



**Privacy Blueprint - Unique
Healthcare Identifiers**

**Individual Healthcare Identifier and
Healthcare Provider Identifier**

Version 1.0 – 18 December 2006

For Comment

National E-Health Transition Authority Ltd

Level 25

56 Pitt Street

Sydney, NSW, 2000

Australia.

www.nehta.gov.au

Disclaimer

NEHTA makes the information and other material ("Information") in this document available in good faith. 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 Web site and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is of the latest revision.

Copyright © 2006, 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.

Table of contents

Executive Summary	i
1 Introduction	1
1.1 Purpose	1
1.2 Intended audience	1
1.3 NEHTA and privacy	2
1.4 Progress to date	3
1.4.1 Preliminary Privacy Impact Assessment	3
1.4.2 Integrating privacy into design	4
2 Unique Healthcare Identifiers	5
2.1 Overview	5
2.1.1 Current problems in healthcare identification	5
2.1.2 What is being proposed?	6
2.1.3 The benefits of improved identification	6
2.2 Unique Healthcare Identification Service	7
2.2.1 How will the Service be managed?	7
2.2.2 Who participates in the Service?	8
2.3 Lifecycle of unique healthcare identifiers	9
2.3.1 Collection and creation	9
2.3.2 What personal information will be collected for the IHI and HPI-I? ..	10
2.3.3 What personal information will be collected for the HPI-O?	10
2.3.4 Restrictions on use	11
2.3.5 Use and disclosure	11
2.3.6 Linkages between the IHI and the HPI	12
2.3.7 Up-to-date and accurate data	13
2.3.8 Information flows	13
3 Mapping information flows against privacy principles	14
3.1 Introduction	14
3.2 Mapping exercise	15
3.3 Does the UHI Service involve the collection of personal or health information? ..	15
3.4 Collection	16
3.5 Use and disclosure	16
3.6 Data quality	17
3.7 Data security	17
3.8 Openness	18
3.9 Access and correction	18
3.10 Identifiers	19
3.11 Anonymity	19
3.12 Transborder data flows	19
3.13 Governance	20
4 Key issues	22
4.1 Overview	22
4.2 Consent and notification	23
4.3 Who is authorised to access UHI records?	25
4.3.1 Individual access	25
4.3.2 Provider access	25
4.3.3 Non-healthcare provider access	25
4.4 UHI data fields	27
4.5 Audit functionality and policy	28
4.6 Masking and pseudonym functionality	29
4.7 A framework for dealing with authorised representatives	30

4.8	Secondary uses	32
5	Consultation and next steps	34
5.1	Privacy Blueprint	34
5.2	Consultation	34
5.2.1	Clinician and Consumer Discussion Forum	34
5.2.2	Privacy Roundtable.....	34
5.2.3	Jurisdictional and Project Reference Groups	35
5.3	Full Privacy Impact Assessment	35
5.4	Privacy Tools.....	36
5.5	Summary of next steps	37
	Appendix A: Glossary	38
	Appendix B: Privacy Materials	40
B.1	Privacy Checklist	40
B.1.1	Checklist for Privacy Compliance	40
B.1.2	Additional Privacy-Positive Measures.....	41
B.2	Privacy Impact Analysis.....	41
B.3	Privacy Management	42

Executive Summary

The Privacy Blueprint on NEHTA's Unique Healthcare Identifiers (UHI) program establishes a clear framework to consider privacy issues raised by the development and implementation of national healthcare identification infrastructure. It summarises NEHTA's progress to date in managing privacy issues arising from the UHI Service and sets out an action plan for future work.

Electronic health (e-health) information systems that securely and efficiently exchange data can significantly improve the manner in which important clinical and administrative information is communicated between healthcare professionals. An essential component for secure and reliable communications within the healthcare sector is the ability to accurately identify both healthcare providers and healthcare consumers. Unique healthcare identifiers will help ensure that the right information relating to the right individual can be delivered to the right healthcare provider.

The benefits from improved healthcare information practices are considered in this Privacy Blueprint, along with the need for introduction of unique identifiers for healthcare providers and individuals.

The UHI Service consists of two discrete identifiers – a Healthcare Provider Identifier for healthcare providers and healthcare organisations, and an Individual Healthcare Identifier for individual consumers. This Privacy Blueprint outlines the nature and function of the UHI Service, and identifies key participants in the proposed system as well as the personal and health information involved and how it will be used.

A number of key privacy issues are examined in detail, such as consent and notice, access, audit and secondary uses. These areas require further work and consultation, before the UHI Service can undergo a full privacy impact assessment (PIA) and progress to the implementation stage. Feedback obtained through the UHI Privacy Blueprint's consultation process will help settle outstanding privacy policy issues.

An outline of consultation activities and next steps sets out NEHTA's ongoing privacy work program. These activities include for example, a Privacy Roundtable workshop in November 2006 and a full PIA of the UHI Service in 2007.

Finally, privacy management approaches from sources such as the Office of the Federal Privacy Commissioner are set out in Appendix B. These will be used during preparation for a full PIA of the UHI Service.

Importantly, this Privacy Blueprint is largely based on a generic Australian privacy analysis, reflecting the fact that it was not known whether the UHI Organisation responsible for managing the UHI Service would be a public or a private sector organisation. This is critical, as the nature of the organisation determines whether it is subject to the public or private sector provisions of the *Privacy Act 1988* (Cth). While the public and private sector privacy principles are similar, there are key differences in coverage and the way they are structured that will impact on the privacy analysis undertaken.

Once the nature of the UHI Organisation is confirmed, NEHTA's ongoing privacy work, including preparation for a full PIA, will immediately commence mapping UHI design and architecture requirements against the most relevant privacy principles, that is, either the Information Privacy Principles or the National Privacy Principles.

This page has been left blank intentionally.

1 Introduction

1.1 Purpose

A Privacy Blueprint sets out a systematic framework to consider the privacy issues raised by the collection and use of personal (including health) information involved with NEHTA's initiatives.

