



## **HI Service Security and Access Framework**

Version 1.0 – 13/11/09

PUBLIC

**National E-Health Transition Authority Ltd**

Level 25

56 Pitt Street

Sydney, NSW, 2000

Australia.

[www.nehta.gov.au](http://www.nehta.gov.au)

**Disclaimer**

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

**Document Control**

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

**Trademarks**

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

**Copyright © 2009, NEHTA.**

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



<b>File Name</b>	HI Security and Access Framework
<b>Original Author(s)</b>	Yvette Lejins, HI Service Security Manager
<b>Creation Date</b>	11/11/2008
<b>Last Saved</b>	13/11/2009

## Document Sign-off

---

<i>Name</i>	<i>Role</i>	<i>Signature</i>	<i>Date</i>
	HI Service Program Manager		

---

## Revision History

---

<b>Version</b>	<b>Revision Date</b>	<b>Author(s)</b>	<b>Revision Notes</b>
<b>0.0</b>		Yvette Lejins	Version 0 finalised – Ready for Medicare Australia’s comment and input
<b>0.1</b>	02/02/2009	Yvette Lejins	Minor updates to reflect Medicare Australia’s input.
<b>0.2</b>	10/09/2009	Yvette Lejins	Updated to reflect current HI Service position.  Updates from David Nissen, Chantal Crowe, Rebecca Burdick and Robyn Cooke
<b>0.3</b>	02/10/2009	Yvette Lejins	Updated after feedback from DOHA
<b>1.0</b>	13/11/2009	Yvette Lejins	Document rename from ‘HI Service Information Security Framework’ to ‘HI Service Security and Access Framework’  Document FINAL

---

## Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>2</b>
1.1	Background to Security Context.....	2
1.2	The Importance of Security.....	2
1.3	Scope.....	3
1.4	Out of Scope .....	3
1.5	Security and Privacy – The Dependencies .....	4
<b>2</b>	<b>Risk Assessments and Audits.....</b>	<b>5</b>
2.1	Initial Threat and Risk Assessment (TRA).....	5
2.1.1	Statement of Applicability .....	5
2.2	End User Access - Threat and Risk Assessment.....	5
2.3	Development and Functional Testing .....	6
2.4	Penetration and Vulnerability Testing .....	7
2.5	Completion Validation Assessment .....	7
<b>3</b>	<b>Technical Security Controls.....</b>	<b>8</b>
3.1	The HI Service Operator’s Controls .....	8
3.1.1	Defence Signals Directorate (DSD).....	8
3.2	Audit Logs, Monitoring and Anomaly Detection .....	8
3.2.1	Capturing of Logs.....	9
3.2.2	Individuals accessing their IHI audit log.....	9
3.2.3	Response to Security Breaches .....	9
3.3	Access Controls .....	9
3.3.1	Role-Based Access Controls.....	10
3.3.2	Roles, Authorisation and Authentication .....	10
3.4	Encryption .....	12
3.5	Security Testing.....	12
<b>4</b>	<b>Non-Technical Controls.....</b>	<b>14</b>
4.1	Policy and Process.....	14
4.2	Awareness .....	14
4.3	Participation Agreements .....	15
4.4	Legislation .....	15
<b>5</b>	<b>Ongoing Governance.....</b>	<b>17</b>
<b>6</b>	<b>References.....</b>	<b>18</b>

This page has been left blank intentionally.

# Executive Summary

Information Security has always been a primary consideration in the design and development of the Health Identifiers (HI) Service. It is recognised that strong information security will contribute to the success of the HI Service by appropriately safeguarding the personal information required to operate the Service. The Security and Access Framework that NEHTA has developed outlines the principles, policies, processes and tools that are to be used to achieve this aim.

NEHTA recognises that a multi-layered approach is needed to safeguard the HI Service, and accordingly the Security and Access Framework incorporates both technical and non-technical controls. These will include:

- Smartcards and PKI certificates to facilitate the accurate identification and authentication of individuals accessing the HI Service;
- Robust audit trails, and proactive monitoring of access to the HI Service by both internal and external users;
- Role-based access control policies;
- Rigorous security testing, to be conducted both prior to and after commencement of operation of the HI Service;
- Ensuring users of the HI Service are adequately trained, through provision of educational programs and other training mechanisms; and
- Obliging healthcare provider organisations to execute Participation Agreements (underpinned by legislation) in order to participate in the HI Service.

