receipt of a healthcare message containing an IHI, the software system should check against the IHI that is held in the local software system for the patient and determine what to do with discrepancies.

Comparison involves identifying the number, the record status and the status of an IHI returned by the HI Service and deciding if there is a variation to the software system IHI record. Variations can be automatically acceptable (higher status) or unacceptable (lower status). Higher status variations can be accepted by the software system whereas lower status variations will cause an exception to be raised for investigation.

An example of potential acceptability and/or exceptions according to held and retrieved IHIs can be seen in Figure 1.

1. [7] HI Service - IHI Searching Guide V1.0

Table 1: Where an IHI of a varying number is returned:

	HI Service returned IHI		
Software system held IHI	**Verified**	**Unverified**	**Provisional**
Verified	Accept (Resolved - will only be performed by HI Service Operator)	Exception - Error	Exception - Error
Unverified	Accept (Resolved - will only happen with HI Service Operator request by individual EoI)	Accept (Resolved - will only be performed by HI Service Operator)	Exception - Error
Provisional	Accept (Resolved – will only happen following successful merge request)	Accept (Resolved – will only happen following successful merge request)	Exception - Error

Table 2: Where the same number with same or varying record status is returned

	HI Service returned IHI record status		
Software system held IHI	**Verified**	**Unverified**	**Provisional**
Verified	Accept/No change	Exception -Error	Exception - Error
Unverified	Accept (Resolved - will happen with HI Service Operator request by individual EoI or notification of duplicates)	Accept/No change	Exception - Error
Provisional	Accept (Resolved - will only happen with HI Service Operator request by individual EoI)	Accept (Resolved – will only happen with Resolve Provisional IHI – Create Unverified IHI request)	Accept/No change

Table 3: Where the same record status but different status is returned

Note:

Check IHIs will only be undertaken on “Active” or “Deceased” status. A “Deceased” status is considered to be “Active”, as the patient death is unconfirmed and notification of “Deceased” status is only retained in the IHI history table. The status of “Active” remains until “Retired” is retrieved from HI Service.

	HI Service returned IHI Status			
Software system held IHI	**Active**	**Deceased**	**Retired****	**Expired****
Verified / Active	Accept	Exception (Record in History only)	Accept	N/A
Unverified / Active	Accept	Exception (Record in History only)	Accept	Accept
Provisional / Active	Accept	Exception (Record in History only)	N/A	Accept

** A "Retired" or "Expired" returned status will also trigger an exception report for current patients, to confirm the death of the patient or expiry of a record.

Table 3 does not reflect action to be taken when a resolved status is returned, and further local analysis is required to determine appropriate action to be taken.

Important Note:

These examples will not apply in all local healthcare facilities and further analysis will be required to ensure that the action taken is in accordance with local policy settings.

2.5 Healthcare individual search characteristics

2.5.1 Processing HI Service requests

The processing architecture is important to understand before considering specific HI Service functions, as it will drive functionality at the lowest level – i.e. Authorised Employees front office functions within a healthcare facility.

The HI Service is a synchronous service. Using synchronous web services has processing, CPU (Central Processing Unit), queuing, and persistence and memory management implications for client systems. Essentially a synchronous web service requires that the sending system maintain active listeners in memory to wait for a response, for every call made. Each listener consumes a processing thread, and memory presenting some challenges to large environments.

If IHIs are not able to be returned within a reasonable timeframe at the time of registration/admission, local policy settings will dictate the process to be followed for patient identification outputs to be generated (i.e. patient labels/wristbands, etc) and if the IHI is to be included. Later retrieval of an IHI may necessitate the re-working of these outputs.

2.6 Initial bulk uploading of IHIs to a software system for the health sector

The HI Service offers an initial bulk upload functionality of IHIs into a software system for the healthcare sector if they choose to implement IHIs via this mechanism.

The bulk upload functionality allows healthcare facilities to extract entries from their software system (in whole or part-current patients only for example), send the extract for matching of IHIs and return to load to their software system.

Healthcare facilities should ensure that their records contain accurate names (surname as a minimum), sex, date of birth and address information.

Collection of Medicare Australia card numbers, and DVA file numbers, will greatly assist in HI Service searches as these are required parameters in several of the mandated search types detailed in section 2.7.1.

Healthcare facilities should be aware to check accurate 'registration' name/s for inclusion in their software system records. Only exact matches will return with an IHI. Healthcare facilities need to consider the advantages of achieving a bulk upload for 'Active' patient records for the previous two years, if not their whole software system. The HI Service will not return Date of Death information for data cleansing purposes but will return a deceased or retired status.

Software system, healthcare record extracts must be partitioned into the corresponding batch file sizes for online or offline transmission. Synchronous batch searching allows for up to 100 records per batch, and asynchronous searching allows for 2000 records per file and as many files as can be held by the USB device.

2.7 Search for IHI

2.7.1 IHI search technique

Four types of searches for IHIs in the HI Service are statistically most likely to return the correct IHI for a patient record. The types of searches for IHI in the HI Service shall be restricted to these four search types to the likelihood of matching the correct IHI to an individual, thereby avoiding clinical risk of misidentification.

Any health software searching for an IHI in the HI Service using the B2B channel shall use no other IHI search types. An HI implementation need not support all the allowed search types. Note that this requirement does not apply to searches containing an IHI as a search parameter (e.g. searches to validate an IHI).

The search types are:

1. Medicare card search with Medicare card number, IRN, Family name, Given name, Date of birth, and Sex;
2. Medicare card search with Medicare card number, Family name, Given name, Date of birth, and Sex;
3. DVA file number search with DVA file number, Family name, Given name, Date of birth, and Sex; and
4. Detailed IHI search with Family name, Given name, Date of birth, Sex and Address.

More than one search may be performed of each search type. For example search type (4) could be performed with one Given name and if this fails the search type may be repeated with a second Given name for that patient record.

If the health software automatically applies one search after another, then the search iteration shall not continue after a matching IHI has been found.

Health software shall not support any other search types when searching for an IHI in the HI Service. A healthcare provider that needs to perform another search type will do so using another channel to the HI Service, such as the HI Service Team.

The search types may be performed using historical data (e.g. using a person's maiden name for the Family name) subject to the condition that historical data

shall be used only if the IHI searches using current data fail to find a matching IHI.

Software systems should scan the healthcare individual records to locate records which meet data criteria for searching in order to identify potential duplicates prior to searching for the IHI. A potential duplicate message is created against each record and appropriate users are notified of the need for investigation.

The software system should warn a user of a potential error and prevent searches proceeding that do not meet the minimum required criteria. Potential returns which are also considered exceptions include:

- Healthcare provider organisations should develop policies regarding the creation and use of provisional and unverified IHIs long before they actually access the HI Service. For example, overseas visitors, individuals wishing to remain anonymous, newborns); or
- Where a "Deceased" status is returned because the HI Service has been notified that the individual is deceased. The HI Service will return a "Deceased" status and further investigation will be required by the healthcare facility if there is a discrepancy in the status with the expected result.

2.7.2 Restricted HI Service Search Functionality

The HI Service has in built IHI Search functions that are now restricted from use by CCA requirements. This functionality includes:

1. Basic IHI search with Family Name, Given Name, Date of Birth and Gender;
2. ID number search with ID Number (either Medicare Australia Card Number, IHI Number or DVA File Number), IRN, Family Name, Given Name, Date of Birth and Gender; and
3. Detailed IHI search with Family Name, Given Name, Date of Birth, Gender, Full Address, Locality, State and Postcode.

2.7.3 IHI search rules

Where the search is performed by an employee authorised to act on behalf of a Healthcare Provider Organisation (HPI-O).

2.7.3.1 Provisional IHI search rules

Provisional IHIs will only be accessible via single record searches only and will not be returned via batch searches. Single record searches will only return the Provisional IHI record when the IHI number is included in the search criteria.

2.7.3.2 Unverified IHI search rules

An Unverified IHI will be accessible via both single record and batch searching using the permitted search types outlined in section 2.7.1.

2.7.3.3 Verified IHI search rules

A Verified IHI will be accessible via both single record and batch searching using the permitted search types outlined in section 2.7.1.

A response will only be returned when a single unique exact match is located.

2.7.3.4 Historical searches

Historical name and address records will include all names and addresses currently stored in the database from the start date of the HI Service. All amendments captured from this date will be included in historical searching. When the historical search flag is selected historical name and/or address details will be included in the search. The default value for the historical flag will be false.

Important Notes:

- Historical searching may require a longer processing response time.
- The name and address provided for search criteria will be matched against both current and historical data. The name and address matched may be from different periods in time (e.g. a record may be found where there is a maiden name and the address is current or where there is a married name at an old address).
- Expired Medicare cards are not considered historical searching data.

2.7.3.5 Batch searching

There are two types of batch searching available through the HI Service:

- Batch searching available via B2B channel; and
- Batch searching available via a secure USB key.

The batch search uses the same rules for searching and matching as for a single IHI request.

2.7.3.6 B2B batch searching

- Allows healthcare provider organisations to search for up to 100 records.

2.7.3.7 USB key batch searching

- Available using a secure USB key;
- Allow an organisation to search for up to 2000 records per file; and
- Multiple files can be sent on each USB key.

The search results will only include name details used in the search criteria and not additional data. For example, if an alias of ‘Bob’ is used instead of ‘Robert’ and Medicare Australia has that alias registered, then ‘Bob’ not ‘Robert’ will be returned in search results.

The search results will not include the address for the healthcare individual even if it is used as part of the search criteria.

When the historical search flag is set to true, the matching process will search on current and historical names and addresses. The HI Service contains historical addresses which commenced as of July 2010. Name and address changes will be included according to any notifications to Medicare Australia since 1 July 2010.

2.8 General

A healthcare individual or provider is usually identified via a combination of identification details such as sex, date of birth, name, address and/or identifier. It is optimal to collect this data once and reuse as often as possible in accordance with existing privacy or other relevant legislation. The specific information used for identification should be that which is most likely to differentiate this individual from all others registered on a database.

The purpose of searching a database should always be to find if the individual is already registered. This should include identifying registrations already on the system that may relate to this individual, particularly if they are registered with some slightly different information (e.g. an old address or a name they no longer use). If a healthcare individual is registered with the HI Service, information previously collected about them will not be associated with the new record, and this may affect their care. If a provider is registered twice, their full registration details will not be available to those who use the database.