A Privacy Blueprint aims to identify the full range of privacy risks that apply to a specific NEHTA initiative so that corresponding action steps may be undertaken to address those risks.

Adopting a Privacy Blueprint process ensures that NEHTA proactively considers its privacy compliance position and promotes a coordinated approach to privacy management. A Privacy Blueprint will be prepared for NEHTA's Shared Electronic Health Record Design (Shared EHR) initiative as well as the Unique Healthcare Identifier (UHI) program.

A clear description of an initiative is essential for a robust assessment of privacy risks. A Privacy Blueprint, however, cannot describe detailed aspects of project design. The design process is dynamic, responding to issues that arise from privacy analysis such as recommendations contained in this Blueprint, or new requirements that arise for an initiative. Likewise, a Privacy Blueprint is a living document, subject to further change and refinement.

In order to put management strategies into practice, a Privacy Blueprint describes a plan of action for addressing privacy. This includes a series of steps:

- Issue and risk identification
- Strategies for privacy management;
- Ongoing privacy impact assessments (PIAs) and
- Development of ongoing privacy tools.

A Privacy Blueprint ensures that privacy is properly integrated into NEHTA's design and implementation work as well as providing a critical consultation mechanism.

1.2 Intended audience

This Privacy Blueprint is intended for a general audience and will be of interest to the health sector, industry groups, government, privacy advocates, health consumers and their representatives. In-depth knowledge of privacy law is not required, although a useful primer on the topic is found in the *NEHTA's Approach to Privacy*, which presents a summary of Australia's privacy environment.

This Privacy Blueprint is being publicly released for comment and will also be used as a tool for consultation activities as discussed in Chapter 5. Feedback is particularly sought in relation to the key questions and issues identified in boxed sections in Chapter 4. Individuals or organisations may provide feedback to NEHTA via the privacyblueprint@nehta.gov.au email address or by mail to:

Privacy Blueprint Feedback
UHI Service
NEHTA
Level 25, 56 Pitt Street
Sydney NSW 2000

In the absence of a clear indication that a submission is intended to be confidential, **NEHTA will treat the feedback received as non-confidential**

and may refer to or quote from the content of submissions in subsequent publications.

The closing date for submissions is **Wednesday 28 February 2007**.

1.3 NEHTA and privacy

From the outset, NEHTA has recognised that privacy is an issue of great concern to Australians – particularly in the health sector. NEHTA outlined a broad overview of its position on privacy in the publication *NEHTA's Approach to Privacy*.

NEHTA must manage the risks of a particularly complex legislative and regulatory environment whilst also recognising that privacy perceptions of the Australian community (individual consumers and healthcare providers) play a major role in ensuring the success of e-health systems. Confidence and trust build upon a strong privacy foundation. NEHTA's initiatives will only be successful if they meet community expectations regarding privacy.

NEHTA's Approach to Privacy identifies six privacy tenets relating to the collection and handling of personal information that are intended to guide NEHTA's work program.

The tenets represent NEHTA's commitment to developing the national foundations for the electronic exchange of information for healthcare purposes in a way that ensures the privacy of this information is appropriately protected.

1.	<p><i>Commitment to Privacy</i></p> <p>A commitment to privacy is the starting point for NEHTA initiatives involving the collection and handling of personal/health information. NEHTA recognises that:</p> <ul style="list-style-type: none"> • privacy is an integral component of a secure and interoperable e-health environment; • it must be embedded in the design process; • it must comply with all legal requirements; and • it should promote privacy-positive approaches.
2.	<p><i>Health-Specific Focus</i></p> <p>All NEHTA initiatives involving the collection and handling of personal/health information are focused on obtaining measurable benefits for individual health consumers and health providers as well as ensuring the improvement of public health outcomes.</p>
3.	<p><i>Individual Participation</i></p> <p>All relevant NEHTA initiatives will seek to maximise the degree of control individuals may exercise over the collection and handling of their personal/health information.</p>
4.	<p><i>Clarity & Transparency of Purpose</i></p> <p>All NEHTA initiatives involving the collection and handling of personal/health information will seek to articulate their intended purposes transparently and clearly.</p>
5.	<p><i>Data Quality, Audit & Security</i></p> <p>All NEHTA initiatives involving the collection and handling of personal/health information will ensure that robust data quality, audit and security measures are put in place.</p>
6.	<p><i>Governance Arrangements</i></p> <p>All NEHTA initiatives involving the collection and handling of personal/health information will be subject to appropriate governance arrangements designed to ensure, amongst other things, that these privacy tenets are supported and progressed into, and beyond, the implementation phase of each initiative.</p>

NEHTA takes a holistic approach to privacy which avoids focusing solely on the application of privacy legislation. Instead, NEHTA seeks to apply a range of strategies to address and mitigate risks or enhance privacy. Accordingly areas of analysis include:

- **Law:** (including legislation or contract) which underpins governance and accountability, defines the extent of the functions of an initiative, proscribing purposes that fall outside those functions, deals with uncertainty of responsibility and allocates appropriate penalties.
- **Technology:** an element of fundamental system design. Technology facilitates finely tuned filtering of who can and cannot have access to personal information and ensures data security such as authenticating those seeking to access a record.
- **Governance and Accountability:** provides policy settings and promotes confidence in an initiative by assuring the community that the operation of the system is subject to stringent oversight, reporting and audit mechanisms and is transparent.
- **Safety net processes:** provides simple mechanisms for rectifying or remedying breaches when the system or persons within the system have acted improperly.
- **Culture:** that is consumer focused and creates a justifiable sense of community trust.

1.4 Progress to date

1.4.1 Preliminary Privacy Impact Assessment

NEHTA commenced internal privacy analysis of the UHI Service in September 2005, which provided an initial assessment of personal information flows likely to occur. Early privacy analysis identified areas in the broad concepts of UHI design where key compliance issues would arise.