The Security and Access Framework will ensure that the privacy, confidentiality, integrity and availability of information within the HI Service are not compromised. This document outlines the components of the framework, and describes the controls that will be in place to appropriately safeguard the HI Service. NEHTA believes that security needs to be operationally realistic for stakeholders, meaning that it must support, rather than hinder, the HI Service. As such, security has been designed to be 'fit for purpose', and to address policy objectives. Appropriate security controls are therefore being implemented in order to meet the HI Service objectives.

NEHTA has adopted a risk management approach that aligns and complies with international best practice information security management standard, ISO/IEC 27001. It also recognises Medicare Australia as the initial HI Service Operator. The HI Service Operator is obligated to comply with the Australian Government's Protective Services Manual (PSM) and 'ACSI-33'. This approach will ensure that the HI Service is appropriately protected whilst meeting the needs of the healthcare community. This framework is complementary to and is a subset of the Security and Access Framework (SAF) being developed by NEHTA for the whole of e-health.

---

# 1 Introduction

## 1.1 Background to Security Context

A primary focus in the development of the Health Identifiers (HI) Service is the security of information.

The objective of this Security and Access Framework is to:

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

NEHTA has ensured that information security is more than technical controls. Layers of technical, physical, administrative, people and process controls will be deployed to ensure that information is appropriately safeguarded. This Security and Access Framework is important as it provides a roadmap for implementation, evaluation and improvement of information security services. It provides an overall sense of direction and guiding principles for action.

NEHTA has adopted a risk management approach aligned to international information security and risk management standards for best practice (namely AS/NZS ISO/IEC 27001). Where appropriate, NEHTA has also aligned its approach to the requirements of the Australian Government Protective Security Manual and Australian Government Information and Communications Technology Security Manual (ACSI 33:2008).

The intent of this framework is to support the aims and objectives of the HI Service balanced with the requirement to protect and secure information. This framework assumes that the reader has a good understanding of the concepts and design of the HI Service. This framework is complementary to and is a subset of the Security and Access Framework (SAF) being developed by NEHTA for the whole of e-health. The SAF will provide relevant guidance for all Australian organisations and systems electronically collecting, securely exchanging, and storing health information.

## 1.2 The Importance of Security

The implementation of a Security and Access Framework is important to the HI Service as it provides assurance that information is being appropriately protected. Security of information is particularly important in the provision of health services as it contributes to ensuring that privacy obligations are met. The HI Service has approached security through a risk management approach, whereby threats and risks have been analysed, and appropriate security controls selected and introduced to manage risks to an acceptable level.

Security plays a key role in the HI Service as it allows for the preservation of the following:

- **Privacy** – this refers to ‘information privacy’, which is focused on the collection and handling of personal information, including health

information. Information privacy has twin objectives: protecting the privacy of an individual's personal information while promoting the authorised and appropriate handling of that information.

- **Confidentiality** – ensuring that information held in the HI Service is not made available or disclosed to unauthorised individuals, entities or processes. Confidentiality is not limited to personal information.
- **Integrity** – safeguarding the accuracy and completeness of information.
- **Availability** – ensuring that the HI Service and information held therein is accessible and usable upon demand by an authorised entity or user.

The confidentiality of health information can often be subjective, rather than objective. Ultimately only an individual can make a proper determination of the sensitivity of their information. For example: a vulnerable individual who is trying to escape an abusive partner may consider their address details much more confidential than their medical history.

A wide range of strategies have been applied to enhance the privacy and confidentiality of the information handled as part of the HI Service, and to address and mitigate risks in these areas. This system has been designed to provide a unique and persistent identifier for individuals and organisations; it is not an 'identification' service. It is important to distinguish between these two concepts.

## 1.3 Scope

The HI Service may be defined as the business services and associated rules, policies and processes that constitute the Individual Healthcare Identifier (IHI) and Healthcare Provider Identifier (HPI) services.

The scope of this Security and Access Framework encompasses the following:

- Persons or systems interacting with the HI Service;
- The personnel responsible for the design, implementation, ongoing operation and governance of the HI Service;
- The information collected for, and handled by the HI Service;
- Associated paper and electronic documents;
- The software and applications to be used to operate the HI Service;
- Participation Agreements for acceptable use of the HI Service;
- Evidence of Identity (EOI) information collected for key participants;
- The physical assets and locations where the HI Service is to be delivered; and
- The image and reputation of the HI Service;
- Healthcare individuals.