2.8.1 Healthcare Individual and Provider Identifiers

Some Commonwealth, State or Territory laws restrict the adoption, use or disclosure of certain unique identifiers. For example, individual healthcare identifiers (IHI) should only be used in accordance with the legislation. A healthcare individual may be assigned a number of other identifiers by different organisations for different purposes. Other identifiers that can be associated with a healthcare individual include but are not limited to:

- Hospital unit record number (Medical Record Number);
- Area/Region Unique Identifier;
- General practice (record) number;
- Health Consumer Identifier;
- Community health service number;
- Mental Health Service Identifier;
- Home and Community Care Identifier;
- Individual Health Identifier (IHI);
- Medicare card number;
- Department of Veterans' Affairs file number; or
- Centrelink customer reference number.

Medicare, DVA and other identifiers assigned by Commonwealth Government agencies are authorised to be used to obtain an IHI from the HI Service. Organisations should manage these and any other identifiers in accordance with any relevant laws and guidelines.

For further information regarding the standards used for developing and implementing some of these identifiers, refer to AS 5017 and ISO7812.

Healthcare providers may also be assigned one or more of the following identifiers for specific purposes:

- Staff Identification Code or Employee number;
- Medicare Provider number (generally collected and stored for Medicare Australia billing purposes);
- Medical Directory Australia number;
- State Medical Registration Board number;
- Australian business number;
- Professional Organisation Membership number; or
- Healthcare Provider Identifier – Individual (HPI-I).

Unique national healthcare identifiers for individuals and providers are comprised of the following combination of data elements:

- Identifier industry code (e.g. health);
- Identifier country code (e.g. Australia);
- Identifier code for the product (e.g. IHI, HPI-I or HPI-O)
- Identifer code for individual or provider; and
- Identifier check digit.

Key principles for assignment of healthcare individual and/or provider identifiers include:

a. Identifiers are of fixed length, and that if they are numeric the leading zeros are retained;

b. Identifiers incorporate a checking algorithm so as to protect against errors due to (at least) single-character transcription errors;

c. Identifiers are unique and cannot be re-used for different people or organisations, under any circumstance; and

d. Organisations issuing identifier numbers should at all times retain a record of information allocated to previously-valid identifiers, and use some sort of (preferably date-based) validity code, rather than define a 'current list' by merely removing entries.

2.8.2 Name

Healthcare individual and providers may use or be known by more than one name over time. At any single point in time, a person has:

- A name they are currently known by (registered or preferred name);
- A name they are officially recognized by (Medicare Card name – required for reporting to Medicare Australia) which may be different to their registered name or reporting name; and
- May have one or more other names (names they have previously been known by).

All known names should be collected and recorded. The healthcare individual/provider's registered name should always be recorded. Additionally, official reporting names should be captured if different to the registered name, as well as any other names (one or more) that they were previously known as. For example, babies may have a name that distinguishes them as an unnamed newborn baby by recording newborn baby of name and/or maiden name (of mother). Similarly, providers may have a professional or business name by which they are known. All these names should be recorded to enable accurate identification and linkage of past, current and future information regarding the individual/provider.

Capturing the following combination data elements for healthcare individuals/providers is recommended:

- Name Title (abbreviation): e.g. Ms, Rev, Prof;
- Name Title Sequence Number: to indicate the first or subsequent name title;
- Given Name: healthcare individual identifying name within the family group;
- Given Name Sequence Number: the first or subsequent given name;

- Family Name: name in common with other members of the individual's family;
- Name Suffix (abbreviation): e.g. Jnr, MP;
- Name Suffix Sequence Number: to indicate the first or subsequent name suffix;
- Name Usage: i.e. registered, reporting, newborn, professional or business, maiden or other name;
- Preferred Name Indicator;
- Name Usage Start Date;
- Name Usage Start Date Accuracy Indicator;
- Name Usage End Date;
- Name Usage End Date Accuracy Indicator; and
- Name Conditional Use Flag: to indicate if the name is unreliable, not for continued use or subject to special privacy or security requirements.

Note:

Some data elements may have multiple occurrences, for example, name title and given name.

2.8.3 Contact details

Generally all healthcare facilities collect healthcare individual addresses and phone numbers. Organisations collecting healthcare provider identification information would also always collect the relevant provider's addresses and phone numbers. In addition, other electronic communication details may also be collected for communication purposes with both healthcare individuals and providers.

2.8.4 Address

All current and past (previously recorded) addresses for a healthcare individual or provider should be recorded and retained for identification and communication purposes. The types of addresses that may be collected for healthcare individuals include:

- Residential address that should always be collected if possible;
- Mailing or postal address if different to residential address;
- Temporary (accommodation) address for healthcare individuals who live overseas but are currently residing in Australia, or for individuals who are in temporary accommodation while receiving treatment, or for other reasons; and/or
- Business or office address if relevant for communication purposes.

The "No Fixed Address Indicator" may be used when a individual/provider does not have a fixed address.

For providers, the addresses that could be collected are:

- Business or office (service delivery) address: one or more would always be collected;
- Mailing or postal address: if different to the business address;

- Temporary accommodation: for providers who normally live overseas but are currently practising in Australia (or vice versa), or who for other reasons, are in temporary accommodation; and/or
- Residential address: where appropriate.

Australian address information is usually collected using the following combination of data elements:

- Australian Address Line: ideally this is collected using the specific address designation data elements;
- Australian Suburb/Town/Locality; and
- Australian State/Territory Identifier – Postal.

Australian Postcode:

- Australian Delivery Point Identifier; or
- Address Purpose Details (including Address Purpose Start Date and Address Purpose End Date).

International Address information is usually collected using the following combination of data elements:

- International Address Line;
- International State/Province;
- International Postcode;
- Country Identifier; and
- Address Purpose Details (including Address Purpose Start Date and Address Purpose End Date).

Australian Address Line can be collected as the combination of the following data elements:

- Australian Unit Type;
- Australian Unit Number;
- Australian Address Site Name;
- Australian Level Type;
- Australian Level Number;
- Australian Street Number;
- Australian Lot Number;
- Australian Street Name;
- Australian Street Type Code;
- Australian Street Suffix Code;
- Australian Postal Delivery Type Code; or
- Australian Postal Delivery Number.

2.8.5 Electronic communication details

Other identification contact details that may be recorded for individuals or providers including fixed line and mobile telephone numbers, facsimile numbers, pager numbers, email or URL addresses. These are referred to as the ‘medium’ of

communication. Full electronic communication details are therefore collected via the following data elements:

- Electronic communication medium: e.g. phone, fax or pager number, email or URL address;
- Electronic communication usage code: business only, personal only or both; and
- Electronic communication details: the actual number or electronic address to be used for communication.

More than one of any of these communication mechanisms may be recorded for any one individual/provider.

2.8.6 Other identifying information

Healthcare individuals may also be identified via a range of other identifying information, some of which may include:

- Sex: male, female, indeterminate/intersex, or not stated/inadequately described;
- Date of Birth and Date of Birth Date Accuracy Indicator: to indicate level of reliability of the date of birth;
- Date of Death and Date of Death Date Accuracy Indicator: to indicate the level or reliability of the date of death;
- Source of Death Notification;
- Country (or Place) of Birth;
- Birth Plurality: indicating a multiple birth i.e. twins;
- Birth Order: e.g. indicating second of a multiple birth; or
- Healthcare individual identification notes.

Healthcare providers may also be identified via one or more of:

- Sex: male, female, intersex/indeterminate or not stated/inadequately described;
- Date of Birth and Date of Birth Date Accuracy Indicator: to indicate level of reliability of the date of birth;
- Date of Death and Date of Death Date Accuracy Indicator: to indicate the level or reliability of the date of death;
- Healthcare Provider Field of Practice: to indicate the fields of practice or occupation of the practicing provider;
- Field of Practice Start Date, Field of Practice End Date, Field of Practice Start Date Accuracy Indicator and Field of Practice End Date Accuracy Indicator.

2.9 Identification of Healthcare Provider Individual and Organisation

The identification of healthcare providers is similar in concept to healthcare individual identification in that both processes identify individuals and organisations using the same unique 16 digit numbering structure. The main difference in identification of healthcare individuals and providers is the

relationships of individual healthcare providers have to organisational healthcare providers.

Generally it is recommended that provider organisations be registered as unique entities. Similarly, individuals should then be registered as individual providers. Additional data attached to the individual provider record would include the identification of the organisations within which the individual practices. This could be via a linkage key or could include much more detailed information if required for additional functions, such as a provider register.

2.10 Healthcare Provider Identifier Organisation characteristics

Healthcare provider organisations are identified using very similar identification data to that used for individuals. They are identified using a combination of:

- Healthcare Provider Identifier – Organisation (HPI-O): comprising the Identifier Designation, Identifier Geographic Area, Identifier Issuer and Identifier Type;
- Organisation Identifier: comprising the Identifier Designation, Identifier Geographic Area, Identifier Issuer and Identifier Type;
- Organisation Name: comprising the Healthcare Provider Organisation Name and Name Usage;
- Organisation Address: as per individual address;
- Electronic Communication Details: Electronic Communication Medium, Usage Code and Details; and/or
- Other Identification Details: including Organisation Start and End Date, Organisation Start Date Accuracy Indicator and Organisation End Date Accuracy Indicator.

2.11 Collection verses exchange

Codes used for data collection via information systems need not be the same codes used for exchange or extraction of data. That is, if users are familiar with certain codes (such as, 'M' as designated for male in the PMI) for data collection, more accurate data collection may result from using these more meaningful codes. Where alternative codes are used, these should be mapped by the information system to storage codes (such as, '1' as designated for male in the database) for data extraction and subsequent use.

2.12 Healthcare Identifier standards and characteristics

2.12.1 IHI Creation[8]

ISO7812

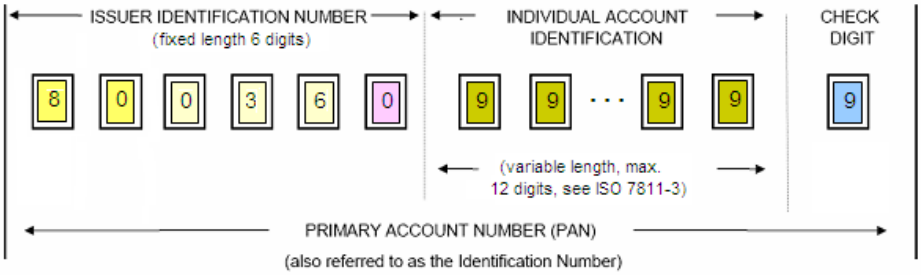
Medicare Australia uses the ISO7812 standard in order to create each IHI.

ISO7812, first published by the International Organisation for Standardization in 1989, is the international standard governing magnetic stripe identification cards,

[8] Healthcare Identifiers Service Information Guide IHI Searching Guide v1.0

such as door entry cards, automated teller machine (ATM) cards, credit cards, and Medicare Card numbers.