Following this initial internal privacy analysis, a preliminary privacy impact assessment (PIA) process was undertaken. A PIA is a process where proposed initiatives, particularly those involving new technologies, are tested against their potential impact on privacy.

An external consultant was engaged in early 2006 to conduct a preliminary PIA for NEHTA's UHI initiative. The preliminary PIA assessed likely privacy compliance risks and tested the degree to which NEHTA's high level concepts for the UHI Service were capable of being privacy compliant.

Overall, the consultancy found that while there was considerable work to be done to manage privacy effectively in the UHI Service, no privacy risks or impacts were identified that could not be managed or mitigated successfully.

Risks identified by NEHTA's own internal privacy analysis as well as NEHTA's proposed management strategies were confirmed by the preliminary PIA process and have informed the development of the UHI Privacy Blueprint as well as the UHI design process over the last six months.

Following the UHI Privacy Blueprint consultation process, NEHTA will then commission an independent, full PIA. This will include a further stage of public consultation and the results of the full PIA will be released publicly. The full PIA is discussed further in Chapter 5.

1.4.2 Integrating privacy into design

Close collaboration within NEHTA between the UHI team (primarily responsible for system design and architecture) and the E-Health Policy unit (primarily responsible for privacy compliance and policy) is fundamental to NEHTA's overarching privacy program.

A specialist privacy professional has been embedded within the UHI team. This generates ongoing liaison and debate within NEHTA about the role of privacy and how to balance privacy requirements against broader governmental objectives. This management approach ensures that, wherever possible, the UHI Service's fundamental system design and architecture incorporates privacy as a matter of course, rather than as an afterthought or as an unintended consequence.

It is NEHTA's view that integrating privacy expertise within the UHI design team ensures that privacy issues are assessed earlier rather than later and that privacy is not simply 'bolted on' during implementation.

2 Unique Healthcare Identifiers

2.1 Overview

Over the course of the next several years, NEHTA's work will trigger many changes in how information is communicated within the healthcare sector. NEHTA's work derives from a clear commitment from all Australian governments to reforming outdated communication practices in health.

There is a clear link between avoidable patient deaths and poor communication and record keeping practices within healthcare. Electronic communication has the capacity to allow doctors, nurses and other healthcare professionals to exchange information quickly, reliably and securely.

In February 2006, the Council of Australian Governments (COAG) approved \$98 million in joint funding to NEHTA to deliver two fundamental elements of reliable electronic communication within healthcare: the Individual Healthcare Identifier (IHI) and the Healthcare Provider Identifier (HPI). Together, these initiatives are referred to as the UHI Service.

The next section discusses some of the difficulties associated with current practice and the benefits that can be achieved through improved provider and individual identification, before going on to describe the UHI Service itself. A glossary of key terms relating to the UHI Service (and shortened versions or acronyms) is found in Appendix A.

2.1.1 Current problems in healthcare identification

Australia's healthcare system relies on an ability to uniquely and accurately identify individuals. Healthcare activities constantly involve the collection, exchange and transmission of health information. This is usually in the context of information about a single patient being exchanged between multiple healthcare providers.

It is critical for patient safety and privacy that this information exchange occurs reliably and securely. Electronic communications offers the possibility of this information being directly exchanged between different health software systems, without the need for human intervention. As an example, a hospital could send information about an individual's emergency visit directly to the computer system of that individual's GP, where it could be automatically placed on the individual's file. Such an exchange however relies upon the ability to accurately and reliably identify the relevant individual and healthcare provider.

The problems associated with current identification practices are becoming more prominent as greater emphasis is placed on the need for continuity of healthcare. High population mobility and multiple points of access to the healthcare system mean that an individual's healthcare information will often be stored in a variety of fragmented, unrelated repositories.

In Australia, there is currently no single method of accurately and reliably identifying individuals or providers. Community GP clinics, pharmacies, pathology laboratories, private and public hospitals and so on all have separate and usually different identification methods and supporting systems to identify individuals receiving healthcare.

Similarly, provider information is stored across multiple information directories maintained by various registration bodies, community imaging, pharmacy and pathology services and public and private hospitals. Each of these identification approaches serve different functions and vary in scope and data accuracy.

Outdated record keeping and poor individual and provider identification practices can, where there is error, result in significant consequences. The

practice of identifying individuals by simply using their name, address and date of birth is no longer the safest and most accurate way to handle health information. For example, test results (and therefore medical treatment decisions) may be attributed to the wrong individual, who happens to have a similar name to the actual patient. An individual’s highly sensitive confidential test results could also be sent mistakenly to a doctor who has a similar name to his or her own doctor. Without the ability to uniquely identify individuals and providers, such events can easily occur.

2.1.2 What is being proposed?

NEHTA is proposing a Unique Healthcare Identification Service. This Service will involve the allocation, issuing and maintenance of unique identifiers for individuals (the IHI) and healthcare providers (the HPI).

The proposed IHI and HPI will consist of a random number that complies with International Standards Organisation requirements and Australian standards for healthcare identifiers. Each number will be linked to records containing appropriate identification and demographic data. No clinical information is required or will be held on the record.

Only healthcare providers that possess a HPI can access IHI information for individuals in their care. Use of an IHI by an individual is not a prerequisite for obtaining healthcare.

There will be two types of HPI issued – an HPI for individual healthcare providers (known as the HPI-I) and an HPI for healthcare provider organisations (known as the HPI-O). Collectively, the IHI, HPI-I and HPI-O are known as unique healthcare identifiers, and the records of identification and demographic data attached to those identifiers are known as the **UHI records**.

In addition, a Healthcare Provider Directory will be established to locate other healthcare providers, in order to route communications for referrals and other healthcare communication purposes.

