HealthSMART Design Authority

health

# IHI Pre-Implementation Project

## IHI Risk Assessment Report

State Government Victoria

nehta

Authorised by the Victoria Government, Melbourne.

To receive this publication in an accessible format email: ocio.generalenquiry@health.vic.gov.au

# Table of Contents

# 1. Document Overview

## 1.1 Purpose

The purpose of the document is to define the Clinical Risk Hazards and associated Controls in the IHI uptake, as defined in the Victorian Pre–Implementation Project.

## 1.2 Intended Audience

The key audience for this document includes:

- Victorian Department of Health;
- NEHTA;
- Health*SMART* stakeholders, including health services;
- Non-Health*SMART* health services of all types and sizes;
- Other jurisdictional health departments
- Health IT system vendors.

## 1.3 References

- NEHTA HI Service Concept of Operations v 1.0 FINAL Nov 2009
- NEHTA Hazard Assessment Report – Health Identifiers Release 1, v 1.0 , Feb, 2010
- NEHTA Individual Healthcare Identifiers Business Requirements v 1.0 FINAL Nov 2009
- NEHTA HI Security and Access framework v 1.0 FINAL Nov 2009
- NEHTA HI Business Use Case Catalogue v 1.0 FINAL Nov 2009
- NEHTA HI Service Catalogue v 1.0 Final Nov 2009
- NEHTA HI Service Glossary v 1.0 DRAFT Nov 2009
- Victorian DOH IHI Integration Simplified Functional Design
- Medicare Australia HI Service - Technical Services Catalogue R3A v3.0.2.doc
- Medicare Australia TECH.SIS.HI.01 - SIS - Common Document for SIS v3.0.2.doc
- Medicare Australia TECH.SIS.HI.02- SIS - Common field processing reference document for SIS v3.0.2.doc
- Medicare Australia TECH.SIS.HI.03 - Update Provisional IHI via B2B v3.0.2.doc
- Medicare Australia TECH.SIS.HI.05 - Update IHI via B2B v3.0.2.doc
- Medicare Australia TECH.SIS.HI.06 - IHI Inquiry Search via B2B v3.0.2.doc
- Medicare Australia TECH.SIS.HI.08 - Resolve Provisional IHI- Merge Records via B2B v3.0.2.doc
- Medicare Australia TECH.SIS.HI.09 - Resolve Provisional IHI- Create Unverified IHI via B2B v3.0.2.doc
- Medicare Australia TECH.SIS.HI.10 - Create Provisional IHI via B2B v3.0.2.doc
- Medicare Australia TECH.SIS.HI.11 - Create Unverified IHI via B2B v3.0.2.doc
- Medicare Australia TECH.SIS.HI.12 - IHI Batch Searching v3.0.2.doc
- Medicare Australia HI Service - IHI Searching Guide v0.3 Draft.doc

- IHI Best Practice Guide (Draft)
- Healthcare Identifiers Act 2010
- Victorian Clinical Governance Policy Framework – A guidebook, Quality Branch, RRHACS, Victorian Government Department of Human Services, 2009
- Clinical Risk Management – Sentinel Events Reporting, Victorian Government, Department of Health, www.health.vic.gov.au/clinrisk/sentinel/ser.htm

# 2. Introduction

This document outlines the clinical risks associated with the introduction of the HI Service Individual Healthcare Identifiers (IHI) to Victorian health services and recommended controls to reduce those risks. It is a companion document to the Business Requirements for integration of IHI into health IT systems and health services operations produced by the Victorian IHI Pre-Implementation Project.

While the focus of this document is upon Health*SMART* health services, this deliverable is intended to be used by all health services, Health departments, and vendors looking to integrate the IHI into their systems and processes.

A constraint upon this review was that specialist training in NEHTA Clinical Safety Management methodology, and NEHTA Clinical Risk Assessment of Release 3 HI Service functionality was not available at the time of this Risk Assessment. Capacity to participate in Jurisdictional Clinical Safety Management was identified during this project as a gap in NEHTA support. The NHCIOF have subsequently sponsored a Gap Analysis and Clinical Safety Management Model to be delivered by NEHTA in January 2011.

The following documents and resources informed this Risk Assessment undertaken against the introduction of the IHI into Victorian Health services:

- NEHTA Hazard Assessment Report – Health Identifiers Release 1, v 1.0
- Victorian Clinical Governance Policy Framework – A guidebook, Quality Branch, RRHACS, Victorian Government Department of Human Services, 2009
- Clinical Risk Management – Sentinel Events Reporting, Victorian Government, Department of Health, www.health.vic.gov.au/clinrisk/sentinel/ser.htm.

Jurisdictional Public health services are expected to make patient safety a priority and establish active Risk Management policies and strategies. Victorian Health services are required to establish a local hospital based Clinical Risk Management program, in line with the Victorian Health Department's Clinical Governance Policy Management. Hospitals report within 3 days incidents concerning defined 'Sentinel Events'. Sentinel Events which potentially concern the Individual Healthcare Identifier include:

- Procedures involving the wrong patient or body part resulting in death or major permanent loss of function.
- Medication errors leading to the death of a patient reasonably believed to be due to incorrect administration of drugs.
- Infant discharge to wrong family.
- Other catastrophic events.

The introduction of healthcare identifiers, whilst designed to improve quality and safety in clinical communication and electronic identification of patients to support clinical care can also increase risk of harm to patients

The Australian Commission on Safety and Quality in Health Care, Report 'Review of Technology Solutions to Patient Misidentification' (2008) notes that:

Throughout the healthcare sector, the failure to identify patients correctly and to correlate that information to an intended clinical intervention continues to result in wrong person, wrong site procedures, medication errors, transfusion errors and diagnostic testing errors.

In examining the potential for technology to assist in solving this problem, the Commission's key finding noted:

- *Diligent execution of appropriate process/workflow remains the key aspect of patient identification. Technology is an enabler, not a sole solution.*
- *To be successful in the long term, implementation implies ubiquitous deployment of the technology throughout the patient journey.*
- *The importance of formally developed corporate implementation strategies, planning, and process scoping should not be underestimated.*

These principles have been taken into account by this project. The Risk Analysis undertaken in this Pre-Implementation Project considered potential effects and possible controls in the areas of the technology performance, the system maintenance, the users' behaviour and an organisation's policies and procedures adjustments.

The introduction of IHIs into clinical settings is also governed by compliance requirements through the Medicare Australia HI Service , NEHTA Conformance and Compliance Assessment processes. and Security and Access Framework The NEHTA conformity assessment requirements apply to the use of the HI Service by "client" applications – the software systems that use the national service operated by Medicare Australia. These requirements are separate and additional to the HI Service software tests required to fulfil Medicare Australia's Notice of integration (NOI) process. It has been assumed in this report that Health Care management software (PAS and Clinical Systems) will meet the requirements of Medicare Australia's NOI and NEHTA's CCA.