Within the HI Service, the ISO7812 contains a single-digit major industry identifier (MII) a six-digit issuer identifier number (IIN), an individual account identification number, and a single digit checksum based on the Luhn Algorithm. The MII forms the first part of the IIN.



The IIN is constructed as follows:

Field Name	Graphic	Format	Domain values	Notes
Industry Code	8 0	2 char fixed mandatory numeric	"80"	ISO 7812 mandates the value for Healthcare is "80". The first character, the MII, of "8" also includes telecommunications and other future industry assignments.
Country Code	036	3 char fixed mandatory numeric	"036"	ISO 3166-1 (Codes for the representation of names of countries and their subdivisions — Part 1: Country codes). Australia is "036".
Number Issuer Code	0	1 char fixed mandatory numeric	"0" "1" "2" "3"	Medicare Australia has registered as "0", "1" , "2", "3"; "0" represents IHI "1" represents HPI-I "2" represents HPI-O "3" represents CSP

The IAN is a unique reference number for a HI participant in the HI service.

Field Name	Graphic	Format	Domain values	Notes
Unique Reference	99...999	9 char fixed mandatory numeric	Randomly generated number	The unique reference number will be a unique 9 digit number that will be randomly generated by the HI Service. It will need to cater for the Australian population (20 million plus) and allow for growth over the life of the HI service.

The IIN and IAN are combined to derive the check digit.

Field Name	Graphic	Format	Domain values	Notes
Check Digit	9	1 char fixed mandatory numeric	0-9	

2.13 Requirements for the national healthcare identification numbering system [9]

As the current steward for the national Healthcare Identifier program, the National E-Health Transition Authority (NEHTA), made the following determination regarding the structural requirements for the Healthcare Identifier:

- All four Healthcare Identifiers must be machine and human readable. They will be usable on items such as cards, tokens, medical documents, and patients' wrist bands;
- All four identifiers need to be visually distinguishable to ensure clinical safety, as all four identifiers will be present side by side in healthcare documents;
- All four identifiers must be the same length (16 digits) to ensure population coverage (21 million) and future availability of numbers, as they will never be reused;
- The numbers should be internationally interoperable in accordance with ISO 7812-1 2006;
- The numbers must not contain any information about a person or organisation such as age, location or field of practice;
- The numbers must not contain any information about a person or organisation that might be discerned from the order in which they were issued. They should be issued randomly from the available number space;
- The numbers must have built-in integrity (IIN and Check digit); and
- Numbers issued for testing and pilot purposes must be identifiable, so they can be easily removed or converted into valid numbers.

These requirements were designed to ensure numbers do not in any way present even the slightest clinical safety risk by causing misidentification due to mix-up in the numbering between healthcare individual and healthcare providers.

The importance of readability cannot be underestimated as it is essential to enhancing safety and quality healthcare outcomes. It will impact usability (and attitudes to change), data integrity (minimise transcription errors) and improve efficiency. Healthcare Identifiers will be validly used in a variety of different settings for a range of healthcare purposes. The following information recommends how the Healthcare Identifiers should be visually represented:

1. A Healthcare Identifier number format for computer displays and manual data entry should read in the following way:
   - Visually rendered as **four groups of four digits**, for example:

8003 6012 0456 7891

2. A Healthcare Identifier number will be used to link the patient to an object identifier (OID) of particular importance when the patient undergoes medical procedures (e.g. implant of a prosthesis):

   - An **object identifier** has the **Healthcare Identifier embedded** and is recorded in the following way:

[9] HI Service use of Issuer Identification Numbers Policy

'1.2.36.1.2001.1003.0.8003.6012.456.7891'

- All Healthcare Identifier OIDs are constructed in the following way:
  a. Split the Healthcare Identifier into **four groups of four digits;**
  b. Remove any leading zeros from the digit group (e.g. 0456 - > 456);
  c. Joining the digit groups into a string, separated with periods - e.g. 8003.6012.456.7891; or
  d. Pre-pending the OID Arc 1.2.36.1.2001.1003 (e.g. 1.2.36.1.2001.1003.0.8003.6012.456.7891

3. A Healthcare Identifier number is embedded in a barcode[10] which is generally used for any hardcopy document where transcription of the Healthcare Identifier is required by the recipient (e.g. pathology laboratories, surgical procedures, pharmacy). A barcode will be used in accordance with healthcare industry standards and is used to improve traceability.

[10] Healthcare is one of the core industries to utilise barcodes to enhance process efficiency. Barcodes are used to manage many critical aspects of healthcare such as to maintain patient's records and medical notes, automate receptions, track and automate medical supplies, check equipment status, and to manage data quickly and accurately.

3 Registration Process

3.1 Identification and registration process

The process of collecting individual identifying information and giving the record a unique identifier is known as registration. The purpose of registration is to uniquely identify an individual and allocate an identifier in order to link information to an individual according to business needs. An organisation's unique identifier should be used to consistently to identify that organisation.

Registration is a distinct process, separate to that of admitting an individual or booking an appointment, though the two processes may be performed at the same time. In some instances, identification confirmation may also occur via an identification check (e.g. a Verified IHI Card requires a 100 point evidence of identity check). Although, it is not compulsory that identification be provided in order to register for an Individual Healthcare Identifier, a healthcare individual can present at a healthcare facility and have assigned to them an Unverified or a Provisional IHI.

For healthcare individuals receiving health services or for providers registering as healthcare practitioners, the following steps of registration are applied:

Step 1: Identification of the individual or (provider) organisation;

Step 2: Collection of registration details into an information system;

Step 3: Determination of whether the individual, or organisation, has been previously registered, by searching the database and reviewing possible matches;

Step 4: Allocation of a unique identifier (or retrieval of existing allocation); and

Step 5: Confirmation of details for previously registered individual's, and update of details as required.

3.2 Healthcare Individual registration

The primary aim of healthcare individual registration is to ensure that any current, previous and future healthcare records are associated with the correct individual. Healthcare individual registration also facilitates the efficient linking of related information including administrative, medical, nursing, laboratory, financial and other relevant information. Sharing and linking such information is integral to the provision of timely, accurate, relevant and reliable data, and is fundamental to the efficient and effective use of health information.

For efficient healthcare individual registration and accurate recording of individual history and demographic data, information must be gathered using effective interviewing techniques, that is, by asking the standard questions. Having the correct and complete record for a healthcare individual will assist in the provision of care to that person. In order to facilitate this type of record a healthcare individual should be registered at the first point of contact or as early in the process as possible. This will aid the creation of and access to a complete health record, healthcare individuals should be registered at the first point of contact or as early in the process as possible.

3.2.1 Registering Healthcare Individuals

Healthcare individuals who should be registered by a healthcare provider include those who have received health services in the past or those new to the service. The types of service for which healthcare individuals should be registered include:

- Community health services;
- Health screening services;
- Counselling;
- Admissions (including waiting lists and bookings);
- Outpatient attendances;
- Emergency department attendances;
- All babies born in a healthcare facility, with multiple births being registered separately;
- Tele-health services;
- Home based services including Hospital-in-the-Home, home visits and outreach services;
- Pathology—healthcare individual from whom specimens are received e.g. blood sample;
- Monitoring—visitors of healthcare individuals who have, or are suspected of having, a communicable disease to enable subsequent follow-up, if required;
- Death certification—healthcare individuals who are 'dead-on-arrival' are generally pronounced dead by a member of staff even though they are not admitted; they may also receive pathology or post-mortem services, and counselling may be provided to relatives;
- Organ donation—to be able to record the care provided to keep the individual alive until time of organ donation;
- Disaster plan services—healthcare individual receiving services following a large scale disaster should be registered in accordance with local disaster plans; and
- Any service where the healthcare individual is unable to be identified at the time of service provision – unconscious healthcare individuals or healthcare individual for whom details are unable to be obtained, should be temporarily registered as 'unknown' healthcare individuals (until correct identification details can be obtained).

Some healthcare individuals that are registered may request to be recorded only under an 'other name' in order to protect their identity. Information systems should allow for such names to be flagged as restricted access and have local policies in place to guide access and security. The types of individuals that may require this service could be staff, individuals under police guard, individual's in police custody, individuals at risk, individual's with court or intervention orders, or persons who are well known (sometimes referred to as VIPs).

Those healthcare individuals that are might be registered separately include:

- Individuals receiving community health based services are generally not registered separately as individuals (individual names are generally recorded but individuals are not always fully registered);

- Babies in utero—details of any tests performed on a foetus or baby in-utero should be recorded in the mother's medical history and against her healthcare identifier;
- Stillborn babies—notification of the birth is required but the baby does not need to be registered by the organisation unless services are provided for the baby (i.e. pathology tests or post mortem examination). Jurisdictional legislation and local policies should be used to guide staff in these circumstances;
- Boarders—some organisations may choose to register these individuals though as they do receive food and accommodation and may need to be billed for services provided (e.g. a 10 day old infant residing with its admitted mother or a parent residing with his/her admitted child); and
- Other exceptions—where due to the special nature of the services the healthcare provider does not register the individual (e.g. telephone counselling about sensitive personal issues). This should be guided by local policy.

3.3 Healthcare Provider registration

Provider registration may be performed to identify healthcare provider individuals that are authorised to provide services and access healthcare individual information within a healthcare facility. Healthcare provider individuals may also be registered in a provider directory.

A provider directory is an information system that contains a register of known healthcare providers (individuals and organisations). A register may be used as a directory to provide information to authorised individuals or organisations on the:

- Identification of one or more healthcare providers;
- Availability of qualified providers in a geographic area;
- Qualifications, credentials and/or experience of a healthcare provider;
- Role or scope of work of a healthcare provider;
- Work locations of a healthcare provider; and
- Contact details of a healthcare provider.

The type of additional information that could be contained in a provider directory could include, but is not limited to:

- Qualifications;
- Specialties;
- Scope of practice;
- Experience;
- Current practicing status;
- Conditions of practice;
- Registration type and details; or
- Special authorisations (e.g. permissions to prescribe certain or restricted medications).

The scope of a provider directory or index can vary widely. Some databases may be limited to a particular type of provider (e.g. Australian physiotherapist graduates) or may have a defined geographic scope (e.g. medical practitioners in the greater Adelaide city). Similarly, some databases may include some or all of

the non-regulated healthcare providers and/or complementary healthcare providers. Examples include: Naturopaths, homeopaths, massage therapists, reiki practitioners and bowen practitioners.