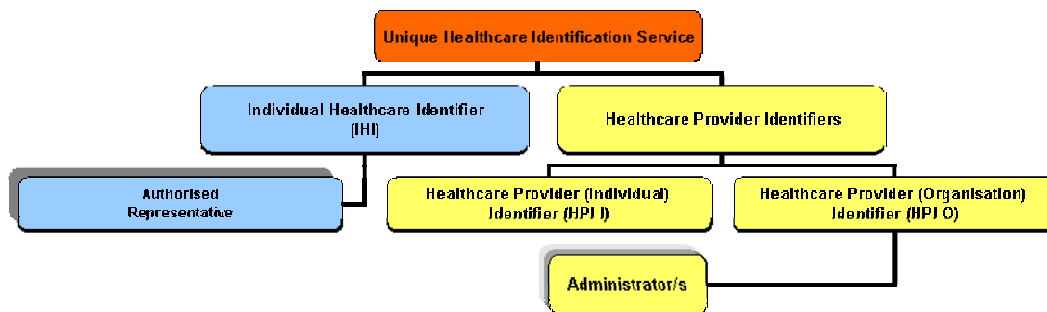


Figure 1: UHI Service span of activity

2.1.3 The benefits of improved identification

The ability to ensure that health information relates to the right individual and is communicated to the right provider is an essential building block for secure and reliable healthcare communication.

The HPI under development by NEHTA establishes the means by which all healthcare providers and organisations in Australia can be accurately and uniquely identified.

The IHI under development by NEHTA establishes the means by which all individuals eligible for healthcare in Australia can be uniquely identified within the healthcare system.

If providers can accurately and confidently identify both other providers and the particular individual they are treating, it ensures that:

- Details of previous care can be quickly related to the current healthcare event; and
- Manual and electronic communications between providers about the one individual are far more reliable.

The IHI will be used primarily by providers to identify individuals. However, an important future benefit of the use of the IHI for individuals is improved portability of their clinical records. The use of the IHI is expected to assist individuals and community providers in aggregating the clinical records of a single individual, at the request of that individual, from a diverse range of previous providers and consulting healthcare services when an individual seeks the services of a new provider.

Another benefit from the establishment of the IHI is the opportunity it creates to decommission a large range of existing individual health consumer index systems maintained by hospitals, individual community healthcare providers, community imaging and laboratory services, pharmacies and jurisdictional health departments. Substantial investment is currently required by all such organisations in order to maintain the integrity of these index systems.

A significant benefit arising from the introduction of a single national Healthcare Provider Directory is the opportunity to decommission the large number of provider directories currently maintained.

With the ability to uniquely identify both individuals and their providers, health information will be able to flow across functional, jurisdictional, administrative and professional boundaries with far greater confidence and reliability. The UHI Service will promote greater integration of healthcare information, preventing organisational and administrative barriers from reducing the quality and safety of healthcare.

2.2 Unique Healthcare Identification Service

2.2.1 How will the Service be managed?

A **Unique Healthcare Identifiers Organisation (UHI Organisation)** will generate unique identifiers for each individual, healthcare provider or healthcare organisation in Australia and collect the identification and demographic information to populate the record from a range of data sources. The UHI Organisation will not collect clinical information.

The COAG funding for the development and implementation of the UHI Service was premised on NEHTA being able to make use of Medicare Australia to establish an initial data set for the IHI, and negotiating with State/Territory registration bodies to obtain data for the HPI.

A key service performed by the UHI Organisation is the disclosure of an individual's IHI and corresponding IHI record to healthcare providers or provider organisations when these are required in the course of providing healthcare to that individual. When the UHI Organisation discloses the IHI and associated IHI record of an individual, the provider is able to correctly and confidently identify the patient, with a unique healthcare identifier that will only ever relate to one particular individual. Disclosure of an individual's details contained in the IHI record, for example, the most up-to-date address to his/her provider ensures the provider can maintain the accuracy and currency of their own records about that patient.

Another key UHI Organisation service is enabling individuals to access and update their own details.

Other UHI Organisation services include:

- Operating an identity and access management regime, which then enables individuals, providers and provider organisations to access the unique healthcare identifiers and records;
- Managing the quality of data held in the records to ensure it is accurate and up to date; and
- Disclosing de-identified data from the records for use, for example, in approved research endeavours.

It is currently unknown whether the UHI Organisation will be a public or private enterprise. NEHTA intends to resolve this issue by early 2007.

2.2.2 Who participates in the Service?

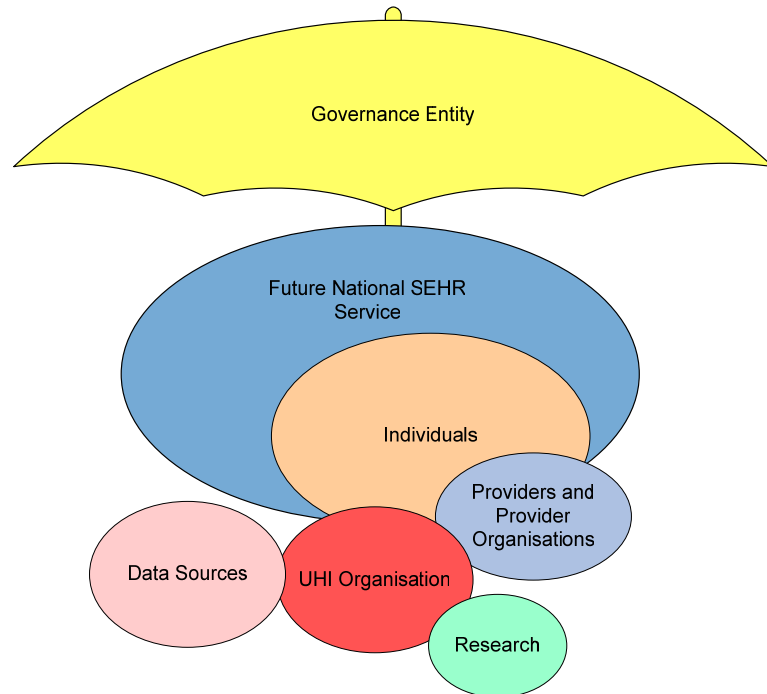


Figure 2: UHI Service participants

Individuals are members of the Australian community seeking healthcare services. Individuals may access their own IHI and accompanying record. Mechanisms will be in place for individuals to update and either directly correct themselves, or request that corrections be made to their own information contained in IHI records. Individuals will be able to view an audit trail of which providers and provider organisations have accessed their IHI and the attached record. Individuals will not have access to HPI records. Use of an IHI is not a prerequisite to obtain healthcare.