## 1.4 Out of Scope

For the purposes of this Security and Access Framework, the following are considered 'out of scope':

- The subsequent storage, use and onward transmission of information provided to authenticated and authorised users of the HI Service;
- Management of policies and processes that are the responsibility of third parties and any data in their custody

---

Whilst the Individual Electronic Healthcare Record (IEHR) is 'out of scope' for this HI Service Security and Access Framework, it is always a consideration in design, forward thinking and planning. The HI Service is intended to provide one of the foundation building blocks to facilitate the IEHR.

## **1.5 Security and Privacy – The Dependencies**

The terms "security" and "privacy" are not mutually exclusive, nor are they interchangeable. Security and privacy are closely related concepts; however, there are important differences that need to be understood in order to ensure the HI Service is designed to address both. Security must be implemented to ensure privacy. Conversely, privacy law requires that appropriate security is in place whenever personal information is collected and/or handled. Throughout this framework, privacy refers to information privacy or data protection.

Security covers the technology, policies, processes, steps and tools that are used to maintain confidentiality and privacy. Security is the mechanism that will protect the privacy of personal information and health information. This includes the ability to control access to IHI and HPI information, as well as to safeguard IHI and HPI information from unauthorised disclosure, alteration, loss or destruction.

Information privacy legislation is concerned with the responsible collection and handling of personal information - the right of each individual to have some control over the way in which his or her personal information is collected, used and in what manner it is disclosed. It addresses the entire information life cycle, from collection to destruction, and contains a security principle. Security offers the ability to be confident that those decisions are respected and implemented.

Australia's current privacy landscape is complicated and fragmented. Differing privacy schemes apply to health and e-health infrastructure across the Commonwealth, States and Territories. NEHTA currently works with a common set of privacy principles based on the Information Privacy Principles (IPPs) found in the Privacy Act 1988 (Cth). Further, NEHTA has committed to six privacy tenets that guide its work. For additional information on these privacy tenets, refer to *NEHTA's Privacy Blueprint - Unique Healthcare Identifiers*, released December 2006. Legislative reform is underway as part of the work with the National Health Information Regulatory Framework (NHIRF) Working Group to ensure that Australia has a uniform approach to health information privacy legislation. This will overcome many of the issues caused by a fragmented privacy patchwork. (For further information, see Section 4.4 Legislation, or 6. References)

## 2 Risk Assessments and Audits

Risk identification and management is fundamental to the development of a secure HI Service. A risk management approach has been adopted to identify and quantify HI Service risks. Risks must be understood and appropriate steps must be taken to manage these risks. Risk assessments are important because they are an objective evaluation of potential loss and probability of occurrence.

NEHTA is committed to ensuring that the HI Service is aligned and complies with best practice information security management. To be most effective, information security must be integrated into the System Development Life Cycle (SDLC) from inception. Recognising this, NEHTA conducted an initial Threat and Risk Assessment (TRA) – allowing for early identification and mitigation of vulnerabilities. This early identification of security risks has ensured that additional costs of 'add on' security will be avoided, and effective security controls can be built into the design of the HI Service from the outset.

Over time the threat landscape of the HI Service has and will change and evolve. For this reason, risk assessments and audits at key times throughout the design and build of the service are imperative to understand the risk profile. At various milestones throughout the project, NEHTA has planned risk assessments and audits. Audits provide confidence and assurance that risks are appropriately addressed. The HI Service Operator is contractually required to comply with reasonable outcomes from these audits and assessments.

### 2.1 Initial Threat and Risk Assessment (TRA)

In February 2008, an independent Threat and Risk Assessment of the HI Service was completed by Computer Services Corporation (CSC). The assessment was conducted prior to the development of any conceptual or detailed technical architecture for the HI Service.

The purpose of the assessment was to identify potential risks and threats and to allow mitigating strategies to be fed into the design phase.

The HI Service Operator is building mitigation strategies and options to be integrated into its design and build of the HI Service, with the effect of reducing or nullifying the risks identified.

#### 2.1.1 Statement of Applicability

A further output from the Threat and Risk Assessment is the Statement of Applicability. The Statement of Applicability is a set of controls (selected from the information security standard ISO/IEC 27001) that are relevant and applicable to the HI Service. Each of these controls is designed to assist in mitigating relevant risks to acceptable levels. It is based on risk treatment processes, legal or regulatory requirements, contractual obligations and NEHTA's requirements for Information Security. Prior to the HI Service 'going live' the Statement of Applicability will be used as a compliance assessment to ensure that NEHTA's security requirements have been satisfied.