3.3.1 Registration via AHPRA

Australian Health Practitioner Regulation Agency (AHPRA) is the single agency responsible for supporting the National Boards and the National Registration and Accreditation Scheme which commenced on 1 July 2010. AHPRA currently manages the registration and accreditation of the 10 health professions listed below:

- Chiropractors;
- Dental practitioners (including dentists, dental hygienists, dental prosthesis's & dental therapists);
- Medical practitioners;
- Nurses and midwives;
- Optometrists;
- Osteopaths;
- Pharmacists;
- Physiotherapists;
- Podiatrists; and
- Psychologists.

The health practitioner groups managed by AHPRA will be expanded to include an additional four from 1 July 2012:

- Aboriginal and Torres Strait Islander health practitioners;
- Chinese medicine practitioners;
- Medical radiation practitioners; and
- Occupational therapists.

The primary role of AHPRA on behalf of the Boards is to protect the public in accordance with the Health Practitioner Regulation National Law Act 2009 and is therefore responsible for registering practitioners and establishing a register for students. This involves monitoring member healthcare practitioner professional and educational requirements, maintaining an accurate public register of health practitioners that indicates practice status and location amongst many relevant information, and undertaking identification checks, including police checks.

Every practitioner who was registered with a state or territory registration board on 30 June 2010 automatically transferred to AHPRA. Health practitioners under this Agency are no longer required to register to practice separately in each jurisdiction as this is a national program. AHPRA is contacting all registered practitioners, within its responsibility, when their registration renewal is due, to advise them of the new process.

Renewal can generally be done online, but there are some professional categories who must provide hard copies of documentation before renewal can be completed.

Each practitioner's new national registration number is published on the online register and will also appear the national registration certificate for each practitioner, along with the date practitioners should renew their registration.

Registration transition has resulted in variations in practitioner's registration type.

3.4 Healthcare Individual registration issues[11]

It is important to be aware of a number of key issues relating to registration and healthcare identification that can impact communication between information systems include:

- Incomplete (e.g. limitation of source systems);
- Incorrect data capture (e.g. due to communication difficulties or trauma);
- Difficulties experienced by staff collecting the information, especially information perceived by the healthcare individual or staff to be sensitive;
- Incorrect recording and transcription errors;
- Failure to capture and/or track changes;
- Failure of the healthcare individual to provide correct, accurate and legible information (e.g. where healthcare individuals are from non-English speaking backgrounds, literacy difficulties);
- Inadequate search processes for matching against existing data;
- Inadequate search processes for matching against existing data;
- Differing data capture requirements and mechanisms;
- Healthcare individual registration data element requirements differ between organisations;
- Time delays in recording healthcare individual details into the healthcare facilities software systems/database;
- Inadequate staff training;
- Inadequate staff resources; and
- Varying methods of data matching.

Information perceived to be sensitive can be difficult to collect due to:

- Lack of understanding by staff or the healthcare individual regarding reasons why the information is collected and how it will be used;
- Reluctance by staff to ask for information perceived to be sensitive;
- Reluctance of healthcare individuals from certain religions or cultures, or of personal beliefs, to identify themselves;
- Concerns regarding privacy and confidentiality; and
- Inconsistent internal collection practices and/or lack of local guidelines.

3.5 How to improve IHI validation and registration processes[12]

To improve the accuracy of healthcare individual data, information systems should be able to flag data that is known to be of poor quality or unreliable. This data should be excluded from matching algorithms or protocols.

[11] Australian Health Care Client and Provider Identification Handbook HB222-2006

[12] Australian Health Care Client and Provider Identification Handbook HB222-2006

Healthcare facilities should have clearly documented policies, procedures and/or guidelines on their registration process. The process of developing these enables discussion of registration practices, agreement on local business rules, and establishment of consistent documented methods of registering healthcare individuals. Healthcare individual search procedures should take into consideration the individual population and data sources being searched, as correct searching is the key to accurate registration and identification.

The scope of the policies and guidelines developed could include:

a) Healthcare individual registration procedures;

b) Guidelines to ensure staff understand the importance of valid registration, the rationale for data collection and how the information is used:

c) This includes guidelines on collection, storage, use and disclosure of healthcare individual information in line with relevant legislation. In particular, it is a requirement of privacy legislation that healthcare providers (individuals and organisations) take reasonable steps to ensure that a patient is aware of the purposes for which their information is being collected.

   The use of 'collection statements' and other similar processes provide a good opportunity to explain to patients why their information is required. Good communication can minimize the risks of subsequent concerns being raised by patients about information handling processes. It can also maximize the ability of providers to obtain reliable information as patients will appreciate the importance of correct identification to subsequent receipt of safe and appropriate care;

d) Allocation of Healthcare Individual Identifiers (IHI);

e) Where healthcare individuals are registered and by whom;

f) Prepared answers for staff when handling individual's in difficult situations;

g) Specification of the tasks included in job descriptions; and

h) Guidelines to assist collection of information including useful questions to ask when obtaining or clarifying information when searching a patient database.

Once policies, procedures and/or guidelines are documented, there should be a program for employee training, which should include information on:

a. Why healthcare individuals are registered;

b. How the information is used;

c. Why accurate registrations are important;

d. What the local business rules are;

e. Where to obtain information; and

f. Tips for effective searching.

Other procedures that could be defined and used for employee training include:

- Registration system operation and troubleshooting;
- Follow up of incomplete data; and
- Data update and management including whom to contact if errors are identified and how to resolve duplicate registrations.

These should be ongoing competency based training programs to support accurate identification and registration of individual's. The programs should include system application training on non-production versions of the client

database application, and if available there should be an auditing program to ensure registration data quality and accuracy can be monitored and managed.

If further assistance is required, the HI Service can be contacted through the following channels:

Online	www.medicareaustralia.gov.au
Email	healthcareidentifiers@medicareaustralia.gov.au
Call	1300 361 457[13]

3.6 Data cleansing

Data cleansing of healthcare individual information should be undertaken on a regular basis in order to ensure a more accurate data match of healthcare individual registration information with the HI Service. Some common issues that have been identified through initial trials at a number of locations include mismatching of IHI records as a consequence of:

- Invalid Medicare Card number;
- Missing Medicare Card number;
- Invalid address; and/or
- Invalid or missing DVA number.

By improving data collection staff will increase match rates when searching for healthcare identifiers for individuals (IHI) and any associated data.

3.7 General principles of identification & registration of Healthcare Individuals and Providers

The following principles should be applied when identifying a healthcare individual or healthcare provider:

- Healthcare individual/providers must be uniquely identified and registered;
- When face-to-face contact with an individual occurs, then some form of identity verification should be attempted. An acceptable method of verifying who a person is on the telephone needs to be determined, such as a question and answer session. The process agreed should not necessarily be the same for individual's and providers;
- To protect confidentiality and security of healthcare data, the individual performing the registration process should not provide identification data to the healthcare individual/provider for verification, rather open questions should be asked for authentication purposes. For example, a individual/provider should be asked probing questions, such as, where do you currently live, what was your previous address or on what day and month were you born, rather than asking 'do you live at "xyz"?' or 'is your date of birth "full date of birth"?';

[13] Healthcare Identifiers Service Information Guide

- ‘Identification confirmation questions’ and responses can be used to assist identification. These are additional data that are often used to confirm the identity of someone accessing their own data, such as, health data from an information system portal. The types of questions that are commonly offered as options for identity confirmation include ‘What is your mother’s maiden name?’, ‘What is the name of the street where you grew up?’ or ‘What is your pet’s name?’. These are similar to a personal identification number and can assist in the identification of a healthcare individual or provider;
- A thorough database search must be performed for all individuals regardless of whether they indicate that they have previously attended/provided a service or have been registered before or not;
- Key identifying data elements must match the healthcare individual/provider’s current and past demographic details to confirm a previous registration, and be agreed to by the individual;
- Unique national healthcare identification numbers must never be re-allocated once assigned;
- A record of any change to key identifying data elements should be maintained for information audit trail processes; and
- A person master index or provider register must always be accessible to meet current and future information needs.

A planned systematic program of auditing should be undertaken to maintain data quality in accordance with the National Privacy Principles.

3.8 Healthcare Individual data collection[14]

Each time a healthcare individual presents at a healthcare facility, it is essential to check that the healthcare individual’s information is up-to-date and complete by confirming with the healthcare individual. When a healthcare individual’s identifying information changes, the changes should be made in registration systems as soon as the information becomes available. A history of changes should also be retained.

Occasionally it may not be possible to elicit the information required from the healthcare individual themselves (e.g. unconscious healthcare individual). In these situations, information will need to be collected from others such as family and friends, collected at a later time, or recorded as unknown and followed up at a later date.

To ensure efficient and accurate healthcare individual registration, information must be gathered using effective interviewing techniques. Eliciting useful information from healthcare individuals and protecting their privacy. Such techniques include the appropriate use of closed and open questions, good listening skills, awareness of non-verbal cues (e.g. use of eye contact and appropriate body language), empathy and patience.

Open investigative questions commence with who, what, where, why, when or how. These open questions are more helpful in obtaining good quality information than closed questions which elicit only a ‘yes’ or ‘no’ answer. Some probing may be required to clarify information; however, staff should be encouraged not to ask leading, presumptive or multiple (i.e. double-barrelled) questions.

[14] Australian Health Care Client and Provider Identification Handbook HB222-2006

To avoid the healthcare individual being able to view other healthcare individual's information, the registration screen should be located where it cannot be seen other than by the staff member entering the information. If left unoccupied, no information should be left on the screen and workstations should be individually password locked. Screen savers should also be used where possible to reduce the chance of casual observation.

If required, the registration screen can be shown to the healthcare individual to confirm the information contained about them, only when the information on the screen is that which relates to them. The registration screen should not be shown to a healthcare individual during the searching process, nor should a healthcare individual be asked to identify which record on a search output list relates to them. Staff should also ensure that any search list cannot be seen in the background if the registration screen does not hide the search results, in the event that the screen is to be shown to a healthcare individual.

Useful questions to ask to clarify information, when searching for a healthcare individual on the database are:

a) What is your family name/surname/last name?

b) What is your given name/first name?

c) Note: A closed question would be 'Are you Mary Smith?'

d) Are there other ways of spelling your name?

e) Have you ever been an individual at this hospital/centre before?

Note: This question could also be extended to cover any other establishments that are on the individual registration system or index.

f) What is your Medicare Australia and/or Department of Veteran Affairs card number?

g) What is your individual reference number on your Medicare card?

h) What is your IHI number?

i) Were you born at this hospital?

j) Are there any alternative or previous names you may have been known by, for example, maiden name or have you changed your name?

k) What is your address?

Note: DO NOT ask 'Do you live at 20 Smith Street,'

l) Who is your GP (general practitioner) or local doctor?

m) What is your mother's maiden name?