It should also be noted that subsequent Releases of the HI Service, or any extension to the valid uses of the IHI, would require additional review for potential additional clinical risks. The findings noted here relate to assessment against current understood of functionality.

# 3. Scope

The scope of this Risk Assessment includes clinical and privacy risks, associated with the adoption of Individual Healthcare Identifiers (IHIs), and their use within the health service and in e-health messaging between health services. Its scope is based upon IHI related functionality detailed in the Medicare Australia HI Service Specifications release v3.02 (at December 2010). The HI Service releases are governed by the Healthcare Identifiers Act 2010.The scope of functional consideration is restricted to IHI searching, obtaining, updating, transferring and maintaining IHIs within a health service, including;

- batch loading of IHIs into a Health*SMART* health service PAS
- obtaining IHIs for patient records, as an ongoing operational activity
- operational management of IHIs: use of the IHIs to support the provision of healthcare and e-health messaging (e-referral, e-Discharge Summary, e-Prescribing, etc).

The Risks and Controls identified are intended to relate to the Business Processes and Use Cases identified in the Victorian IHI Pre-Implementation Project.[1]

The preferred architecture for the IHI capture in the Victorian health service is as an alternate identifier. The local URN will not be replaced in the short term by the IHI in Victorian health services.

This Risk Assessment did not consider the obtaining and use of healthcare identifiers beyond the individual healthcare identifier (IHI), i.e. the scope does not include Provider Healthcare Identifiers, HPI-I and HPI-O.

[1] See Integration of Individual Healthcare Identifiers, Victorian Department of Health, IHI Pre-Implementation Project, NEHTA, 2010.

# 4. Risk Assessment Report Summary

## 4.1 Approach

Review of the Hazards associated with the implementation of Individual Healthcare Identifiers into the Victorian public health sector was undertaken through a series of workshops with health service representatives. Representatives included health information managers and clinicians, and a representative of the Quality and Safety Branch, Department of Health Victoria.

The participants were informed by an earlier Assessment Report on Healthcare Identifiers Release 1, undertaken by NEHTA, as an indication of the nature of potential hazards to be considered.

The workshops identified four hazard areas associated with IHI implementation, including:

- Misidentification of the patient with IHI.
- Inability to identify the patient by IHI in clinical care.
- Privacy of patient information breached.
- Whole or part of the system unavailable or access denied.

The Hazards discussed were aligned, where possible to a subset of those identified in the NEHTA Assessment report on Release 1.

A classification system[2] was used to assess the level of clinical risk, including severity and likelihood associated with an identified hazard. The Risk Classification system used is summarised in Appendix 1.

## 4.2 Implementation Assumptions

For the purposes of this risk assessment, it has been assumed that Vendors and health services will implement:

- Business processes to enable end users to adapt and establish new working practices to maximise the efficient use of the IHI.
- Policies and procedures to enable and direct end users in the areas of access and use of the system and methods of maintaining business continuity in the event of a system failure.
- Appropriate local configurations to ensure interface with the health services downstream systems and testing this, as required.
- Training of end users to ensure their competence in the use of the system as designed, the significance of key processes and any workarounds that may be required.
- Quality procedures to ensure the accuracy of any patient related demographic and identifying data, input by end users.
- Use of the IHI in conjunction with the local UR number for internal clinical and administrative patient activity.

[2] NEHTA Hazard Assessment Report – Health Identifiers Release 1, v 1.0 , Feb, 2010, Sentry Clinical Safety Risk Assessment Criteria.

## 4.3 Results Overview

Assessment of the level of Clinical Risk associated with the introduction and use of the IHI was seen to be mitigated internally for health services through its use in conjunction with a local UR number. The effect of not relying solely on the IHI was that it reduced overall risk levels. Therefore it is important to realise that the ratings noted in the following review would have been assessed as higher in a situation where the IHI is used singularly to identify a patient.

Where the IHI is used singularly at the point of exchange between health services, ie the sending or receiving a patient referral with an IHI, increased checking of patient demographics with the HI Service to verify the IHI has been included in the controls.

There were two key Clinical Hazards reviewed where the clinical risk was assessed as Medium, however only where the IHI is used in conjunction with a local UR number. If the IHI is used in isolation then these Clinical Hazards would result in High risks.

The identified Hazards were:

- Misidentification of the patient associated with an IHI.
- Inability to identify the patient by IHI in a clinical care setting.

The rating of Medium defines that the clinical risk is of moderate severity and that it may create a situation that is serious and potentially life threatening, however the clinical risk may also be avoided/prevented by a Clinician. This level risk requires that stakeholders be notified of the risk as soon as practicable and appropriate mitigating actions agreed.

If the IHI is used singularly these Clinical Hazards would be considered High risk. High Risk signifies major or catastrophic severity risks that create a situation that is inherently and immediately threatening to a patient's life. The clinical Hazard may results in permanent harm and/or death to a patient. Harm is unlikely to be prevented by a Clinician in these circumstances. This category will also apply to a Clinical Hazard that causes many occurrences of Moderate or Major Severity.

There were a further two key Hazards reviewed where the clinical risk was assessed as Low, including:

- Privacy of patient information breached.
- Whole or part of the system unavailable or access denied.

The rating of Low defines that the clinical risk is of minimal or minor severity and it may present significant or latent risk, which is not immediately or necessarily life-threatening. Quality of care may be impacted, however harm is likely to be prevented by a Clinician. These low level risks represent justifiable residual risks where a report, such as this, documents the recommended controls and supporting evidence.

Appropriate controls for each of these Hazards are detailed in section 5.

It is important to note that the assessment of all hazards was made in the context of the IHI being an **alternate identifier** in the Victorian health service system. Significant risk was seen to be offset or modified by the existence of a local URN in addition to the IHI.

Over time the IHI is intended to become ubiquitous, certainly as a patient reference in care coordination business processes and e-health messages. While not being considered currently, some health services may elect to replace their local URN with the IHI.

With each new Release by the HI Service, additional Risk reviews should be undertaken, as changes may have taken place or additional services provided. Additional risk assessments should be conducted at the time of implementation by a health service, or upon any change in use or reliance on the IHI by a health service.

It was agreed by the reviewers that health services in Victoria should not rely solely on the IHI (or the URN) for patient identification, but would always use available patient demographic information as well.

General findings by the health service representatives also recommended training and (organisational) change management to enable skills development for all those responsible for IHI capture and maintenance. The detailed implementation plan for the IHI was not considered in this report.

It was also recognised that additional funding and/or personnel would be required in the implementation of the IHI. Additional resources were seen as needed to incorporate this identifier into clinical settings, due to changed business processes required until the IHI becomes common and exists as a standard in patient identification.