Authorised representatives are individuals who have legal authority to act on behalf of someone else. For example, a person may be an authorised representative for another under a guardianship order.

Healthcare Providers (providers) are all the different types of accredited healthcare practitioners that constitute Australia's health sector, for example GPs, pharmacists and nurses. Providers use their own HPI-I to receive their patient's IHI record containing their patient's up-to-date personal information.

Healthcare Provider Organisations (provider organisations) are the various healthcare provider entities that constitute Australia's health sector, for example, a hospital emergency department or a pathology laboratory. Provider organisations are allocated HPI-Os. Employees of a provider organisation who do not provide 'healthcare' (e.g. administrative workers) will

use the HPI-O of the organisation they work for to receive the IHI and corresponding IHI record for individuals receiving healthcare from their organisation.

UHI Organisation is the entity that will operate and manage the UHI Service, that is, the national piece of e-health infrastructure comprising two discrete identifiers – the HPI for providers, and the IHI for individuals. The UHI organisation will establish the two unique healthcare identifiers and manage the ongoing collection and use of personal information associated with each individual or provider's identifier.

Data sources are the various entities and individuals that disclose personal information to the UHI Organisation. Personal information provided by data sources is stored in the IHI, HPI-I or HPI-O record (as appropriate). Data sources are used either as the primary source of data or as a secondary cross-check on data already held in the records. Examples of primary data sources include Medicare Australia and State/Territory registration bodies.

Research bodies may request the disclosure of de-identified data from the UHI Organisation in order to undertake suitably approved research in the public interest.

Governance Entity has accountability for the UHI Organisation. The Governance entity will be responsible for activities such as complaints handling and oversight measures.

Electronic Health Record systems managed by provider organisations will access and receive personal information from the UHI Organisation in order to attribute medical event summaries to the correct individuals. EHR systems are currently already in place at various provider organisations throughout Australia.

Possible future *national* Shared Electronic Health Record (Shared EHR) systems may access and receive personal information from the UHI Organisation in order to manage an individual's Shared EHR. A Shared EHR will allow access to an individual's summary health record from anywhere in Australia. Currently, NEHTA is tasked to develop the design of such a system, for COAG's funding consideration in late 2007.

2.3 Lifecycle of unique healthcare identifiers

2.3.1 Collection and creation

The IHI, HPI-I and HPI-O will be persistent identifiers – only one identifier will ever be allocated to and used by each individual, provider and provider organisation and it will span their lifetime.

Individuals will be allocated an IHI and a corresponding IHI record by the UHI Organisation. It is intended that the UHI Organisation would create the initial IHI data set using personal information currently held by Medicare Australia. Medicare Australia would be required to undertake appropriate consent and notification processes before the IHI can be created, disclosed and used by the UHI Organisation. The UHI Organisation would likewise rely on Medicare Australia's processes for verifying the identity of individuals.

The UHI Organisation will create the HPI-I using personal information currently held by healthcare professional registration bodies (data sources). These data sources will be required to undertake appropriate consent and notification processes before the HPI-I can be created, disclosed and used by the UHI Organisation. The UHI Organisation will rely on these data sources for verification of identity.

The UHI Organisation will create the HPI-O using information provided by provider organisations and accreditation bodies.

The precise arrangements for ongoing collection of information for the IHI, HPI-I and HPI-O have yet to be finalised in the design process. The UHI Organisation will need to undertake different notification and compliance steps for such ongoing collection as opposed to the initial leveraged data.

Chapter 4 discusses issues relating to individuals who may be empowered to act on behalf of another individual due to, for example, reduced decision making capacity.

2.3.2 What personal information will be collected for the IHI and HPI-I?

The IHI and HPI-I records will consist of three parts – a summary record, an identification record and a demographic record.

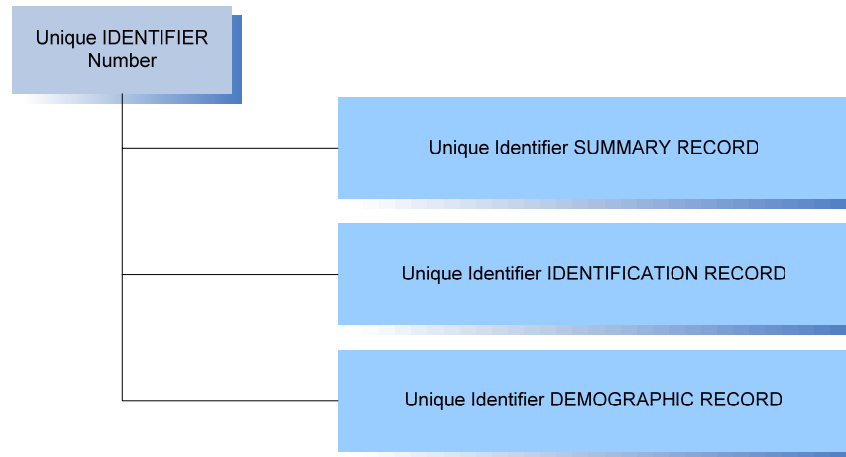


Figure 3: UHI record levels

The three types of IHI and HPI-I records act to segregate the data elements held by the UHI Organisation about an individual. The summary record will contain the minimum number of data fields to facilitate a provider searching for and locating either an individual's IHI (and record) or another provider's HPI-I (and record). The data fields contained in the summary record might include an individual's name, sex and date of birth.