### 2.2 End User Access - Threat and Risk Assessment

---

The potential user base of the HI Service is diverse. Once fully operational, it is expected that upwards of 500,000 Healthcare Provider Individuals (HPI-I's) will participate in the HI Service. In addition, large numbers of HI Service Users<sup>1</sup> will require access to the service to facilitate the delivery of healthcare services. The end user security assessment has allowed NEHTA to ascertain security vulnerabilities, risks and threats that an end user presents at a 'typical' healthcare setting, and gain an understanding of current security practices and awareness levels.

In order to obtain a cross section of the healthcare community in a diverse array of healthcare settings, a range of private and public health organisations were visited. Numerous staff members were interviewed, and practices and processes reviewed and evaluated.

The End User Security Reviews assessed the following:

- A large city public hospital
- A children's public hospital
- A private pathology and radiology service
- A private hospital
- A rural public hospital

The End User Security Reviews clearly found that there are instances in which particular users may share user credentials (whether they be passwords or tokens) to facilitate their obligation to patient care. In situations such as a hectic Emergency Department or a large onsite trauma situation, the adherence to business processes which promote unique identification and authentication of users of the HI Service may not be practically possible.

The security controls and awareness levels found in these assessments have been varied. These findings are invaluable as they provide a solid 'real world' understanding of security in a variety of healthcare settings. They will give primary input into appropriate baseline security controls that will need to be included in Participation Agreements, and security considerations that will need to be included in the design of third party health systems (such as Patient Administration Systems).

These reviews have ultimately assisted in designing and developing effective and usable controls for the HI Service.

## **2.3 Development and Functional Testing**

Numerous test case specifications have been developed and are to be executed in the pre-production environment to ensure that the HI Service system is being developed and built to a secure state. Testing is occurring to validate the system's conformance to security requirements and to identify potential security vulnerabilities within the system. Any vulnerability identified during testing can therefore be addressed prior to deployment of the HI Service.

---

<sup>1</sup> A HI Service user – an individual employed by a Healthcare Provider Organisation to support the day to day functional requirements of the HI Service. For example, a Medical Receptionist or an Admissions Clerk at a hospital.

## 2.4 Penetration and Vulnerability Testing

Penetration and Vulnerability Testing<sup>2</sup> will occur prior in both pre-production and production environments. This will provide a level of assurance and validation that the Service is adequately protected from external threats. Assurance testing and validation of the environment housing the HI Service will be undertaken prior to 'go live'.

Independent Penetration Testing will occur collaboratively between NEHTA and Medicare Australia. NEHTA will have full transparency of findings. Once the HI Service is operational, external testing will become a regular undertaking to assist in mitigating the risk profile of the Service. Penetration Testing will serve as a tool to ensure continuous improvement.

## 2.5 Completion Validation Assessment

It is commonly found that risks identified during the initial or design assessment phases may not have been fully mitigated to an acceptable level due to a number of reasons, including but not limited to technical limitations, costs, time constraints and so on. Given the residual risks and threats, a key reason for conducting the risk assessment during this phase is to ensure that the authorities and custodians of the service are fully aware of any residual risks (including those not sufficiently mitigated) in relation to the Service.

---

<sup>2</sup> Penetration and Vulnerability Testing will evaluate the security of the HI Service System by simulating attacks from malicious sources. The process involves a pro-active analysis of the system for any potential vulnerabilities that may result from inadequate system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures.

---

# 3 Technical Security Controls

Multiple technical security controls will play an integral part in securing the HI Service. It must be recognised that technical controls will not solely address security, and that they must integrate and work in parallel with administrative, people and process controls to provide a holistic security environment. Technical controls will be preventative, detective and corrective.

## 3.1 The HI Service Operator's Controls

NEHTA has core security requirements that must be met and delivered by the HI Service Operator (initially Medicare Australia). In the design, build and operation of the HI Service, the initial HI Service Operator will be leveraging off existing security controls that are in place. NEHTA will be conducting independent risk assessments to determine a security risk profile. The HI Service Operator will be required to comply with the reasonable outcomes of these audits and assessments.

As an Australian Government Agency, the initial HI Service Operator is required to comply with the minimum security requirements of the Australian Government ICT Security Manual ("ACSI-33"). Whilst NEHTA does not enforce or prescribe to ACSI-33's requirements, the HI Service Operator is obligated to ensure that it adheres to them. ACSI-33 is a prescriptive set of security requirements designed to enable government agencies to achieve an assured level of IT Security.