At the point of data collection, healthcare individuals should be informed about the information collected, how it will be used, where it is held, who has access to it and to whom it may be disclosed.

Employees may be provided with a 'Frequently Asked Question & Answers' sheet (FAQs) to assist in the collection of individual information. This type of information may also be included in brochures or fact sheets that can be handed out to healthcare individuals.

3.9 New Healthcare Individual registrations

When a healthcare individual presents at a healthcare facility, an initial search will need to be conducted to locate their Individual Healthcare Identifier (IHI), for

more details on the various search rules that apply please refer to Section "Search for IHI".

A healthcare facility will also need to be able to create Individual Healthcare Identifiers on an adhoc basis, with new registration processes being undertaken for the following scenarios:

- If an initial search does not return an Individual Healthcare Identifier (IHI);
- The patient is unable to be identified (e.g. unconscious or incapacitated); or
- Registering a newborn.

There are two types of Individual Healthcare Identifiers that can be created at a healthcare facility which include an Unverified IHI or a Provisional IHI.

3.10 Searching a Healthcare Individual client database

Healthcare individuals should not be prompted with any identifying details that may have been found on a search, since doing so provides the healthcare individual with information that potentially identifies other healthcare individuals who are registered on the software system database. Doing so would be a breach of privacy laws

Additional questions may be required to obtain details from some healthcare individuals but this needs to be done carefully. This will generally occur when attempting to identify a healthcare individual and reducing the probability of creating a duplicate record. Search output may include multiple healthcare individuals of the same name so caution is required to ensure an exact match.

It may be appropriate in this situation to use a leading question to determine if they have previously lived at a certain address. This can be asked indirectly or generally by asking:

'Have you ever lived in <suburb>?'

Then if the answer is 'Yes',

Ask: 'What was your address there?'

Once the identity of the healthcare individual is confirmed they should be informed about collection of information, how it will be used, where it is held, who will have access to it and to whom it may be disclosed. This information may be provided through privacy brochures and fact sheets.

The following key identifying data are commonly used in a healthcare individual search:

- Family name;
- Date of birth or age; or
- Sex.

In addition, the following identifying data may also be used:

- Other names;
- Health identification number (such as Medicare Card number, IHI number or DVA card number);
- Mother's original family (maiden) name;

- Residential address or suburb;
- Country of birth;
- Telephone number; or
- Date of death.

3.11 Authenticated sources and existing data

There are various authenticated data sources that are recognized for the purpose of interacting with the HI Service.

Data sources are selected on the basis that they can provide high quality demographic and professional information to support the unique identification of healthcare individuals and healthcare providers and limit the risk of incorrectly assigning a Healthcare Identifier.

Medicare Australia, Department of Veterans' Affairs, and Department General principles of identification and of Defence will provide existing demographic information to the service operator to support the assignment of Healthcare Identifiers to the majority of Australians.

AHPRA is referred to as a national registration authority and will be the primary provider of information associated with healthcare practitioners. Medicare Australia also enables healthcare practitioners not covered by AHPRA but eligible under the HI Act 2010 to register and receive a healthcare identifier (HPI-I). There are no other data sources currently enabled by legislation. The establishment of any future professional registration bodies will only occur with the approval of Australian Health Ministers Council

3.12 Security management processes[15]

Access to the HI Service is controlled through the implementation of technical, legislative and policy processes that include;

- Role based access controls, applied to all users of the HI Service;
- Clear separation of roles, such as differentiating between authorised employees who are responsible for maintaining organisational information, and those that require access to individuals' identifiers and other personal information;
- PKI certificates for access by Authorised Employees;
- Implementing physical technical controls for access by HI Service; and
- Smartcards or tokens.

The Healthcare Identifiers Regulations 2010 require that the HI Service operator is able to identify each individual who has accessed the service by name. There are options for how this is done, such as, providing details to the HI Service or retaining a local record that can be accessed by the HI Service upon request.

Best practice principles must be applied for security and access controls when authorised employees are directly accessing the HI Service in accordance with ACSI-33.

[15] HI Service Security and Access Framework

Healthcare organisations will be responsible for monitoring, managing and restricting access to the HI Service by their authorised employees. Organisations will be obliged to restrict access to their PKI certificates through the enforcement of policy, procedures and local system administration controls.

4 Data quality management processes

Data of variable quality is very often matched against other data of variable quality, often leading to considerable imprecision. Data collected may be of poor quality because of:

- Factors influencing data capture including communication difficulties at the point of collection;
- Recording and transcription errors;
- Changes to key identification information that are not recorded; and
- Incomplete searching of existing registration data.

Sound and consistent data collection processes are the basis of accurate data matching and linkage. These processes should be recorded in procedure documents and provided to all Authorised Employees that interact with the HI Service irrespective of whether their role and position is temporary, contract or permanent.

Accurate identification of healthcare individuals and/or providers is reliant on thorough searching processes and consistent methods of registration. A structured information quality management assessment process that reviews data quality on a regular basis is highly recommended. Where data is being linked or being used for clinical care it is vital that data is accurate and monitored regularly.

Data should be validated at the point of entry and not on filing of the whole record. In particular, data used to link healthcare individual/provider records should be validated at the field level rather than at the function or screen level. This will assist in assuring collection of quality data. Accuracy flags add additional mechanisms to support data linkage and allow for exclusion of inaccurate, unreliable or unknown data values from the data matching process. It is also recommended that all the critical data fields have flags to indicate both the quality; the date last verified, checked or updated and start and end dates where applicable.

Routine reports and data management processes should be established to identify duplicate registrations. This may include automated and/or manual process. The resolution of these ‘Duplicates’ should follow an agreed process.

Changes made to an individual’s identification should be recorded by any health information registration or service provision information software system. The old identifying information (e.g. name or address) should be retained for historical purposes, with the new correct information being captured as the new /current identifying details.

Acceptable error rates should be determined by each organisation and measured for compliance.

5 Healthcare Individual client data linkage[16]

5.1 Healthcare Individual client data linkage

Historically, healthcare facilities such as hospitals and community health services have allocated and used a single healthcare individual client identifier within their own organisation. This identifier has generally been known as the unit record number (URN) or medical record number (MRN). Many States and Territories have grouped their healthcare facilities such as hospitals and community health services into broader enterprises (such as Area or Regional Health Services), creating larger management structures and organisations that need to manage a number of patient identifiers used by various parts of the organisation. To be able to provide comprehensive services across these, sometimes very large organisations, these numbers and the related information need to be linked to enable appropriate information to be available to appropriate healthcare service providers.

The methods of linking several patient identifiers across a large organisation include:

a) Allocation of a single unique 'enterprise wide' identifier that replaces other identifiers and is used to identify the healthcare individual across all parts of the organisation (which may be referred to as the client index [for the organisation]), or

b) A behind-the-scenes directory system that enables continued use of the existing patient identifiers whilst linking them within the directory to enable various parts of the organisation to draw on and communicate health information associated with individual patients.

Both of these options contain the same information but are implemented differently. The method of implementation depends on the environment in which the system is being established. Selection of the identifier (unique enterprise number or local record number) that is used locally is generally determined by the logistical implications of adopting the identifier to manage the paper based health records. Hence practically, many identifiers may continue to be used, with a directory linking information as appropriate to support healthcare provision.

5.2 Enterprise Healthcare Individual client index

Where two or more healthcare individual client master indices are linked or amalgamated, various terms have been coined. Common terms are enterprise master patient index (EMPI), healthcare individual client directory, healthcare individual client database, or healthcare individual client master index (CMI). For the purposes of this guide, they will be referred to as an enterprise healthcare individual client index.

An enterprise healthcare individual client index, therefore, is a directory or record of all healthcare individual clients or potential healthcare individual clients registered by an enterprise (an organisation of one or more healthcare facilities).

[16] Australian Health Care Client and Provider Identification Handbook HB222-2006

Although the concept of 'enterprises' is not new to health, the sharing of healthcare individual client information and healthcare individual client indices at an enterprise level is still at an early stage of development.

Work has been undertaken in all Australian States and Territories in the past few years on the development of some form of regional, specialty and/or sector healthcare individual client index (see Appendix B for further details). One of the critical steps in these projects is data matching and the ongoing management of the healthcare individual client indices.

Enterprise healthcare individual client indices usually contain demographic information about a healthcare individual client, linking different identifiers used by other information systems that refer to the same healthcare individual client (while the source systems remain unchanged). With this model, a unique 'enterprise' healthcare individual client identifier is not used, existing numbers are not replaced, and generally a single electronic healthcare individual record is not created. The directory enables linkage of healthcare individual client records to create a longitudinal, multi-facility healthcare record but it does not contain the record itself. It is not a clinical information system.

5.3 Linking Healthcare Individual client records

Healthcare individuals should always be informed when their data is being linked with other data, even if the use of the combined data is the same as that for the source data.

Identifying the healthcare individual within the same system is beneficial, but the system should also attempt to reconcile the same healthcare individual across all of the existing records it has, from all authenticated sources. By doing this, the system can truly achieve a comprehensive record of all activity available on a healthcare individual. The primary identifier cannot be used for this type of reconcile, because the primary identifier is tied to and is valid for only the authenticated source system that generated it.

For example:

A healthcare individual may have a primary identifier of 12345 from source ABC. That same healthcare individual may have a record in system XYZ, but the primary identifier will most certainly be different. The, primary identifier 12345 will most likely be assigned to a different healthcare individual client software system XYZ. So, using the primary identifier to attempt to reconcile these two records will result in an erroneous match, if the authenticated source is not considered, as well.

Reconciliation between authenticated sources can be done using secondary identifiers. Secondary identifiers exist independently of an authenticated source (for example, a date of birth is not assigned by any system (it is a characteristic of a healthcare individual client), but is collected by most systems). Individual secondary identifiers are not specific enough on their own to positively identify the healthcare individual client

For example:

More than one healthcare individual client can have the same date of birth and the same sex will apply to ~50% of a given population. However, if used in conjunction with each other, and with weights given based on the availability and accuracy of the data collected as a second identifier, reconciliation of data can approach a ~100% certainty.

There are several secondary identifiers, which, with proper weighting, can be used to effectively reconcile healthcare individual client across authenticated

sources. Identifiers that are assigned to a healthcare individual client based on information received from multiple authenticated sources can be considered robust secondary identifiers.

5.4 Restricted use of identifiers

Individual client identifiers assigned by the Commonwealth Government such as, Medicare card number, DVA number, and Centrelink customer reference number have restricted usage which is either underpinned by legislation or addressed by Australian standards. These identifiers cannot be used as data elements for healthcare individual client identification or be used as the private sector agency identifier for the healthcare individual client, however are authorised under the HI Act to be used to obtain an IHI from the HI Service.