## 4.4 Discussion of the Hazards Assessed as Medium

The following Clinical Hazards were identified with a status of Medium Clinical Risk when used in conjunction with a local URN and of High Clinical Risk when used singularly:

- Misidentification of the patient associated with an IHI.
- Inability to identify the patient by IHI in a clinical care setting.

In both the Clinical Hazards assessed as Medium/High the risk outcome could result in:

a. Clinician may perform treatment on the wrong patient.

b. User may not be able to contact a patient when it is urgent to do so, e.g.

   i. Adverse or unexpected test results received
   ii. Changes to planned treatment or pre-admission instructions
   iii. Changes to drug regimen

c. Written communications with the patient such as appointment letters may be delivered to wrong address, wrong patient.

d. Users may be supplied inadequate or incorrect output from decision support algorithms that utilise demographic data, e.g. age, gender.

Detailed controls were identified for each including controls for system operation, person operation, and organisational policy and training.

### 4.4.1 Misidentification of the patient associated with an IHI

Misidentification was seen as a frequent or probable occurrence, in initial uptake, where data cleansing may not have occurred at the local PAS level and where duplicate records may not have been pre-identified and merged.

In the absence of agreed controls reducing this hazard, the following potential outcome of misidentification of patient may include:

- Users may inappropriately associate a patient or their clinical record with another patient's record.
- User/system may allocate an IHI to the wrong patient record.
- User may allocate an IHI to multiple records (duplicates not identified) for the same patient.
- When accessing a patient record in the future, using the correct IHI an inappropriately linked record may be returned or the correct record possibly with important information may not be found (i.e. the user may not recognise the linkages between patient records).

Assumptions were made in considering the controls appropriate for this hazard, including:

1. The HI Service has correctly associated the Verified IHI to a 'valid' individual using a Trusted Data Source marker. Eg Medicare or DVA number.
2. The local service may not have the same demographic data as the HI Service has for the individual.
3. The local service may not have the same TDS identifier for the individual as the HI Service has for the individual (Historical Medicare numbers will be included in HI Search, however Medicare card fraud cannot be discounted).

4. The local service may not have the same data structure capabilities as the HI Service, for optimised search capability.

Possible mitigations for this hazard include:

- Data quality assurance within PAS applications (standards applied, accurate Trusted Data sources present).
- Policy development at local level regarding access to and control of IHI information.
- Business process changes and training in registration practices and maintenance( front and back office procedures for allocating and resolving IHI).
- System rules and restrictions on search and application of IHIs.
- Policies and training to prevent reliance on the IHI alone for patient identification.

The residual likelihood[3] of this hazard was seen as less frequent but still present with a continuing Medium to potentially High clinical risk. It is the expectation of the reviewers, that the controls suggested are acted upon during implementation in order to mitigate this ongoing risk.

Full details of controls are included in Section 6.

### 4.4.2 Inability to identify patient by IHI in a clinical care setting

Inability to identify the patient by IHI in clinical care setting was seen as probable to occasional likelihood, especially in the event of IHI use in addition to the local URN. This hazard was considered to be more prevalent during the initial phases of implementation, until the IHI was a ubiquitous identifier for all patients.

Lack of identification of the patient by IHI during clinical care was seen as an issue where:

- Physical and or technical limitations (primary or downstream system limitations) results in an inability to display the IHI on all outputs (eg wristbands, pathology orders, etc);
- The IHI was not retrieved on commencement of an episode of care (confirmation and/or timing of receipt delaying availability).

This hazard was considered to be partially mitigated in the initial phases of implementation through the continued use of and reliance upon the local URN. However if the controls are not adequately addressed, then the hazard would be carried into later phases where it is expected that the IHI should become a reliable and commonly used identifier. The hazard therefore is seen as one of transition and mitigated by acceptance of the IHI over a specified time. As there is currently no specified uptake timetable, this risk could remain open.

The potential outcomes of an inability to identify the patient by IHI include:

- User may associate the patient with the wrong record/procedure.
- Clinician may perform treatment on the wrong patient.
- The user may not be able to contact a patient when it is urgent to do so; e.g.
    - Adverse or unexpected test results.
    - Changes to planned treatment or pre-admission instructions.
    - Changes to drug regimens.
- Written communications with the patient such as appointment letters may be delivered to wrong address, wrong patient.
- Users may be supplied inadequate or incorrect output from decision support algorithms that utilise demographic data, e.g. age, gender.

[3] Residual Likelihood referrers to the degree of likelihood of the Risk remaining after the controls have been enacted.

The following assumptions were made in considering the controls appropriate for this hazard, including:

1. The local system has the ability to assign an IHI to a patient record.
2. The local system has the ability to produce outputs identifying a patient by IHI and required demographic details.
3. The local system has the ability to update IHI output identification in a timely manner according to HI Service changes to IHI.

Possible mitigations for this hazard include:

- System requirements for accurate display of IHI against patient details on all outputs, including bar coded IHI.
- System requirements for transfer of IHI (including all components) to all downstream or external systems, including supporting demographic information (ie that information used to obtain or check the IHI).
- Organisational change to train and encourage user best practice in acquiring an IHI upon registration.
- System checking of the IHI upon patient presentation and referral on and the transfer of only the latest available IHI.
- Policies and user training to ensure that the IHI alone is not used to establish the patient's identity.

Residual likelihood of this hazard was seen to be probable with a continuing Medium to High clinical risk.

Full details of controls are included in Section 6.

## 4.5 Discussion of the Hazards Assessed as Low

The following Clinical Hazards were identified with a status of Low Clinical Risk:

- Privacy of patient information breached
- Whole or part of the system unavailable or access denied

These risks were considered to potentially present significant risk to the patient, though not immediately or necessarily life-threatening. Harm is likely to be prevented by the Clinician. They may also present a latent risk impacting the quality of care.

The likelihood of these risks were assessed as remote or improbable in regard to patient privacy breaches and probable in terms of system failure, but the severity of each was assessed as minor or minimal.

### 4.5.1 Privacy of Patient Information Breached

This hazard was assessed as remote or improbable both in immediate and residual risk, particularly as the IHI has no patient identifying features of its own. A breach of privacy may occur where an IHI and other identifying data is transmitted to a third party incorrectly or inadvertently. Internal health service controls are assumed and described in the controls section, which are meant to avoid inappropriate access.

The hazard was perceived as possible with the following potential outcomes:

- Patient information, including the IHI, is inappropriately revealed to a third party. The organisation and responsible individuals will face legal penalties.

The following assumptions were also recognised as system or health service features which will guard against this risk:

1. The Organisation (health service) has policies and procedures which support privacy and security.
2. The Organisation has instituted, and enforces, security access to the HI Service and related data according to the legislative and regulatory requirements.
3. The local system has role based access controls, to a suitable level of granularity.
4. The local system includes full audit trails of all actions against a patient record.

Possible mitigations for this hazard were identified in areas of:

a. Best practice guide, education / training and the compliance regime with regulations.