The identification record contains all of the data fields that were present for the summary record and also additional data fields required to positively identify a particular individual. For example where two individuals might have the same surname and date of birth – it might be necessary to use the address field to identify the correct IHI and record.

The demographic record contains all the data fields used for the summary and identification records and all the remaining additional data fields which may not have been essential to accurately identify an individual, but are required to provide safe and high quality healthcare. For individuals this information might include a mobile phone number. For providers, this might include the geographic address where a provider practices, or a provider's email address.

The types of data fields to be collected on individuals and providers and the method of collection, including appropriate consent processes are discussed in Chapters 3 and 4.

2.3.3 What personal information will be collected for the HPI-O?

The HPI-O record will hold identifying characteristics for a provider organisation. Organisational identifying information contains far less personal information than that collected for the IHI and the HPI-I. Provider organisation characteristics may include an organisation's name, location

(address), general contact details and possibly information about the particular healthcare services offered at that location.

As a provider organisation can only act through its authorised employees, personal information on nominated representatives for a particular HPI-O will be collected by the UHI Organisation. The type of information collected on nominated representatives will be similar to the requirements in place for registration requirements in corporate law.

In order to audit HPI-O access to UHI records, an authentication mechanism will be required to ensure that only those healthcare provider organisations entitled to access UHI records gain access. Such an authentication mechanism may require the collection of personal information regarding employees of a particular HPI-O in order to control HPI-O access to UHI records. Chapter 3 discusses NEHTA's Identity Management initiative, which will examine the requirements for authentication mechanisms for the UHI Service. Issues raised by HPI-O access to the UHI records are discussed in Chapter 3.

Much of the information required for the HPI and IHI Records will be collected indirectly from third parties (Data Sources): for example, State/Territory medical registration authorities. Depending on the data field and the data source, the information received from the Data Sources may be cross-checked against other potential Data Sources, for example, the Australia Post's Geocoded National Address File and Births, Deaths and Marriages Registries for date of death data.

2.3.4 Restrictions on use

A provider or a provider organisation must hold an active HPI-I or HPI-O in order to gain access to the UHI records. Use of an IHI by an individual, however, is not a prerequisite to obtain healthcare.

The IHI and the HPI are to be used only within the Australian healthcare sector. The World Health Organisation defines healthcare as "any type of services provided by professionals or paraprofessionals with an impact on health status". NEHTA's HPI program currently covers medical practitioners, pharmacists, dentists, nurses and allied health professionals. Restrictions on use of the IHI and HPI will be enforced through:

- Existing legislation/regulation at the State/Territory and Federal level (eg. privacy and health records legislation);
- Participation agreements between the UHI Organisation, providers, provider organisations and individuals;
- Appropriate access controls and processes across all participants in the UHI Service; and
- Internal and external/independent audit processes.

Governance and enforcement issues are discussed in Chapter 3.

2.3.5 Use and disclosure

IHI and HPI data held in the records will be disclosed primarily to providers and provider organisations for use in the course of delivering healthcare to individuals.

IHI data will be disclosed to individuals seeking to access and/or update their own IHI and IHI record. The UHI Organisation will also disclose to individuals identifying information regarding the providers that have accessed their IHI and IHI record.

The primary purpose for use of the IHI and IHI record is the accurate identification of individuals across all healthcare settings.

Accurate individual identification ensures that, as part of a healthcare interaction:

- the correct health information is associated with the correct corresponding individual; and
- electronic and paper-based communications (for example, discharge summaries and referrals) between providers about an individual relate to the correct person.

Accordingly, an individual's IHI and IHI record will be accessed and used to identify that individual and over time it will become his/her primary healthcare identifier. The IHI could be used to attribute clinical information accurately to the individual – for example, to electronically report test results from a pathology laboratory to a general practitioner, or to label a bottle of medication.

The primary purpose for use of the HPI and HPI record is the accurate identification and authentication of providers and provider organisations across all healthcare settings.

Accurate provider identification and authentication ensures that:

- an individual's health information is accurately associated with the correct provider;
- electronic and paper based communications (for example, discharge summaries and referrals) occur between the correct providers; and
- providers are appropriately authenticated and authorised to access the UHI records.

A provider might, for example, search the Healthcare Provider Directory for an appropriate specialist to refer an individual. The UHI Service ensures that the provider can identify the specialist with certainty using the HPI-I and confirm the correct contact details to communicate a referral advice to that specialist with reference to a specific individual's IHI.

Disclosure of IHI and HPI data to providers will occur via online enquiries through a provider or provider organisation's own computer system. These online enquiries are likely to be triggered by particular business processes, for example, generating a referral letter.

Multiple mechanisms will be established to allow individuals to access their own IHI and IHI record. Current mechanisms under consideration include: via general internet access (with the appropriate authentication credentials such as a User ID and password), shop fronts or through a national call centre.

Appropriate security and access control rules will ensure that only authorised access occurs. Access control and identity management measures such as electronic authentication credentials are discussed in Chapter 3. Potential secondary uses of IHI and HPI data are discussed in Chapter 4.

2.3.6 Linkages between the IHI and the HPI

The IHI and the HPI may be linked in various circumstances:

- A medical record may record the IHI, HPI-I and HPI-O relating to a particular healthcare event.
- HPI-Os and HPI-s will be linked reflecting the particular provider organisations that providers are associated with.
- The HPI-I of a provider who has accessed an individual's IHI will be linked to that IHI record through the audit log. Similarly when a provider organisation accesses an IHI, the HPI-O and administrator details will be linked to that IHI record through the audit log.
- The mechanisms managing authorised representatives for individuals may involve the UHI Organisation linking two IHI's.