Some laws establish different rules for public sector and private sector organisations. All healthcare service providers need to be aware of the laws that apply specifically to them. Guidance regarding the use of healthcare individual client identification can be found in the Australian standard AS 5017.

5.5 Data matching

For healthcare individual or provider identifiers to be linked, the identifying data about the healthcare individual/provider needs to be matched. Data may be matched in one of two ways:

a) Deterministic matching—is where data is only matched where identifying information (such as family name, initial of first given name, date of birth and sex) are identical; or

b) Probabilistic matching—is where weights are assigned to identifying data elements to identify whether two records are a true match, a non-match, or a highly probable match.

These techniques/approaches are not mutually exclusive.

Errors can easily occur when matching data as there can be:

a) False non-matches or Type I Errors—which is failure to match identifying data which is associated with the same individual; these errors create duplicate records; or

b) False matches or Type II Errors—which is where records are matched but are in fact not associated with the same individual; these errors are called overlays.

Whenever data linkage involves the use of identifying personal information, providers must ensure that use of the information is permitted under the privacy laws that apply to them. If the information has been collected by the organisation from the individual for the purposes of providing healthcare, and the linkage is being performed for this purpose, then ordinarily it will be permitted by such laws as it is being used for the purpose for which it was collected. Information should not be linked for other purposes and it is strongly recommended that legal advice is sought before any attempts to use information for any other purpose is considered.

5.6 Passive or active mode of data linkage

The implementation options for linking healthcare individual client data across an enterprise include what is termed ‘Active’ or ‘Passive’ modes. The passive mode (retrospective matching) is where the index operates in the background.

Authorised employees, who register healthcare individual client, are only concerned with the local registration of the healthcare individual client and not the enterprise level registration. This form of implementation requires manual data reconciliation of potential duplicates after the registration has occurred.

The active mode (prospective matching) involves direct registration in the broader enterprise-wide healthcare individual client index. Local registration systems, across which the healthcare individual client are linked, interface directly and in real-time to the central healthcare individual client index which allocates the linking identifier. The matching is done at the point of registration and no retrospective reconciliation is required.

5.7 Process of Healthcare Individual client data linkage

The selection of appropriate primary and secondary identifiers, and the configuration of healthcare individual match and reconcile parameters within a system must be assessed individually by each healthcare facility, based on the number and authenticity of sources, and the quality of the data collected for the identifier itself. Below is a partial list of questions that should be asked as part of the healthcare individual identifier design process:

What is the frequency of availability of each of the demographic fields being considered as healthcare individual identifiers?

- What is the level of trust of the data collected in the healthcare individual identifier field?
- How does each healthcare individual identifier field rate in comparison to the other identifiers?

  For example: Date of birth may have a greater weight than sex?
- What is the reliability and consistency with which this identifier is present, and correct, for a given healthcare individual?
- Is the data collected for this identifier a 'free text' field, or do users select from a predefined, codified set of reference data?

Below are some general recommendations for the weighting of certain identifiers:

Family Name should be weighted more heavily than Given Name, due to the variations that can occur with Given Name;

- First Given Name should be weighted more heavily than the second and subsequent Given Names (if second and subsequent Given Names are used); or
- Date of Birth should be weighted more heavily than Sex.

Below are some general recommendations on the level and degree of healthcare individual for a matching:

- Weighted searches, particularly where large databases of healthcare individual client records exist, often take up more system resources and can impact the system's overall performance. It is generally best to do weighted searches only when necessary, and not on information received from authenticated sources; and
- All systems should, if possible, make demographic data elements that are selected as healthcare individual identifiers, required or mandatory fields. Users should pick the values for these fields from a codified 'drop down' list. Free text fields should be avoided.

Therefore, the configuration of a software system for the healthcare sector, to effectively identify healthcare individuals, match them to existing healthcare individual records and reconcile across multiple sources of healthcare individual information is individual to each healthcare facility. Often, the parameters selected and the configuration of the match and reconcile will not prove to be optimum from the initial design. It is critical that any configuration be tested thoroughly prior to implementation.

6 Pseudonymous and Anonymous data

6.1 What is a Pseudonym?

Pseudonyms are often used to hide an individual's real identity and in their broadest context may be used by writers' using pen names and graffiti artists' using tags. However, in the health setting it is anticipated that it will be used by victims of family violence as an added privacy protection and well known personalities.

Pseudonymous healthcare is underpinned by Federal Government policy and by international standard ISO 25237.

6.2 Pseudonymous IHI

In certain circumstances a person may want to access healthcare services using a pseudonym to mitigate against the potential risks of seeking healthcare services using their real identity. The HI Service has the capability to issue a Pseudonym IHI at the request of the healthcare individual.

A healthcare individual will be provided with an alternative name, date of birth and address when he or she applies for a Pseudonym IHI. This will ensure that their personal information held within the HI Service is concealed from other users.

A Pseudonym IHI will be linked to the healthcare individual's Verified IHI via a unique key that will have secure access controls to prevent any visible linkage. A healthcare individual with a Pseudonym IHI will be provided with an IHI card to allow him/her to use it in the same way as s/he would use a Verified IHI card.

Healthcare facilities will not be able to identify when an individual uses a Pseudonym IHI. There will be no flag or information provided by the HI Service to indicate that the IHI for the individual presenting is anything other than a Verified IHI.

6.3 Applying for a Pseudonymous IHI

An individual, seeking Pseudonymous healthcare:

- Must have an existing Verified IHI record; or
- May only have one 'real' and one Pseudonym IHI record at any one time.

An individual seeking to apply for a Pseudonymous IHI record should contact the HI Service Operator, Medicare Australia, to obtain an application form [17].

A third party may request the creation of one Pseudonym IHI record for an individual in their care. In these circumstances, evidence of authority of the third party to act on behalf of that individual seeking pseudonymous healthcare must be provided.

Once, evidence of authority and identity has been confirmed for the third party and the healthcare individual, the HI Service Operator can create a Pseudonym IHI record with a Verified status.

[17] *Application to request a pseudonym Individual Healthcare Identifier record 4484.02.12.10*

Important Note:

The request for a Pseudonym IHI record must not create a duplicate record and at least one of the demographic details provided must be unique and must not match any existing record held in the HI Services database for another healthcare individual. The following demographic details are required to create the pseudonymous IHI:

- First name;
- Family name;
- Date of birth;
- Sex; and
- Address

6.4 Anonymous IHI

Anonymous healthcare is currently provided to individuals across the Australian healthcare sector and in many instances is provided as a free service (e.g. sexual health clinic, adolescent healthcare services). Healthcare identifiers do not change the way that anonymous healthcare services are provided. Individuals can still seek treatment and services on an anonymous basis. In these instances, an IHI would not be used by the healthcare provider.

Alternatively, an individual may take steps to have an Unverified IHI created using an alternative name and other identifying information when they access healthcare services. n

Healthcare facilities will have to determine whether or not to use Unverified IHIs when providing anonymous healthcare to individuals. It is strongly recommended that a healthcare facility consider developing local policy to support authorised employees in the processes required for creation and use of Unverified IHIs.

If local policy supports the use of Unverified IHIs, Authorised Employees should create an Unverified IHI using an alternative name, a new date of birth and new address for the healthcare individual seeking healthcare. Best practice principles recommend that the healthcare individual must be provided with a copy of this information (including the unverified IHI number). This will allow them to use their unverified IHI for ongoing treatment purposes if they so choose.

The healthcare individual will be provided with advice indicating that he or she will be responsible for managing this information should they wish to use it in the future. Individuals should also be advised that a claim for government healthcare benefits may only be made against the details listed on an individual's Medicare card.

An Unverified IHI may remain active, if the individual so wishes, for his or her lifetime, or until the recorded age of the individual reaches 130 years.

The individual may elect to have the information associated with their Unverified IHI merged with their Verified IHI at some time in the future.

7 Healthcare Individual client and provider identification messaging

7.1 Obtaining Healthcare Provider Identifiers

A health practitioner engaged in the direct provision of health services, as defined by the Privacy Act 1988, may be eligible for a healthcare identifier (HPI-I) if they meet the criteria defined in the HI Act 2010. An eligible health practitioner may be registered with AHPRA or with the HI Service Operator.

AHPRA Registered

Requests for the creation of HPI-I records via B2B must be received from a registered and certified data source through the established web service channel.

The HI Service receives regular files from registered and certified data sources containing requests for the creation of HPI-I records.

The following mandatory information must be included in the web service request when creating a new HPI-I record:

- Name details;
- Personal details, including sex and date of birth;
- Address details;
- Provider details, including speciality information; or
- Electronic communication details.

Notification of the newly created HPI-I is provided to the healthcare provider by the data source.

The Healthcare Provider Individuals must provide consent to have nominated professional and business details published in the HI Service Healthcare Provider Directory.

Non AHPRA registered

An HPI-I record may be created by the HI Service Operator where a health practitioner is eligible under the legislation but not associated with a data source such as AHPRA.

To enable the creation of a new HPI-I record, health practitioners must:

- Complete a HPI-I registration form;
- Provide evidence of identity; and
- Provide evidence that they are a member of a professional association that relates to healthcare (as defined in the Healthcare Identifiers Regulation 2010).

7.2 Authenticated sources and existing data

7.2.1 Searching for HPI-Is in the Healthcare Provider Directory

The HI Service Healthcare Provider Directory is established and maintained by the HI Service Operator. The HI Service records the professional and business details of the healthcare providers who have consented to those details being included in the Healthcare Provider Directory. Only authorised users of the Healthcare Provider Directory will have access[18].

Only Healthcare Provider Identifier Individuals (HPI-Is) who have consented to have information recorded in the Healthcare Provider Directory may be searched for and accessed for the purposes of communicating and managing health information. A search can be conducted using their:

- HPI-I;
- Authorised Employee, OMO, RO status; or
- HPI-O.

7.2.2 Enable HPI-O Record in Healthcare Provider Directory

At the same time as creating an HPI-O record for a Seed or Network Organisation an entry may be simultaneously created in the Healthcare Provider Directory.

An entry in the Healthcare Provider Directory may only occur with the consent of the Responsible Officer or the Organisation Maintenance Officer of the Seed HPI-O, or the Organisation Maintenance Officer of a Network HPI-O.