- System features enhanced to include security based access and full audit trail capability, including user training to ensure userids and passwords are not shared between staff, and sessions are locked or closed when the user leaves the terminal.
- Adoption of the mandatory elements of the NEHTA Security and Access Framework, including protection of IT systems and data.

Full details of all suggested controls are noted in Section 5.

### 4.5.2 Whole or part of the system unavailable or access denied

This risk was assessed as probable or occasional in immediate or residual risk, with minimal or minor severity. This risk is mitigated by the IHI being an alternative identifier to a local URN, which is not dependent on the HI Service infrastructure and will suffice as an alternative (at least in transition period).

The Potential Outcome of the hazard was seen to be that the patient may not be able to be identified by their IHI in clinical setting in a timely manner, and:

a. the system may not be able to associate an IHI with the patient
b. the system may not be able to validate or check an incoming IHI from an external source (referral, order or discharge summary)
c. the user may associate the patient and a record or procedure incorrectly.

If this hazard eventuates then the risks described in hazards 001 and 002 may come into play for specific periods of time.

It was assumed however that:

1. The HI Service performs according to established SLAs and notifies organisational users of scheduled outages.
2. The Organisation has Continuity of Business policies and procedures which support system failures/downtime.
3. The Organisation has instituted security access to HI Service according to the legislative and regulatory requirements.
4. The organisation has maintained Security and Access compliance according to HI Service requirements.
5. RO and OMO roles are defined within the organisation and staff are committed to meeting the demands of these roles.
6. The local system has role based access controls.

Possible mitigations for this hazard were identified in areas of:

- System behaviour to queue requests to HI Service for later action. Manual processes adopted, Business continuity plans adopted.
- HI Service SLAs and local system performance guarantees.

- System conformance with Medicare Australia and NEHTA CCA requirements.
- Appropriate access controls enforced locally.
    - Full details of all suggested controls are noted in section 5.
- Medicare Australia and NEHTA to ensure that the HI Service meets sector availability requirements.

# 5. Detailed Hazards Assessment and Recommended Controls

## 5.1 Hazard 001: Misidentification of the patient associated with an IHI

<table>
<tr><td colspan="2">HAZARD: 001 Misidentification of the patient associated with an IHI.<br><br>(Includes NEHTA Release 1 Review Hazard H010 & H020)</td></tr>
<tr><td>Hazard Context<br><br>Relates to the whole or part of the HI Service and local system end to end IHI search and retrieval.<br><br>Applies to all channels through which the IHI is supplied.</td><td>Severity: Moderate to Major</td></tr>
<tr><td>Initial Likelihood: Probable</td><td>Residual Likelihood: Occasional</td></tr>
<tr><td>Initial risk class: Medium where used in conjunction with URN and/or demographic data. High where used singularly.</td><td>Residual risk class: Medium where used in conjunction with URN and/or demographic data. High where used singularly.</td></tr>
<tr><td colspan="2">Potential Outcome:<br><br>1. Uniqueness property of IHI not maintained<br>a. Users may inappropriately associate a patient or their clinical record with another patient’s record.<br>i. User may allocate an IHI to the wrong patient record.<br>ii. User may allocate an IHI to multiple records (duplicates) for the same patient.<br>b. When accessing patient record in future, using the correct IHI an inappropriately linked record may be returned or the correct record possibly with important information may not be found.<br>i. If IHI is allocated to wrong patient record and this record is automatically matched to other internal records (in case of multi-campus enterprise), which are linked across that enterprise for use in clinical systems, there is a potential outcome involving clinical risk around diagnostic tests, medications, etc.<br>2. Value error:<br>a. End user may not be able to contact the correct patient when it is urgent to do so; eg:<br>i. Adverse or unexpected test results<br>ii. Changes to planned treatment or pre-admission instructions<br>iii. Changes to drug regimens<br>b. Written communication with patient such as appointment letters may be delivered to wrong address, wrong patient.<br>c. End users may be supplied inadequate output from decision support algorithms that utilise demographic data, e.g. age, gender.</td></tr>
<tr><td colspan="2">Assumptions:<br><br>1. The HI Service has correctly associated the Verified IHI to a ‘valid’ individual using a Trusted Data Source marker. Eg Medicare or DVA number<br>2. The local service may not have the same demographic data as HI Service has for the individual.<br>3. The local service may not have the same TDS identifier for the individual as the HI Service has for the individual.<br>4. The local service may not have the same data structure capabilities as the HI Service for effective search capability.</td></tr>
</table>

| | | | |
|---|---|---|---|
| Causes | | Controls | |
| System | 1. No match found when searching HI Service– unable to match IHI with a patient record. | 1.1 Ext | The user will search for a patient using both IHI and demographic details in combination, in order to ensure selection of correct patient record.<br>Alternatively, the user may search by the IHI alone, but must then use available patient demographic information to ensure that the correct patient record has been found. |
| | | 1.2 System | Local system allows search criteria on IHI data. Searches for patient records should be undertaken in conjunction with other demographic data and/or Trusted Data Source (Medicare or DVA number). |
| | | 1.3 System | Where demographic search alone is performed the local system will iterate through aliases and alternate address information for unsuccessful match results from HI Service queries. |
| | | 1.4 Ext/Org/ System | Local policies and processes for **registering** patients, including IHI capture, include best practice data capture and validation rules. |
| | | 1.5 Ext/Org | Front office/user best practice (including asking patients for details on their Medicare record) exists when **updating** patient demographics/TDS on presentation.[4] |
| | | 1.6 System | The system will support an automated ‘ ‘Check IHI’ function if any crucial patient demographic elements change (eg Given/Surname/DOB/Sex/Medicare Card/DVA details) |
| | | 1.7 System/Org | Processes to resolve the situation in which an IHI should be available will be reflected in the system, and in the Best Practice Guide. |
| | | 1.8 Ext/System | The IHI fields will remain blank until further information is available from the patient, if an IHI cannot be retrieved for the patient. |
| | | 1.9 Ext | In future use of IHI in the context of PCEHR the user may be required to establish the patient’s identity at the point of care, ensuring a correct allocation of a Verified IHI is established. (may require photo ID or similar) |
| System | 2. Match found to a local record however incorrect patient identified.<br>o Fault in PAS data, resulting in a false IHI match returned<br>o Fault in HI Service data, | 2.1 System | Local system stores patient demographic data (in a format consistent with that used in the HI service) according to accepted Australian standards.<br>(Note that the address format remains a potential risk, with few health IT systems supporting the Australian standard. Other solution options may be available.). |
| | | 2.2 System | Local search criteria allow IHI details only to be returned where there is exact match, within the PAS, of minimum unique demographic data. |