2.3.7 Up-to-date and accurate data

The benefits of the UHI Service can only be realised if the IHI and HPI records are up to date and accurate. Accordingly, data quality activities are critical to the success of the UHI Service. The UHI Organisation will undertake data quality activities including:

- Managing the integrity of the UHI records, ensuring the IHI and HPI are unique and persistent.
- Enabling record updates, the data for which will be received from a range of data sources such as professional registration bodies, individuals, providers and provider organisations. Individuals may request providers or provider organisations to send IHI record updates to the UHI Organisation on their behalf.
- Investigating and resolving duplicate and replicate situations where for example, one individual is associated with two IHI's or where one IHI may be associated with two individuals. These activities may require the suspension, deactivation, linkage or reissue of identifiers.
- Suspension of the activity status of an IHI or HPI where that individual, provider or provider organisation has ceased to participate in the UHI Service.
- Deactivation or retirement of an IHI or HPI which may be required when an individual has passed away, a provider organisation has ceased operations or a provider has retired.

The data quality in the UHI records will also rely on provider and provider organisations adhering to rigorous systems specifications and certification rules in relation to information management practices.

2.3.8 Information flows

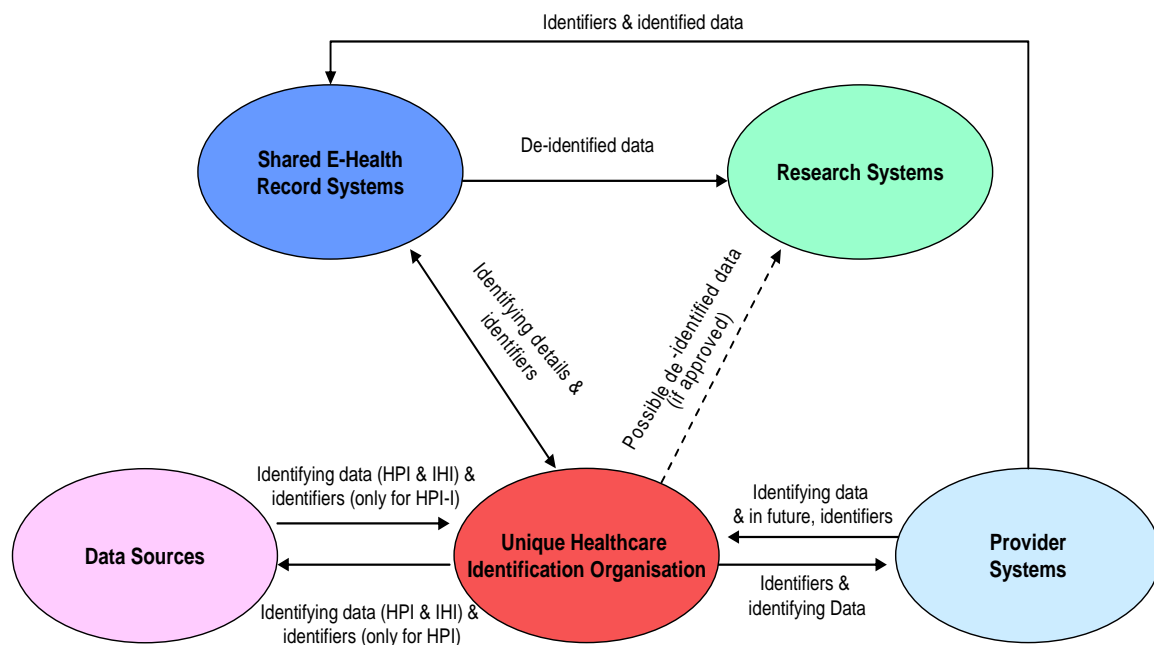


Figure 4: Map of information flows

3 Mapping information flows against privacy principles

3.1 Introduction

As discussed in NEHTA's *Approach to Privacy* document, Australia's current privacy landscape is best described as a 'patchwork'. Nevertheless, the shared sources of most Australian privacy laws mean that it is possible to analyse the various sets of privacy principles and extract a common set of privacy principles for the handling of health information. In NEHTA's *Approach to Privacy* these principles were shown as follows.

Privacy Principle		General Compliance Requirements
1	Collection	<ul style="list-style-type: none"> Collection is necessary; and Consent is obtained or collection authorised by or under law; and Individuals are notified of the collection.
2	Use and Disclosure Primary Purpose	<ul style="list-style-type: none"> Allowed
	Use and Disclosure Secondary Purposes	<ul style="list-style-type: none"> Secondary purposes are directly related to primary purpose and within individual's reasonable expectations; or Consent is obtained; or Required or authorised by law; or Serious or imminent threat to any individual's life, health or safety.
3	Data Quality	<ul style="list-style-type: none"> Information is accurate, complete and up to date.
4	Data Security	<ul style="list-style-type: none"> Protection from misuse, loss and unauthorised access, modification and disclosure; and Destroy or de-identify information that is no longer necessary.
5	Openness	<ul style="list-style-type: none"> Provide a document that clearly sets out policies on handling personal information.
6	Access and Correction	<ul style="list-style-type: none"> On request and excluding certain circumstances, provide individuals with access to their personal and health information; Where reasonable, correcting health information at the request of the individual.
7	Identifiers	<ul style="list-style-type: none"> Assignment of identifiers must be necessary; Adoption of identifiers must be in accordance with prescribed circumstances.
8	Anonymity	<ul style="list-style-type: none"> Allow anonymity where lawful and practical.

9	Transborder Data Flows	<ul style="list-style-type: none"> • Transfer if reasonable belief recipient is subject to comparable information privacy scheme; or • Transfer with individual's consent; or • Transfer is necessary for contract at the request of, or to benefit the individual.
---	------------------------	--

Table 1: Common Privacy Principles for the Collection & Handling of Health Information

NEHTA's work to date in relation to the UHI Service has been based on the application and analysis of this summary set of privacy principles. In the absence of a single, coordinated national scheme regulating information privacy in Australia, this summary represents a benchmark for NEHTA's work. Likewise, in the absence of knowing what type of legal entity (i.e. public sector or private sector) would be given the role of UHI Organisation, this summary provides the best approach to identifying and responding to privacy risks.