The HI Service Operator is able to leverage their existing infrastructure and network security controls to provide intrusion detection for the HI Service.

### 3.1.1 Defence Signals Directorate (DSD)

DSD is an Australian Government Agency, under the umbrella of the Department of Defence. DSD provides a range of information security services to ensure that Australian Government Agencies can protect sensitive electronic information systems so they are not susceptible to unauthorised access, compromise or disruption. Directed by the Protective Services Manual (PSM), issued by the Attorney General's Department, the DSD has developed ACSI-33 as a security requirements mandate.

NEHTA is seeking advice from DSD to ensure that the HI Service will be future and technology proofed from any changes to the ACSI-33. NEHTA will seek to ensure that legislation will support the service to operate without being impacted by any future changes to ACSI-33. The legislation must be technology neutral to allow the Service to adapt to changing risks and threat environments.

## 3.2 Audit Logs, Monitoring and Anomaly Detection

Audit trails will play an integral role in ensuring that the HI Service is appropriately accessed and used. Audit and monitoring capabilities will ensure that any inappropriate use can be detected and responded to. The design of the Service will allow for all activities to be logged and audited. Users will be advised through Participation Agreements, training and login banners that all access and activity will be audited and monitored.

### **3.2.1 Capturing of Logs**

There will be two (2) distinct types of logs. Those captured and stored by the HI Service Operator, and those mandated via the Participation Agreements that will be required to be captured by healthcare provider organisations.

The HI Service Operator audit logs will play a key role in providing the ability to determine the level and rate of compliance with Participation Agreements, in addition to providing quantifiable levels of assurance.

### **3.2.2 Individuals accessing their IHI audit log**

All healthcare individuals will be able to review the logs of access to their IHI records, enabling them to identify and report potential unwarranted or inappropriate access. The HI Service will store detailed audit logs of all user access to an HI record. These audit logs will form the trails that will identify anyone who may inappropriately access the data. The information captured in the logs will provide details of who created, activated, verified, accessed, updated or deactivated an IHI record and when this was undertaken.

Individuals will be able to access the audit log associated to their IHI record at a Medicare Shopfront, online (via the HPOS system) or over the phone. It should be noted that for the audit log details captured in the instance of an HI User accessing the record (from within a healthcare provider organisation), that it will record access from the organisation. However, the actual individual that has accessed the record will need to be identified by that organisation. The same will be true for any bulk updates extracted from the HI Service by an HPI-O authorised process.

### **3.2.3 Response to Security Breaches**

A security breach can be defined as any attempted or successful, unauthorised access, use, disclosure, modification or destruction of the HI Service and the data it contains. A security breach will not only be limited to inappropriate access to personal or sensitive information but also to the database as a whole.

If it is suspected that the HI Service is being used inappropriately, the issue will be escalated for response and resolution. Potential misuse will firstly be referred to the healthcare provider organisation where the suspected breach has occurred. Compliance with Participation Agreements will require that all users accessing the HI Service via their organisation will be uniquely identifiable within their HPI-O setting and audit logs capturing their activities will be maintained. This will provide a chain of evidence for forensic purposes to facilitate investigation.

Security incident response guidelines will be developed, and HI Service Participation Agreements will articulate standard terms and conditions, some of which will be enforceable. There will be clear mechanisms in place to identify the types, numbers and costs of breaches so that their impact can be measured and quantified. Ultimately the HI Service Operator is responsible for investigating suspected security breaches.

## **3.3 Access Controls**

The objective of access controls is to ensure only legitimate access to information. Mechanisms to control access by users of the HI Service will be a core element of user identification.

---

The control of access by users is based on two factors for authentication, which the HI Service design will incorporate:

- Something you **have** (e.g. ID card, smartcard, certificate (soft token), or mobile)
- Something you **know** (e.g. a password, passphrase, PIN Number)

Access to the HI Service will be controlled through implementation of the following mechanisms, policies and controls;

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

It is recognised that it is best practice security to uniquely identify all users directly accessing the HI Service, as well as being a mandatory compliance issue with ACSI-33.

### **3.3.1 Role-Based Access Controls**

Role-based Access Control is a method deployed to regulate job functions and permissions based on specific roles in a system. All access granted to the HI Service will be permitted through the assignment of specific user roles. This will ensure that the HI Service adequately protects the privacy of healthcare individual and provider individual information.