[4] Any recorded patient information that does not align with the HI Service, or Medicare Australia, record will result in an IHI not being matched. The entering

| | | | |
|---|---|---|---|
| | resulting in a false match returned | | (Minimum unique data includes selected items from Given/Surname/DOB/Gender/Address/TDS) |
| System | 3. Manual IHI transcription errors | 3.1 System | Local system supports electronic capture of data from the HI Service and accurate display of IHI format. Manual entry of IHI data is largely prevented, and is only available through exception management processes. |
| | | 3.2 System | Local system allows manual entry of data only where a check digit function exists to validate entry, and the IHI is checked against the HI Service following manual data entry. If either check fails the IHI will not be stored against the patient record, and an exception raised. |
| System | 4. Where inconsistency exists between the HI Service and local PAS stored IHI type (on Check IHI Use Case) | 4.1 System | The local system has the ability to identify contrasting **retrieved** IHI number from HI Service to PAS **stored** IHI number and will flag the record for manual resolution.<br>(IHI number may vary in type or status – a hierarchy of number types and statuses will be built into systems to cater for automatic resolution, but exceptions to this process will need to be handled manually). |
| | | 4.2 System | Where a record is flagged as containing a conflicting IHI number, no IHI patient output data is produced until resolution and certainty of correct IHI allocation is achieved.<br>(Patient output data to be created without IHI). |
| | | 4.3 Ext | Where a record flagged for resolution (4.1) has been resolved during admission, patient identification outputs should be updated with correct IHI information. (e.g. recreation of wristbands/labels, etc). |
| Ext | 5. Identified errors/mismatches or duplicate records in matching. | 5.1 Ext | Back office function exists to merge and de-merge whole or parts of patient records, within the broader context of patient records management. |
| Ext | 6. TDS information accuracy not maintained (Medicare or DVA number accuracy) | 6.1 System | Local system allows for accurate capture (scan preferred) and display of Trusted Data Source information e.g. Medicare & DVA numbers. |
| | | 6.2 System | Use of the OVP/Eclipse service to validate Medicare number and personal details. |
| | | 6.3 System | There should be no automated change to Medicare data captured apart from acceptable Medicare validations. |
| Ext | 7. Medicare fraud scenario in which all the information is correct but the patient is not the person referred to on the Medicare card. | 7.1 System | No control currently available. |
| | | 7.2 Ext | Future use of an Evidence of Identity process to identify patient (possibly relevant to PCEHR usage scenario). |

| | | | |
|---|---|---|---|
| Ext | 8. Patient may not have a Verified IHI, or wish to have it used. | 8.1 System | Where no match is found an **Unverified IHI** may be created ONLY where other criteria are met:<br>o Patient is not a resident of Australia, and hence doesn't qualify for a Medicare card.<br>o Patient requests anonymity.<br>o Newborn registration [5](local policy may be required to activate or disable this function)<br>Local System will flag alternate criteria met or patient request for Unverified. |
| | | 8.2 System | Patient may have a 'regular' Unverified IHI that they use. Search HI Service using information provided by patient. |
| | | 8.3 System | The system has the ability to link an Unverified IHI to a Verified IHI upon resolution by HI Service. |
| Ext | 9. Patient demographic details not obtainable at time of registration. | 9.1 System | Where no match is found/possible, a **Provisional IHI** may be created ONLY when patient demographic detail is not obtainable (i.e. patient is unconscious and no carer/responsible other is available to provide details).[6] |
| | | 9.2 System | The system flags the requirement to user to resolve the provisional IHI (through subsequent local capture of demographic details) before 90 days expiry. |
| | | 9.3 Ext/Org | The user follows best practice in updating the local patient demographic details and seeking a permanent IHI for the patient (ie a Verified or Unverified IHI). |
| System | 10. Multiple local record matches found to IHI request.<br>Multiple PAS records exist with the same IHI | 10.1 System | IHI matches to multiple records within the local system are flagged and no allocation of IHI is made automatically. |
| | | 10.2 System | The local system supports notification to all users of identified potential duplicate patient record that duplicates exist until resolution is achieved. |
| | | 10.3 Ext | Back office function exists to manually resolve identified duplicate records with potential same IHI. |
| | | 10.4 Ext | Back office function exists to merge or de-merge whole or parts of patient records |
| System | 11. Maintenance of IHI changes (the IHI can change characteristics without HI Service users being notified) | 11.1 System | Local system supports regular automated checking and updating of IHI type and status according to definable parameters. |
| | | 11.2 System | Local system automated checking and updating of IHI stored data (on presentation, referral or routine processing) will resolve IHI status changes according to the specified hierarchy of type and status. |
| | | 11.3 System | Local system will retain historical data of IHI changes in type and status. All IHI patient data to be searchable. |
| | | 11.4 System | The system produces reports which can be locally configured to assist manual maintenance of IHI |

[5] Note IHI Workshop attendees preference to NOT use Unverified IHI for Newborn registrations

[6] Note IHI Workshop attendees preference to NOT use Provisional IHIs.

| | | | |
|---|---|---|---|
| | | | data. |
| Ext | 12. Inappropriate application / use of the IHI through lack of user knowledge. | 12.1 Ext | Ensure all staff responsible for acquiring, maintaining and using the IHI are appropriately trained, and are aware of their responsibilities under the various Acts. |
| | | 12.2 Org | Updated Organisation policies and procedures to reflect best practice and compliance requirements for handling IHI. |
| | | 12.3 Org | Comprehensive business change management support to ensure best practice adoption and use of the IHI. |
| | | 12.4 System | System to control and guide user behaviour where possible, eg warn the user before they perform a potentially questionable activity. |
| | | 12.5 Org | Adoption of IHI best practice and compliance requirements in health service Accreditation standards. |