The entry in the Healthcare Provider Directory will only contain the contact details that have been consented to by the Seed HPI-O and may include its business name, number and address.[19]

7.3 Healthcare Individual messaging

To create and send electronic communication of data between systems depends on the accurate transfer of healthcare individual identifiers. HL7 provides a framework for the transfer of healthcare individual identifiers in demographic (ADT) transactions, which can be used to notify healthcare software systems of the presence of a healthcare individual, as well as to reconcile personal records that pertain to the same healthcare individual. HL7 also provides for the transfer of healthcare individual information as part of transactions concerning clinical events for that person. For further information refer to Australian standard AS 4700.1, Implementation of Health Level Seven (HL7) Part 1.

Patient administration provides the Australian model for the transfer of healthcare individual identifiers between systems, using the current version of HL7.

Examples, of electronic communication of data for healthcare individuals may include clinical documents or request services such as a referrals, discharge summaries, pathology or prescriptions to name a few.

---

[18] s31 HI Bill 2010 (Cth)

[19] HI Service Life Cycle Document V.09

7.4 Healthcare Provider messaging

The communication of data for healthcare providers, between health information systems (via interfaces) is done in a number of ways, and in several different contexts. The most common need is in the context of the relationship of the healthcare provider to a healthcare individual (usually under the context of a healthcare visit, encounter or episode of care). AS 4700.1 provides the Australian model for the transfer of healthcare provider information in this setting.

Another, aspect of the transfer of healthcare provider information, concerns communicating reference data on the healthcare providers that routinely provide care within a healthcare system from one electronic system to another. Automating the process of transfer of healthcare provider reference data between systems allows the data to be entered in one master system, with the data being then published to all other interested systems. Several standards exist that can accomplish this type of data transfer, including HL7.

HL7 provides for the transfer of healthcare provider data (as well as other forms of data) in the Master Files section of the HL7 standard, using the MFN (Master File Notification) trigger event. Currently, there is no Australian Standard that provides guidance on the transfer of this type of information via HL7. This section provides a mapping of the content of the Healthcare Provider Identifier data elements that can be used to construct HL7 version 2.4 MFN Staff and Practitioner Master File messages.

NOTE:

At present, HL7 version 2.4 does not have an effective way of transferring detailed information (address, electronic communications details and start/end date). In practice, a custom Z segment can be crafted to contain these data elements, upon the agreement of all concerned parties. Standards practice in Australia with regard to Z segments in HL7 is to limit the creation of these segments whenever possible.

7.5 Healthcare Individual and Provider standards:

The design of the HI Service's individual and provider identifiers is based on the Australian standards AS4846 – 2006 for healthcare providers and AS5017 – 2006 for healthcare individuals.

Software systems will be required to undergo compliance for the healthcare sector, should be as compliant as possible to the standards, in order to meet the requirements of the HI Service. Previous versions of HL7 may not deliver full compatibility when healthcare information is exchanged.

7.6 Healthcare Individual standards

The objective of the AS5017-2006 Standard is to provide the healthcare industry with a specific standard for Healthcare Client Identification for Clinical and Administrative Data Management Purposes (data structure and specification) which promotes uniformly good practice in identifying individuals and recording identifying data. The Standard also provides the basis for future linkage of data as authorised by law and appropriate for clinical management of patients and statistical research purposes.

This Standard applies to all providers of healthcare services in the Australian healthcare system. It defines demographic and other identifying data elements suited to capture and use for identification in healthcare settings and provides

guidance on their application. It also makes recommendations about the nature and form of healthcare provider identifiers.

Accordingly, this Standard includes only the minimum dataset required for unambiguous identification. It is recognized that specific applications such as provider directories or service locators will require additional data to fulfil their purposes. The Standard provides a generic set of identifying information which is application independent and is listed below:

a) Identifying individual and organisational healthcare providers;

b) The recording of healthcare provider identifying data; and

c) Ensuring that data being associated with any given healthcare provider, and upon which clinical communication and data aggregation are based, are appropriately associated with that individual or organisation and no other.

7.7 Healthcare Provider standards

The AS4846 – 2006 standard is the result of healthcare industry's needs for a common, best practice approach to the way data, used for the purpose of identifying healthcare providers, are captured and stored.

Its objective is to provide the health industry with a specific Standard for Healthcare Provider Identification for Clinical and Administrative Data Management purposes (data structure and specification) which promotes uniformly good practice in identifying individual providers and recording identifying data; this will assist significantly in ensuring that records relating to each individual provider will be associated with that individual or organisation and no other.

This Standard has important uses in conjunction with AS 5017, Healthcare Client Identification. For example, when patient healthcare information is shared between various healthcare providers for purposes of clinical management, AS 5017 should be used to ensure the unique identification of the patient associated with a particular provider.

This Standard does not supersede any other standard but acts as a consolidation of best practice principles and guidelines for collection and storage of Healthcare Provider Identification data.

The objectives of this Standard are to promote uniformly good practice in—

a) Identifying individual and organisational healthcare providers;

b) The recording of healthcare provider identifying data; and

c) Ensuring that data being associated with any given healthcare provider, and upon which clinical communication and data aggregation are based, are appropriately associated with that individual or organisation and no other.

Note:

The Standard can be applied to a wider range of providers than might be traditionally considered.

7.8 Messaging – Exchange of data

The exchange of data (clinical documents and/or service requests) for a healthcare individual and/or provider via electronic communication should be validated i.e. Mutual authentication of digital credentials should occur when sending and receiving electronic communication of data.

A message containing an IHI should only be accepted when the organisation and system compliance status is verified. This can be achieved when the digital credentials of a healthcare organisation and/or provider have been authenticated and confirmed.

If the sender is not known to the recipient, the digital credentials are invalid or have been revoked, it is recommended that the digital credentials of the Healthcare Provider Identifier Individual (HPI-I) or Healthcare Provider Organisation (HPI-O) be blocked and the message rejected.

Note:

Healthcare Identifiers may or may not be fully pre-populated within an application system. If however, the healthcare individual identifier is already pre-populated, this would be a system decision point.

Electronic communication of data regarding a healthcare individual may include a Provisional, Unverified or Verified IHI.

8 Contracted Service Providers

8.1 Background

In the drafting of the Healthcare Identifiers Act 2010 and Healthcare Identifiers Regulations 2010 the role of Contracted Service Providers (CSPs) and information technology services they provide to the health sector were recognised. The legislation defines a CSP as an entity that provides:

a) Information technology services relating to the communication of health information; or

b) Health information management services.

To a healthcare provider; under a contract with the healthcare provider.

[s5 Healthcare Identifiers Act 2010]

A CSP can only interact with the HI Service if it is authorised and linked to an eligible healthcare organisation. Authorisation to interact with the HI Service is for an employee of the CSP only, and the HPI-O is responsible for the ongoing management of this contract arrangement and advising the HI Service of any changes.

[s36 Healthcare Identifiers Act 2010]

8.2 Registering Contracted Service Providers

CSPs are required to be registered within the HI Service. The HI Service Operator requires a CSP to complete a registration form provide certified documentation regarding the services provided to health and the nominated CSP Officer.

Once a CSP has been successfully registered with the HI Service, the CSP Officer can elect to display the CSP business details in the HI Service Contracted Service Provider Directory.

A digital credential to facilitate the online communication between themselves and other healthcare providers will be provided at the time of registration.

CSPs are required to pass a set of acceptance criteria as part of the registration process. The criteria consist of:

- ABN or an ACN;
- Declaration of Intention to provide software services to the healthcare sector in Australia; and
- A nominated CSP Officer.

8.3 Functions

CSPs are only able to access the HI Service following authorisation by the HPI-O that they are contracted to perform specific functions.

Although the CSP organisation is registered in the same manner as a Healthcare Provider Organisation, CSPs do not have authorisation to create or join any part of a network of organisations below them. CSPs are recognised as entities in their own right but cannot interact with the HI Service without the authorisation of a HPI-O.

Each CSP must have a CSP Officer registered and linked to the CSP record within the HI Service. This Officer will be issued an individual PKI certificate upon request.

A CSP will be able to access the same suite of HI transactions and processes as the HPI-O they are contracted to via HI Service. However, a CSP cannot:

- Add or remove the relationship between the CSP and an HPI-O;
- A CSP has no ability to manage organisation structures or networks or join a network hierarchy; or
- HPD organisation entry however they can maintain the currency of the CSP data held in the CSP directory.

9 Compliance, Conformance and Accreditation Program

9.1 Software Conformance Requirements

HI software conformance requirements [NEHTA2011a] have been created to help software developers develop health software that:

- Minimises risks to clinical safety, privacy and information security;
- Implements good practice in the acquisition, use and disclosure of healthcare identifiers;
- Assists healthcare providers to comply with the *Healthcare Identifiers Act 2010* [HIACT2010] and the Healthcare Identifiers Regulations 2010 [HIREGS2010]; and
- Achieves the expected benefits of using healthcare identifiers.

These conformance requirements have been defined for a set of business use cases that describe the usage of healthcare identifiers by health software. To determine which conformance requirements apply to a health software implementation, a developer first identifies the business use cases that apply to their HI implementation. Once these are known, the conformance requirements corresponding to the relevant business use cases are identified in the Use of Healthcare Identifiers in Health Software Systems document. Support for some of the conformance requirements is mandatory for the selected business use cases while others are recommended.

Business use cases are described in terms of business process models to illustrate the workflow, tasks and decisions for each business use case. They are intended to be generic and applicable to any healthcare setting. Aspects of a business use case that must be supported by HI implementations are explicitly stated as HI conformance requirements.

HI implementations must conform to the conformance requirements of business use cases they support and not implement any prohibited capabilities for these business use cases.

9.2 The approach to conformance testing

Correct use of the HI Service's Individual Healthcare Identifiers (IHIs) will improve the efficiency and quality of health care. The adoption of IHIs by healthcare providers with the support of software systems will help to address the management of disparate patient information. Conversely, HI implementations that do not properly manage and use local copies of individual healthcare identifiers may pose a risk to clinical safety and fail to realise the full benefits of using the HI Service's IHIs.

When healthcare identifiers are incorrectly managed:

- A healthcare recipient may be misidentified (e.g. due to transcription errors in manually entered identifiers);
- More than one healthcare identifier may exist for the same healthcare recipient; and
- The same identifier may be associated with records of more than one healthcare recipient.

Associating the wrong health information to a healthcare recipient can jeopardise clinical safety, through the introduction of errors such as:

- Medication errors;
- Incorrect surgical interventions; and
- Diagnostic testing errors.

To mitigate these risks and achieve the benefits of using the HI Service's IHIs:

- Conformance tests are derived from HI conformance requirements;
- Conformance tests include both positive and negative functional test cases to ensure that wrong behaviour or wrong data is handled correctly; and
- Software conformance testing is to be performed by NATA accredited, independent test laboratories that have incorporated HI into their scope of testing.