The creation and assignment of particular roles to distinct classes of users ensures that users can access only the specific information of the HI Service that is necessary to perform their day-to-day functions. Role-based Access Control also makes revocation and updating of access rights more flexible. User profiles can be modified in a timely manner, allowing for more centralised control over changes in policy.

Each user of the Service will have a specific HI Service role based on their business requirements and responsibilities. Users' access to the Service will be determined by their role. Role-based access will be strictly on a 'need to know' approach, and clearly outlined in Participation Agreements. This will allow for fine granularity of access to certain components of the Service to be tightly controlled, and will assist in ensuring that minimal rights are allocated to each user.

### **3.3.2 Roles, Authorisation and Authentication**

#### **3.3.2.1 Healthcare Individuals**

Upon request and after being appropriately identified, individuals can obtain a user-id and password to access an online portal to view their own IHI information. Individuals will further be able to view the audit log associated with their IHI through this online service.

Individuals may also contact the HI Service Operator via phone, facsimile, mail or via one of its shop fronts to obtain this information.

### 3.3.2.2 Healthcare Provider Individuals

Healthcare provider individuals (possessors of HPI-Is) will be identified through their professional registration process or other approved processes. Access will be either by identifying themselves to an HI Service officer by phone, person, fax or mail or by using a PKI certificate to electronically access the HI Service. Certificates will be available upon request using the National Authentication Service for Health (NASH).

As an individual healthcare provider they will be able to access their own provider information. However, they must provide evidence, either to a body acting as a Trusted Data Source to the HI Service, or directly to the HI Service Operator, that they are employed by a healthcare provider organisation, before being permitted to access the core HI Service. The core HI Service includes IHIs and associated healthcare individual information, and the healthcare provider directory services (which include the details of healthcare provider organisations and consenting healthcare provider individuals).

### 3.3.2.3 Organisational Public Officer (OPO) and Organisational Maintenance Roles (OMR)

Organisation Public Officers (OPOs) will be responsible for healthcare provider organisations' participation in the HI Service. That is, OPOs will be responsible for initially registering an organisation to participate, or for withdrawing an organisation's participation.

Organisational Maintenance Roles (OMRs) will be responsible for maintaining the organisation's information in the HI Service, and for managing access to the HI Service by the workers employed at the organisation or its subsidiaries (networked organisations).

All OPOs will be required to undergo a full Evidence of Identity (EOI) check as part of the process of initially registering the healthcare provider organisation, or if the designated OPO is to change. The EOI information provided by an OPO will allow them to later authenticate themselves to a HI Service Officer. OPOs can also use a PKI certificate to access the Service<sup>3</sup>.

Individuals performing the OMR role will be identified and registered by the OPO, or their delegate (i.e. an officer who has previously been registered to perform the organisation maintenance role). Registration of OMRs will require certain demographic information to be recorded. This enables them to authenticate themselves when calling a HI Service Officer and for their access to the Service to be logged. OMRs can use a PKI certificate associated with their organisational role to electronically access the HI Service.

### 3.3.2.4 HI Users and Authorised Processes

A healthcare provider organisation may identify and authorise certain employees who are not healthcare provider individuals to access the HI Service. The healthcare provider organisation may achieve this by instituting an authorised process (on a server or personal computer), and through an organisational PKI certificate. To minimise the privacy impact whilst maximising confidence in authorisation, these organisational certificates will only identify the individual within the context of their organisation and not the wider community.

---

<sup>3</sup> If, at a future stage, it is determined that OPOs require access to an online service

---

HI Users from clinical HPI-Os will have restricted access<sup>4</sup> to IHI data and the healthcare provider individual provider directory service.

Organisations will be responsible for monitoring and restricting access to the HI Service by their workers and they will be obliged to restrict access to their PKI certificates through the introduction and enforcement of policy, procedures and local system administration controls. Healthcare provider organisations will also be required to allocate a unique identifier to each of its nominated HI Users, and will be obliged to maintain system logs recording all instances of access by its employees to the HI Service. These baseline security standards will be communicated through the Participation Agreements.

The above described security elements concerning access by HI Users to the HI Service have been developed from the perspective that each organisation will be responsible, and in the best position, to correctly identify its workers.

### **3.3.2.5 Trusted Data Sources**

Trusted Data Sources will be authoritative external sources of initial and updated data to the HI Service. The data supplied by Trusted Data Sources must meet NEHTA's formatting requirements, and must be of the highest standard of quality and accuracy.