## 5.2 Hazard 002: Inability to identify patient by IHI in clinical care setting

<table>
<tr><td colspan="4">HAZARD: H002 Inability to identify patient by IHI in clinical care setting.<br>(Includes NEHTA Release 1 Review Hazard H020 and H030)</td></tr>
<tr><td colspan="2">Hazard Context<br>Relates to the whole or part of the HI Service and local system, in the end to end IHI search and retrieval.<br>Applies to all channels through which the IHI may be supplied.<br>Applies to use and exchange of the IHI between local and external systems.</td><td colspan="2">Severity: Moderate to Major</td></tr>
<tr><td colspan="2">Initial Likelihood: Probable</td><td colspan="2">Residual Likelihood: Probable</td></tr>
<tr><td colspan="2">Initial risk class: Medium where used in conjunction with URN. High where used singularly.</td><td colspan="2">Residual risk class: Medium where used in conjunction with URN. High where used singularly.</td></tr>
<tr><td colspan="4">Potential Outcome:<br>1. Patient may not be able to be reliably identified by the IHI (alone) in a clinical setting<br>a. User may associate the patient with the wrong record/procedure.<br>2. Value error:<br>a. Clinician may perform treatment on the wrong patient.<br>b. User may not be able to contact a patient when it is urgent to do so; eg<br>i. Adverse or unexpected test results<br>ii. Changes to planned treatment or pre-admission instructions<br>iii. Changes to drug regimens<br>c. Written communications with the patient such as appointment letters may be delivered to wrong address, wrong patient.<br>d. Users may be supplied inadequate or incorrect output from decision support algorithms that utilise demographic data, eg Age, gender.</td></tr>
<tr><td colspan="4">Assumptions:<br>1. The local system has the ability to allocate an IHI to a patient.<br>2. The local system has the ability to produce outputs identifying a patient by IHI.<br>3. The local system has the ability to update IHI output identification in a timely manner according to HI Service changes to IHI.</td></tr>
<tr><td colspan="2">Causes</td><td colspan="2">Controls</td></tr>
<tr><td>System</td><td>1. Inaccurate or missing display of IHI against patient details</td><td>1.1 System</td><td>Local system will display IHI on all patient identification screens in addition to local URN (patient Banner to include IHI type and status).<br>This requirement will exist for an agreed transition period until the presence of Verified IHIs, or appropriate Unverified IHI is ubiquitous and stable.</td></tr>
<tr><td></td><td></td><td>1.2 System</td><td>Local system will supply IHI to all patient identification outputs. (eg wristbands, patient labels, letters, referral docs, discharge docs, order docs, reports, etc).</td></tr>
<tr><td></td><td></td><td>1.3 System</td><td>Local system will provide capability of output of IHI as bar coded, electronic message format, and/or print media.</td></tr>
<tr><td></td><td></td><td>1.4 Ext</td><td>The user will identify the patient IHI as soon as possible upon registration to ensure use on all</td></tr>
</table>

| | | | |
|---|---|---|---|
| | | | patient identification outputs. (see exception Hazard 001 -item 4.2). |
| | | 1.5 Ext | The User will never rely solely on the IHI for patient identification in a clinical setting. |
| System | 2. Inaccurate or missing IHI in exchange of patient data to/from other systems. | 2. 1 System | The local system will perform an automated 'check' on the IHI type and status when receiving or sending an IHI from /to 'external' systems (outside own network).<br>Matching patient demographic data, used to validate the IHI, will also be checked.<br>*This requirement represents recommended best practice but may be relaxed when exchanging IHI information with a (formally accredited) trusted partner, or when the IHI has been checked recently.* |
| | | 2.2 System | Local system will send only a Verified (active) IHI or an appropriate active Unverified (active) IHI on Referral or Discharge information. Provisional IHI may only be used in specific circumstances (see Hazard 001 –item 9).<br>*This action is intended to create the circumstances for trusting data exchange. This requirement will exist for an agreed transition period until the presence of Verified IHIs, or justifiable Unverified IHI is ubiquitous and stable and the IHI can replace the URN.* |
| | | 2.3 Ext | In the event of a missing (or altered status) Verified or Unverified (active) IHI for Referral or Discharge the IHI field should remain blank.<br>*This action is intended to create the circumstances for trusting data exchange. This requirement will exist for an agreed transition period until the presence of IHIs is ubiquitous and stable..*<br>*Note potential mandatory requirement for the IHI on e-Referrals and Discharge Summaries.* |
| | | 2.4 System/Ext | In the event of the use of a Provisional IHI in referral, the receiving health service is expected to return a Referral Update message with accurate IHI when patient details are determined, and sending health service should update patient details appropriately.( see Hazard 001 – items 9.2 & 9.3). |
| | | 2.5 System | Local systems will comply with HI Service Compliance, Conformance and Assessment requirements and be able to indicate compliance on exchange of IHI data to other electronic systems. |
| | | 2.6 System | Local system will be able to 'acknowledge' Trusted data sources and will automatically process the received IHI. |
| | | 2.7 System/Ext | Local systems will be able to "recognise" untrusted data sources and will NOT automatically process a received IHI. Local systems will perform a check of the IHI and the user will perform manual alignment of data prior to acceptance. |
| | | 2.8 Org | Healthcare services' Quality Assurance systems will ensure use only of applications complying with CCA requirements. |

| | | | |
|---|---|---|---|
| | | | *This requirement will be applicable after a period of transition to be defined in the CCA process.* |
| | | 2.9 Org | Healthcare services will ensure best practice standards are trained and adhered to in the use of current IHI for patient identification in all exchanges with external systems. |
| Ext | 3. Inappropriate application / use of the IHI through lack of user knowledge. | 3.1 Ext | Ensure all staff responsible for acquiring, maintaining and using the IHI are appropriately trained, and are aware of their responsibilities under the various Acts. |
| | | 3.2 Org | Updated Organisation policies and procedures to reflect best practice and compliance requirements for handling IHI. |
| | | 3.3 Org | Comprehensive business change management support to ensure best practice adoption and use of the IHI. |
| | | 3.4 System | System to control and guide user behaviour where possible, eg warn the user before they perform a potentially questionable activity. |
| | | 3.5 Org | Adoption of IHI best practice and compliance requirements in health service Accreditation standards. |

## 5.3 Hazard 003: Privacy of patient information is breached

<table>
<tr><td colspan="4">HAZARD: H003 Privacy of patient information is breached.</td></tr>
<tr><td colspan="2">Hazard Context<br>Relates to the whole or part of the HI Service and the local system, for end to end IHI search and retrieval.<br>Applies to all channels through which the IHI is supplied.<br>Applies to use and exchange of the IHI between local and external systems.</td><td colspan="2">Severity: Minor</td></tr>
<tr><td colspan="2">Initial Likelihood: Remote</td><td colspan="2">Residual Likelihood: Remote</td></tr>
<tr><td colspan="2">Initial risk class: Very Low</td><td colspan="2">Residual risk class: Very Low</td></tr>
<tr><td colspan="4">Potential Outcome:<br>1. Patient information, including the IHI, is inappropriately revealed to a third party.<br>2. Organisation and individual face legal penalties.</td></tr>
<tr><td colspan="4">Assumptions:<br>1. The Organisation (health service) has policies and procedures which support privacy and security.<br>2. The Organisation has instituted, and enforces, security access to the HI Service and related data according to the legislative and regulatory requirements.<br>3. The local system has role based access controls, to a suitable level of granularity.<br>4. The local system includes full audit trails of all actions against a patient record.</td></tr>
<tr><td colspan="2">Causes</td><td colspan="2">Controls</td></tr>
<tr><td>Ext</td><td>1.Privacy breaches</td><td>1.1 Org</td><td>RO and OMR roles and responsibilities allocated and maintained within the organisation. HI User access appropriately recorded and maintained.</td></tr>
<tr><td></td><td></td><td>1.2 Ext/Org</td><td>Best practice guide, education / training and the Compliance regime with regulations exist to control user behaviour and guide Organisation policies and procedures.</td></tr>
<tr><td></td><td></td><td>1.3 System</td><td>Role based access exists to patient registration and all HI functions.</td></tr>
<tr><td></td><td></td><td>1.4 System</td><td>Audit logs maintained of all IHI related actions including user id, time, date and action undertaken against a patient record – including viewing.</td></tr>
<tr><td></td><td>2. Security breaches</td><td>2.1 System, Ext</td><td>All messages incorporating the IHI transmitted over the Internet to be signed and encrypted.</td></tr>
<tr><td></td><td></td><td>2.2 System</td><td>User access to the PAS and hence the HI Service to be managed by role based access.</td></tr>
<tr><td></td><td></td><td>2.3</td><td>Logs and audit trails to be retained in accordance</td></tr>
</table>