Health software vendor representatives, the Department of Health and Ageing and Medicare Australia have agreed that testing must be performed by NATA accredited test laboratories who have added HI conformance to their scope to ensure that identified risks for the clinically-safe use of identifiers are properly addressed. The use of NATA accredited test laboratories ensures Australian and international testing standards are applied in a consistent manner.

9.3 Test laboratory accreditation

To recognise conformance of a HI implementation, an independent assessment of conformance must be performed by a test laboratory with the following NATA accreditations (www.nata.asn.au):

1. General requirements for testing laboratories [ISO17025]; and
2. Specific accreditation for testing HI implementations for conformance to HI software conformance requirements using the process described in this document. This is subclass 22.40.02 of NATA's '22.40 Healthcare Tests' accreditation.

Test laboratory accreditation uses criteria and procedures specifically developed to determine technical competence. NATA accreditation is a formal recognition of the competence of a test laboratory's ability to perform testing of health software systems that manage and apply healthcare identifiers. Use of accredited laboratories provides assurance of consistent testing according to the HI conformance assessment scheme.

9.4 Relevant technical requirements

Detailed conformance requirements are listed in the following requirements:

- Use of Healthcare Identifiers in Health Information Systems: Software Conformance Requirements [NEHTA2011a]. It is proposed that this NEHTA document be submitted to the Standards Australia IT-014 work group program for 2011/2012 with a view to creating an Australian Technical Specification.

9.5 Minimum conformance requirements

Conformance requirements are defined for a set of business use cases that describe the usage of Healthcare Identifiers by software systems for the healthcare sector [NEHTA2010d].

Business process models describe the workflow, tasks and decisions for each business use case. They are only intended as a guide for developers of implementations and aspects of a business use case that must be supported by implementations are explicitly stated as HI Service conformance requirements [NEHTA2010a].

Implementations must conform to the mandatory and relevant conditional conformance requirements of business use cases they support and not implement any prohibited capabilities for these business use cases.

9.6 Medicare Australia's testing requirements for the HI service interface

A health software system may obtain access to the HI Service either:

- Directly, through web services that access the HI Service interface; or
- Indirectly, through third-party software that accesses the HI Service.

To implement web services for the HI Service, Medicare Australia's Licensed Material should be used. The HI Service Licensed Material contains information for developers such as the HI Service System Interface Specifications [HISIS], HI Service Developers Guide, Web Services Description Language definitions and XML Schema definitions. The Licensed Material may be obtained when developers accept the terms and conditions of the Licence Agreement - Use of the Healthcare Identifiers Licensed Material for Notice of Connection.

Medicare Australia manages the Notice of Connection (NOC) testing process. The NOC tests that a software system can connect to the HI Service. Medicare Australia does not charge developers to test for a NOC.

NOC testing is performed independently to the HI conformance tests. The HI conformance tests are performed to assure the safe use of healthcare identifiers by a health software system and the NOC tests are performed to determine that software can connect to the HI Service.

NOC testing and HI conformance testing may be performed in any order although it is recommended that NOC testing is performed first.

Further information in regards to the Licensed Material and NOC testing process may be obtained from the Medicare Australia website.

9.7 Medicare Australia's HI Service vendor environment

Medicare Australia's vendor environment allows developers to develop and test their HI implementations to ensure they will connect to the HI Service. Medicare Australia's NOC testing is also performed in the vendor environment.

Access to the vendor environment is given to developers once they have accepted the terms and conditions of the Licence Agreement - Use of the Healthcare Identifiers Licensed Material for Notice of Connection. Test data for the HI Service web services will be given to developers to assist with transmissions into the vendor environment.

The vendor environment is a shared by other developers doing business for other Medicare Australia online programs. Medicare Australia does not charge developers for use of the vendor environment.

Further information in regards to the Licensed Material and NOC testing process may be obtained from the Medicare Australia website.

10 Scenarios

10.1 Common healthcare client and provider scenarios

The aim of the following section is to describe potential scenarios between a healthcare individual, healthcare provider individual and/or organisation.

It is not the intention of this document to specify every possible interaction between the HI Service and the above mentioned participants, but to in fact recommend the best practice principles to follow for a particular business scenario.

10.1.1 Mergers and/or Acquisitions

10.1.1.1 Healthcare provider organisation registered within the HI Service.

A primary healthcare provider organisation that is registered within the HI Service acquires another healthcare provider organisation:

- That is also registered within the HI Service; or
- That is not registered within the HI Service; however, the primary organisation would like the secondary organisation to participate in the HI Service.

NOTE:

If the primary organisation, is registered within the HI Service it can either be a Seed or Network Healthcare Provider Organisation (HPI-O).

10.1.2 Healthcare provider organisation that is not registered within the HI Service

A primary healthcare provider organisation that is not registered within the HI Service acquires an organisation:

- That does not meet the HI Service eligibility criteria however, can continue to provide healthcare services and operate as a business entity; and
- Meets the HI Service eligibility criteria.

NOTE:

Organisations not registered within the HI Service can acquire organisations that are currently registered within the HI Service.

10.1.3 Considerations

The following is a list of considerations for healthcare provider organisations that acquire another healthcare provider organisation:

- Will the Responsible Officer (RO) or the Seed Organisation Maintenance Officer (OMO) for the primary organisation continue to perform the role of an RO and Seed OMO for the primary healthcare organisation and the newly acquired healthcare organisation or will a new Responsible Officer (RO) or Seed Organisation Maintenance Officer (OMO) be appointed to the position? If a new Responsible Officer (RO) or Seed Organisation Maintenance Officer (OMO) is appointed to the position of an RO and See OMO, the details need to be changed within the HI Service.
- If the Organisation Maintenance Officer (OMO) for the primary organisation continues to perform the role of an OMO for the primary healthcare organisation are there any new additional Organisation Maintenance Officers (OMO) required for he newly acquired healthcare organisation? If so, the details for the new Organisation Maintenance Officer (OMOs) will have to be registered within the HI Service.
- Is the status of the healthcare provider organisation that has been acquired to be set to 'Deactivated' or 'Retired' from the HI Service?
- A primary healthcare provider organisation that is registered within the HI Service and acquires another healthcare provider organisation, may require the following information to be requested, maintained, validated and/or updated within the HI Service:
    - Responsible Officer (RO) details;
    - Organisation Maintenance Officer (OMO) details;
    - Healthcare Provider Identifier Organisation (HPI-O) details;
    - Healthcare Provider Identifier Organisation (HPI-I) details;
    - Linking HPIs to existing and new HPI-O;
    - Removing links between a HPI-Os and HPI-Is; and
    - HI Service Healthcare Provider Directory details for a HPI-I and HPI-O for publication
- To register a new healthcare provider organisation within the HI Service:
    - Request digital credential for a Healthcare Provider Identifier Organisation (HPI-O);
    - To nominate and register a Organisation Maintenance Officer (OMO);
    - Publish details within the HI Service Healthcare Provider Directory; and
    - Create links between a HPIs and HPI-Os
- Is the Contracted Service Provider for the acquired healthcare provider organisation the same as the primary healthcare provider organisation or is it different?

Appendix A: ICP Business Use Cases

Authorised Employee – Front Office
UC.005 Search for patient health record
UC.010 Register patient
UC.015 Update patient health record
UC.017 Unknown and incapacitated/unconscious patient becomes known
Authorised Employee – Administration / IT
Patient record maintenance
UC.020 Initial PAS IHI load (batch retrieval)
UC.025 Bulk Update of IHI details
UC.030 Maintain data quality (offline asynchronous batch retrieval)
UC.035 Merge patient health records
UC.040 Split patient record
Provide Authorised Employee access to the PAS
UC.045 Individual Logon
UC.050 Shared Logon
UC.055 PAS does not support logon
E-health Messages
UC.060 Generate electronic health message
UC.065 Receive electronic health message
Responsible Officer (RO)
UC.070 Register Seed HPI-O
UC.075 Request digital credential for Seed HPI-O
UC.080 Maintain HPI-O Details
UC.085 Retire Seed HPI-O
UC.290 - Retire, Deactivate or Activate Seed HPI-O
Mergers / Acquisitions
UC.090 Acquire an organisation
UC.100 Maintain RO detail
UC.105 Maintain RO or Seed OMO
UC.110 Establish Seed OMO
UC.115 Maintain Seed OMO
UC.120 Software system audit log enquiries
Organisation Maintenance Officer (OMO)
UC.125 Maintain OMO details
UC.130 Validate HPI-I
UC.295 - Retire, Deactivate or Reactivate Seed HPI-O
UC.190 Link CSP to HPI-O
HI Service Healthcare Provider Directory (HPD)
UC.135 Publish HPI-O to HI Service HPD
UC.140 Link HPI-I to HPI-O in HPD
UC.145 Remove HPI-O to HPI-I link
HPI-O
UC.150 Register Network HPI-O
UC.155 Request digital credential for Network HPI-O
UC.160 Register OMO for Network HPI-O
UC.165 Retire Network HPI-O
UC.170 HPD publication for Network HPI-O
UC.175 Link HPI-I to HPI-O
UC.180 Maintain HPI-O details
UC.185 HI Service audit log enquiry
Contracted Service Provider (CSP)
UC.195 Remove CSP to HPI-O link
Healthcare Provider Identifier Individual (HPI-I)

HPI-I activities
UC.200 Register a HPI-I directly through the HI Service
UC.205 Request digital credential for HPI-I
UC.210 Access HPI-I audit log
UC.215 Maintain HPI-I details
UC.220 Maintain HPI-I details (allocation by national registration authority)
HPD activities
UC.225 Publish HPI-I to HI Service HPD
UC.230 Authorise link to HPI-O in HPD
UC.235 Remove HPI-I to HPI-O link
UC.240 Search for HPI-Is in HI Service HPD
UC.241 Search for HPI-Os in HI Service HPD
Contracted Service Provider
UC.245 Register CSP
UC.250 Publish in CSP Directory
UC.255 Nominate CSP Officer
UC.260 Update CSP Officer
UC.265 Retire CSP
UC.270 Maintain CSP Details
UC.285 Search for CSP in CSP Directory

Appendix B: Comments Log:

For all questions or issues, update the below table with as much appropriate information as possible.

Section Title	Section Number	Comment	Priority (H/M/L)	Reviewers Name

Legend:

Section Title: include the relevant section title.

Section Number: include the relevant section number.

Comment: include what you would like to change and the rationale for the change.

Priority:

- High – guide must be updated to incorporate feedback prior to release.
- Medium – further discussion or clarification required.
- Low – Grammatical or typographical error.