### **3.3.2.6 HI Service Officer and Other Service Operator Staff**

The HI Service Officer's primary role will be to enable HI Service participants (whether they be individual consumers, healthcare provider individuals or representatives of healthcare provider organisations) to access the HI Service by non-electronic (manual) means<sup>5</sup>.

The HI Service Operator's existing processes to identify its staff and control internal access will be leveraged. These processes include staff undergoing both EOI checks and security clearances.

Staff will only be able to access HI Service from authorised locations using internally issued credentials. The HI Service Operator will determine the type of credentials to be used based on the risks.

While the HI Service Operator has full access to the HI Service data:

- All access will be logged; and
- Any changes or access will be traceable to a request from a user of the service or an authorised (regular or ad-hoc) procedure required to maintain the system.

## **3.4 Encryption**

All electronic communication channels of the HI Service will be protected with encryption techniques. This will assist in ensuring that any HI information in transit will remain confidential and safeguarded from any interception attacks.

## **3.5 Security Testing**

Security testing will be performed to verify that the HI Service protects data and maintains functionality and policy settings as intended. Each area of confidentiality, integrity, authentication, authorisation and non-repudiation

---

<sup>4</sup> What information is accessible is yet to be determined

<sup>5</sup> Other staff employed by the HI Service Operator will be tasked with undertaking system maintenance.

will be tested to ensure full security of the Service. These areas will be covered during the phases of PKI testing, user acceptance testing and penetration testing. Security test scenarios will be integrated into all testing undertaken prior to go-live. It is also expected that testing will continue in production to ensure that any improvements and changes are secure.

The approach to testing will ensure that deterministic behaviour is followed throughout the entire system. Penetration security tests will be planned and executed at the service level and not just when a fully integrated system has been delivered. The web services testing will be done to ensure resistance from common attack methods and rejection at a desired range.

---

# 4 Non-Technical Controls

## 4.1 Policy and Process

The business rules and operational policies that have been developed collaboratively by NEHTA and the initial HI Service Operator ensure that access to the data held in the HI Service is appropriately constrained, and that the information is protected from unauthorised access, use or disclosure.

These policies include (but are not limited to) the following:-

- The decision to associate only a limited set of data with an IHI;
- Generally limiting access to the HI Service to users employed in the healthcare sector (whether as clinicians or support workers), or by the HI Service Operator;
- Restricting the possible results to a search to;-
  - a single exact match; or
  - an error messagedepending on the accuracy and/or completeness of the search entered;
- Restricting the data returned in response to an IHI search to an individual's name, date of birth, IHI and IHI status;
- Leveraging the HI Service Operator's existing robust evidence of identity processes;
- Ensuring that any vulnerable individual can be allocated an IHI associated with pseudonymous data (but linked to his or her verified identity);
- Ensuring that each transaction in connection with an IHI, HPI-I or HPI-O is recorded in a system log;
- Ensuring that healthcare individuals and healthcare provider individuals are able to easily access the audit log associated with their IHI or HPI-I;
- Ensuring the regular and complete resolution of replica and duplicate IHI, HPI-I and HPI-O records; and
- Ensuring that IHIs or HPI-Is in relation to deceased individuals are effectively retired.

## 4.2 Awareness

Whilst technology controls will be required, the users of any information technology service are often the weakest link in a security chain, in that it is far more difficult to exercise control over the behaviour of users. Prior to being given access, users will be given guidance on appropriate usage and participation in the HI Service. It is envisaged that this guidance will be in the form of a process and procedures manual, and through the provision of online training modules. The manual and training modules will canvass the business processes to be followed by users, in addition to outlining their obligations under the relevant privacy scheme.

At the point of authentication to the HI Service, all users will be required to respond to a login banner before access to the system will be granted.

### 4.3 Participation Agreements

Participation Agreements will be a necessary requirement for healthcare provider organisations to actively participate in HI Service. A Participation Agreement will be executed as part of an overall registration process. The Participation Agreement will form an integral part of the security framework, providing the foundation for best practice security. Participation Agreements will include enforceable terms and conditions, underpinned by legislation, and will address a broad range of fundamental areas of responsibility.

In order to access the HI Service, healthcare provider organisations will be required to address the following areas in relation to security:

- Comply to minimum baseline security requirements (including areas such as account creation, unique identification of users in interfacing systems to the HI Service, password management strategies, firewalls, anti-malware, audit trails);
- Participating organisations will be required to maintain any computer and other ancillary electronic equipment to meet a minimum standard of being technologically adequate for the purposes of the IHI and HPI services;
- Have mechanisms in place to manage risks and liabilities;
- Have policy and procedures that address information security and privacy; and
- Provide education and training to all HI Service authorised users so that they are aware of their responsibilities.