| | | | |
|---|---|---|---|
| | | System | with legislation. |
| | | 2.4 Org/Ext | Organisation policies and procedures ensure user access restricted by role. |
| | | 2.5 Org/Ext | All hospital staff without an HPI-I who have access to internal systems storing the IHI to be identified as authorised organisational users, and notification provided to the HI Service operator. |
| | | 2.6 Ext | Education and training of PAS users and other health service staff with respect to their security responsibilities. |
| | | 2.7 Ext | Periodic internal (and external) security and access audits, to ensure privacy and information security compliance is maintained (may be included in the SAF). |
| | | 2.8 Ext | Adoption of the mandatory elements of the NEHTA Security and Access Framework, including protection of IT systems and data. |

## 5.4 Hazard 004: Whole of part of the system is unavailable or access is inappropriately denied

<table>
<tr><td colspan="4">HAZARD: H004 Whole or part of the system is unavailable or access is inappropriately denied.<br>(Includes NEHTA Release 1 Review Hazards H010 and H120)</td></tr>
<tr><td colspan="2">Hazard Context<br>Relates to the whole of part of the HI Service and local system, for end to end IHI search and retrieval.<br>Applies to all channels through which the IHI is supplied.</td><td colspan="2">Severity: Minor</td></tr>
<tr><td colspan="2">Initial Likelihood: Probable</td><td colspan="2">Residual Likelihood: Probable</td></tr>
<tr><td colspan="2">Initial risk class: Low</td><td colspan="2">Residual risk class: Low</td></tr>
<tr><td colspan="4">Potential Outcome:<br>1. Patient may not be able to be identified by IHI in clinical setting<br>a. System may not be able to associate an IHI with the patient.<br>b. System may not be able to validate or check an incoming IHI from external source ( referral/order/discharge)<br>c. System may not be able to validate or check an IHI on an outgoing message (referral, order, discharge summary).<br>d. End user may associate the wrong patient with the wrong record/procedure.<br>2. Value error:<br>a. End user may perform treatment on the wrong patient.<br>b. End user may not be able to contact a patient when it is urgent to do so; eg<br>i. Adverse or unexpected test results<br>ii. Changes to planned treatment or pre-admission instructions<br>iii. Changes to drug regimens<br>c. Written communications with a patient, such as appointment letters, may be delivered to wrong address, wrong patient.<br>d. End users may be supplied inadequate or incorrect output from decision support algorithms that utilise demographic data, eg age, gender.</td></tr>
<tr><td colspan="4">Assumptions:<br>1. The HI Service performs according to established SLAs and notifies organisational users of scheduled outages.<br>2. The Organisation has Continuity of Business policies and procedures which support system failures/downtime.<br>3. The Organisation has instituted security access to HI Service according to the legislative and regulatory requirements.<br>4. The organisation has maintained Security and Access compliance according to HI Service requirements.<br>5. RO and OMO roles are defined within the organisation and staff are committed to meeting the demands of these roles.<br>6. The local system has role based access controls.</td></tr>
<tr><td colspan="2">Causes</td><td colspan="2">Controls</td></tr>
<tr><td>System</td><td>1.Periods of non-availability of the HI Service</td><td>1.1 System</td><td>All request to be queued by the local system and forwarded to the HI Service when it becomes available. Users to be notified.</td></tr>
<tr><td></td><td></td><td>1.2 Ext</td><td>Revert to manual processes on extended non-availability of the HI Service. Business Continuity plans are enacted.<br>For HI Service access (IHI data) it may be possible to use an alternate channel, e.g. the</td></tr>
</table>

| | | | |
|---|---|---|---|
| | | | Provider Portal. |
| | | 1.3 System | HI Service to ensure appropriate provision is made to identify and prevent Internet based attacks upon the service, e.g. a Denial of Service attack. |
| System | 2. Periods of poor performance of the HI Service or other system components. | 2.1 Ext/Org | Ensure users can operate independently of remote system response times. Business Continuity plans are enacted in worst case scenarios. |
| | | 2.2. System | Use asynchronous messaging techniques for management of the IHI. |
| | | 2.3 Ext/Org | Report apparent missed HI Service SLAs to governance body. |
| | | 2.4 System | HI Service and local environment to ensure appropriate provision is made to identify and prevent Internet based attacks upon the service, eg a Denial of Service attack. |
| System | 3. Local System non-availability | 3.1 Ext | Revert to manual processes on extended non-availability of the local system. Business Continuity plans are enacted. |
| | | 3.2 Ext | Report outage and apparent missed SLAs and/or vendor system performance issues. |
| System | 4. Vendor system inaccurately allocates IHI. | 4.1 System | Vendor application carries current Medicare Australia and CCA authorisation. |
| | | 4.2 Org | Comprehensive testing prior to implementation will help to ensure accuracy. |
| | | 4.3 Org | Any potential conflict or question about the allocation of an IHI will be brought to the user's attention, and the user will make the final decision. |
| | | 4.4 System | HI Service and local network environment to have appropriate provision to ensure that Internet based attacks upon the service are identified and prevented, eg a SQL injection attack. |
| System | 5. Access denied to HI Service | 5.1 Org | RO and OMR roles and responsibilities allocated and maintained within the organisation. HI User access appropriately recorded and maintained. |
| | | 5.2 System | HI Service to ensure appropriate provision is made to identify and prevent Internet based attacks upon the service, eg a Denial of Service attack. |
| | | 5.3 Org | Organisational PKI certificates, used for HI Service access, to be maintained in good order at all times. |

# 6. Appendix: NEHTA Sentry Clinical Safety Risk Assessment Criteria:

## 6.1 Clinical Risk Severity Categories

**Table 1** below defines categories for the Severity of consequences associated with Clinical Hazards. These categories reflect single incidents, which may affect individual patients or several patients at once. Due to the nature of HI Releases as additional advisory systems, there is the potential for a Clinical Hazard to be detected and for harm to be prevented (primarily by the Clinician) and this is reflected in the Clinical Hazard categorisation.

**Table 1 Severity Categories**

| Severity Category | Definition |
|---|---|
| Catastrophic | The clinical Hazard results in permanent harm and/or death to a patient.<br>This category will also apply to a Clinical Hazard that causes many occurrences of Major Severity. |
| Major | The Clinical Hazard creates a situation that is inherently and immediately threatening to a patient's life. Harm is unlikely to be prevented by Clinician.<br>This category will also apply to a Clinical Hazard that causes many occurrences of Moderate Severity. |
| Moderate | The Clinical Hazard presents a serious and imminent Clinical Safety risk to a patient by allowing a life-threatening situation to develop. Harm may be prevented by Clinician.<br>This category will also apply to a Clinical Hazard that causes any occurrences of Minor Severity. |
| Minor | The Clinical Hazard presents a significant risk to a patient, though not one that is immediately or necessarily life threatening. Harm is likely to be prevented by Clinician.<br>This category will also apply to a Clinical Hazard that causes many occurrences of Minimal Severity. |
| Minimal | The Clinical Hazard presents a latent risk, which may impact on the quality of the patient care if ignored. |
| Benign | The Clinical Hazard has no foreseeable impact on patient care. |

## 6.2 Likelihood Categories

**Table 2** below defines categories for the Likelihood of the occurrence of Clinical Hazards.

**Table 2 Likelihood Categories**

| Likelihood Category | Definition |
|---|---|
| Frequent | Likely to be continually experienced |
| Probable | Likely to occur regularly |
| Occasional | Likely to occur several times |
| Remote | Likely to occur some times |

| | |
|---|---|
| Improbable | Unlikely, but may exceptionally occur |
| Incredible | Extremely unlikely that the event will occur at all |

## 6.3 Clinical Risk Classification Matrix

**Table 3** below combines the Severity and Likelihood categories to provide a classification of Clinical Risk. These classifications have been grouped into Residential Risk Acceptance Categories, as defined in Table 4.

**Table 3 Clinical Risk Classification Matrix**

| **Clinical Risk Classification** | | | | | | |
|---|---|---|---|---|---|---|
| **Likelihood** | **Severity** | **Minimal** | **Minor** | **Moderate** | **Major** | **Catastrophic** |
| Frequent | | **Low** | **Low** | **Medium** | **High** | **High** |
| Probable | | **Low** | **Low** | **Medium** | **High** | **High** |
| Occasional | | **Very Low** | **Low** | **Medium** | **High** | **High** |
| Remote | | **Very Low** | **Very Low** | **Low** | **Medium** | **High** |
| Improbable | | **Very Low** | **Very Low** | **Low** | **Medium** | **High** |
| Incredible | | **Very Low** | **Very Low** | **Very Low** | **Low** | **Medium** |

# 7. Glossary

| Term | Description |
|---|---|
| After Presentation | A term used to describe when the patient is present in the health service, i.e. on or after presentation. This enables health staff to validate Medicare and demographic details directly with the patient. |
| B2B | Business to business, a term used to describe the web service based functions implemented in the HI Service. |
| BDM | Birth, Deaths & Marriages |
| Before Presentation | A term to describe the period prior to a patient presenting at the health service, in which a referral may be received, an entry created on a waiting list, and an appointment made, with the appropriate notifications. The patient is not readily available to confirm their Medicare number or demographic details, though this can be done via telephone, email, letter, etc. |
| CCA | A NEHTA group responsible for Compliance, Conformance and Accreditation. |
| CMS | Community Management System |
| DOB | Date of Birth |
| DH | Victorian Department of Health |
| DVA | Commonwealth Department of Veterans' Affairs |
| ED | Emergency Department |
| EOI | Evidence of Identity |
| Episode | A single admission to a health service for a particular condition or conditions, or<br>A period of care for a particular condition, often covered by a single referral (supporting multiple admissions or attendances). |
| FoI | Freedom of Information |
| HI | Healthcare Identifier Service |
| HIM | Health Information Manager, a specialist in the management of health information, including patient records. |
| HPI-I | Healthcare Provider Identifier – Individual. A unique number to be assigned to every person involved in healthcare service delivery. |
| HPI-O | Healthcare Provider Identifier – Organisation, a unique number that will be assigned to all organisations involved in healthcare service delivery |
| HPOS | Health Professional Online Services, a portal provided by Medicare Australia. |
| HSD | The Victorian Human Services Directory |
| Health*SMART* | The Victorian Department of Health Health*SMART* program is responsible for managing processes to select, configure and implement applications to reflect state wide requirements (state wide footprint) into participating healthcare agencies. Additionally, the Health*SMART* program is responsible for establishing and managing the shared ICT infrastructure that is required to support these applications and agencies use of them. |
| ID | Identity or identifier |
| IHI | The Individual Healthcare Identifier, which Medicare Australia allocated to every active Medicare enrolee, on the 1st July 2010. |
| IHI Record Status | There are three record statuses of IHIs:<br>• Verified<br>• Unverified |

| Term | Description |
|---|---|
| | • Provisional |
| IHI Status | There are five IHI Statuses of IHIs:<br>• Active<br>• Deceased<br>• Retired<br>• Expired<br>• Resolved |
| IP | Inpatient |
| IRN | Individual Reference Number, used on the Medicare card to identify each individual recorded on the card. |
| MSO | Medicare Service Operator |
| NASH | The National Authentication Service for Health (NASH) project being delivered through NEHTA will deliver the first nationwide security service to enable healthcare organisations and individuals to exchange e-health information. |
| NEHTA | National eHealth Transition Authority |
| NOI | Notice of Integration, Medicare Australia's formal validation process to be used by systems wishing to connect to the HI Service. |
| NOK | Next of Kin |
| OP | Outpatient |
| OPD | Outpatient Department |
| PAS | Patient Administration System – a system used for the recording of patient and provider information to support management and coordination of service provision. Within Health*SMART* this functionality is provided by either a consolidated Patient and Client Management System (P&CMS) through the iSOFT iPM application, or Community Management System through the Trak application for stand-alone metropolitan community health centres. |
| Referral | A referral is defined within the Australian standard as "the communication with the intention of initiating patient/client care transfer, from the provider making the referral (the originator) to the provider expected to act on the referral (the destination)."<br>In the context of this document a referral is used as a representative health service request or report, and the reader should consider Orders (pathology, diagnostic imaging, etc), discharge summaries, etc. |
| SLA | Service Level Agreement, a contractual agreement that defines the required levels of services required from a vendor/supplier. For example, a common SLA may define that the system be available 98% of the time, and 100% of the time during working hours. |
| TDS | Trusted Data Source, which refers to Medicare Australia and the Commonwealth Department of Veterans' Affairs in the initial allocation of IHIs within the HI Service.<br>In the context of the IHI Pre-Implementation project, an organisation participating in e-health messaging, who has met the compliance/accreditation criteria, is also referred to as a trusted data source. |
| UC | Use case, part of the UML standard used to document tasks or business process steps. |
| UML | Unified Modelling Language. An international standard for documenting the design of an application. |
| URN | Unit Record Number |