Participation Agreements will need to be in place for healthcare provider organisations. From a security perspective, larger organisations will be required to implement or demonstrate more rigorous and thorough baseline security. If non-compliance with Participation Agreements is identified an organisation may have their access revoked. It should be noted that NEHTA's security requirements must strike a balancing act between prescriptive requirements that will ensure participants' compliance, and requirements flexible enough to encourage participation and to move with the changes to technology.

Individual and organisational responsibilities and accountabilities will be communicated to HI Service users at various access points to the HI Service. These regular warnings will be complementary to the provisions of the Participation Agreements.

A continuous improvement model will also be used as a way of ensuring that essential processes are managed to a level that will be effective for the HI Service. A process improvement approach will provide the HI Service with the essential elements of effective processes. This improvement process will be very useful in Participation Agreements as it will assist in integrating traditionally separate organisational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes.

### 4.4 Legislation

In 2006, the Council of Australian Governments (COAG) agreed upon a national approach to the development of individual and healthcare provider identifiers, within the broader context of e-health and with the ultimate aim of improving patient safety and the efficiency of health care. To achieve this objective, in July 2007 the Australian Health Ministers Council (AHMC) agreed

---

to the development of a National Health Information Regulatory Framework (NHIRF) to support e-health initiatives.

The NHIRF Working Group is undertaking the development of legislation enabling the Healthcare Identifiers (HI) Service ("the enabling legislation"). The enabling legislation will regulate the management and operation of the HI Service and the assignment of individual and healthcare provider identifiers. It will also place appropriate parameters around the collection, use and disclosure of personal information that the HI Service will hold, within the context of existing privacy legislation and frameworks.

In July 2009, the Australian Health Ministers' Advisory Council issued a consultation paper, *Healthcare identifiers and privacy: Discussion paper on proposals for legislative support*, seeking comment on legislative proposals to support the establishment and implementation of national healthcare identifiers and enhanced arrangements for the privacy of health information. The consultation paper foreshadowed that the identifiers legislation will, broadly, achieve the following:-

- Authorise the use of individual and provider identifiers for the purposes of healthcare identification, health information management and communication;
- Authorise the HI Service Operator to operate the HI Service;
- Set out the processes for participating in the HI Service; and
- Define the processes for complaints and enquiries.

The consultation paper states that information security arrangements will be underpinned by a combination of existing Commonwealth, state and territory privacy and health regulation, as well as additional provisions in the healthcare identifiers enabling legislation where there is an identified need for additional safeguards.

## 5 Ongoing Governance

Once the HI Service is operational, the performance standards and compliance metrics will be established specifically in relation to information security. This will underpin this Information Security Framework to ensure that information security is appropriately managed.

There will be a clear demarcation of security roles and responsibilities. The HI Service Operator will be responsible for ensuring the integrity and availability of the HI Service data and infrastructure, and will ensure that the confidentiality of any data held by the Service is maintained. The HI Service Operator will be responsible for the day-to-day administration of the HI Service, and will undertake ongoing testing and assessments of security.

Once operational, the focal points of security will change. Security auditing, monitoring and reporting will become the focus for security management. To achieve these security measures, the HI Service Operator will be required to provide regular reports to the governance authority against predefined metrics. The HI Service Operator will assist with external security audits, and assist the governance authority to investigate security related incidents.

Ongoing governance may extend to multiple authorities. For example, the Privacy Commissioner may have a role in auditing and investigating privacy and security breaches, and the Ministerial Council, as a strategic overseer, may have a role in terms of requiring the HI Service Operator to provide regular reports on security. The governance authority will oversee and make fundamental arrangements for the continual improvement of the HI Service. It will dictate and benchmark minimum security standards.

---

## 6 References

- Information security management standard, ISO/IEC 27001
- Australian Government Protective Security Manual and Australian Government Information and Communications Technology Security Manual (ACSI 33:2008).
- National Privacy Principles (NPPs) found in the Privacy Act 1988 (Cth).
- *NEHTA's Privacy Blueprint - Unique Healthcare Identifiers.*
- National Health Information Regulatory Framework (NHIRF) Working Group
- *NEHTA's Threat and Risk Assessment* of the HI Service completed by Computer Services Corporation (CSC)
- Australian Government ICT Security Manual ("ACSI-33")

[END]