As discussed in Chapter 5, once it is known whether the UHI Organisation is a public or private entity, NEHTA will commence mapping the information flows described in Chapter 3 against the requirements of the most relevant privacy principles in the *Privacy Act 1988* (Cth), that is either the Information Privacy Principles (IPPs) or the National Privacy Principles (NPPs).

3.2 Mapping exercise

A key aspect of privacy analysis involves mapping proposed information flows against the requirements of privacy principles. NEHTA's findings in relation to the mapping of the UHI Service requirements against privacy requirements are summarised below. At this stage there are no clear impediments to the UHI Service, however, it is noted that it has not been possible to conduct a definitive privacy analysis in advance of determining the legal structure of the UHI Organisation.

Despite the fact that no privacy risks or impacts have been identified that cannot be managed or mitigated successfully, it is clear that there is still considerable work to do to manage privacy effectively in the UHI Service and that ongoing PIAs will need to be conducted.

This is discussed further in Chapter 5.

3.3 Does the UHI Service involve the collection of personal or health information?

In Australia, 'personal information' is broadly defined as:

Information or an opinion recorded about an individual whose identity is apparent, or can reasonably be ascertained.

In the private sector provisions of the *Privacy Act 1988* (Cth) 'health information' is broadly defined as:

Personal information that is associated with information about an individual's health or is collected to provide a health service.

The information contained in the IHI, HPI-I and HPI-O records constitutes 'personal information' under Australian privacy laws and is subject to protection under those laws. Further, IHI information would be categorised as 'health information' under the private sector provisions of the *Privacy Act 1988* (Cth). Additional consent requirements attach to the collection of health information under the private sector provisions of the Privacy Act. Depending

on the legal structure of the UHI Organisation this may need to be factored into compliance requirements.

In terms of NEHTA's current analysis, all of the information to be collected and handled by the UHI Organisation must comply with the following privacy principles.

3.4 Collection

The collection principle is critical to overall privacy compliance. If collection requirements are managed well, down stream information uses, disclosures and other forms of information handling are likely to be acceptable.

As a starting point, collection of personal information must be necessary for an organisation's function. NEHTA will therefore need to demonstrate the necessity of all data fields to be collected for carrying out the function of accurate identification in all healthcare settings and any associated secondary functions.

Clear purpose statement and collection notices contribute to discharging collection obligations by establishing that such information is necessary for an organisation to carry out its functions and activities.

Secondly, in the health context, individuals must either consent to the collection of their information, or there must be lawful authority to collect the information without consent.

The UHI Organisation will employ two methods of information collection which will require different compliance steps. The first type, leveraged collection, will be an indirect collection of information from pre-existing data stores, for example those held by Medicare Australia. Responsibility for compliance with collection requirements will lie with the custodians of the original data and the UHI Organisation must ensure that these third parties undertake appropriate compliance processes.

A second method will be the ongoing collection of information occurring after the initial creation of the UHI repository. The UHI Organisation will be directly responsible for carrying out compliance processes in relation to ongoing collection.

3.5 Use and disclosure

The use and disclosure principle aims to ensure that there are appropriate limits to the subsequent use and disclosure of personal (including health) information. Compliance with this principle is directly tied to an organisation's ability to clearly and accurately articulate the purposes of collection.

The primary purpose of collecting information enables all uses and disclosures of that information that are necessary to achieve the primary purpose.

NEHTA considers that all UHI Organisation uses and disclosures of information relating to the primary purpose; accurate identification of individuals and providers across all healthcare settings, will be allowed.

NEHTA will examine any proposed secondary uses and disclosures of information to determine whether they are uses that can be characterised as directly related to the primary purpose of accurate identification. These secondary purposes must be regarded as being within the reasonable expectations of the community as a directly related secondary use. Directly-related secondary uses might include, for example, administrative (or quasi-clinical) processes, such as sending vaccination reminder letters or organising home visits. Directly-related secondary uses and disclosures do not require additional consents.

All other secondary uses and disclosures of information must be either directly related to the primary purpose, or will require further support such as lawful authority or consent before they can occur.

3.6 Data quality

The data quality principle requires that information is accurate, complete and up-to-date.

NEHTA has developed a data quality framework to describe quality assurance and quality control processes that focus on data quality management, standardised data inspection, operational data quality, issues tracking, issue remediation, manual intervention when necessary, integrity of data exchange, contingency planning and validation.

Data quality governance policies will provide guidelines for community participation. They are broad in scope and define the framework for community oversight of UHI data quality. The governance policies define the criteria for participants to join the community and methods to measure conformance to established policies.

Business rules governing the relationship between different types of Data Sources and the UHI Organisation, specifying the data exchanges to take place will be critical to ensure data quality.

Finally, and importantly, individuals will be encouraged to ensure their data is accurate, complete and up-to-date and will be provided with access and correction rights to their own records.

3.7 Data security

The data security principle is concerned with the protection of personal information from misuse, loss and unauthorised access, modification and disclosure and requires that information is destroyed or de-identified when it is no longer necessary. This principle must be interpreted subject to other legislation such as public records legislation.

The security components of the UHI Service will be complex and require that significant security measures are in place prior to full implementation of the UHI Service.

Within the NEHTA work program, a number of initiatives are being undertaken which will establish relevant security 'building blocks'.

NEHTA will provide the foundation for secure electronic communications amongst healthcare providers, by defining a set of secure messaging standards to be used in e-health. These standards will allow for a flexible and dynamic approach to e-health interoperability and can help ensure the evolution of an e-health environment that is sustainable and affordable.

A key aspect of protecting the integrity of information is to have strong identity management mechanisms in place. These mechanisms offer a major opportunity to introduce benefits to individual privacy as part of the UHI Service.

Authentication mechanisms must be two-way and are important to ensure that:

- individuals can be certain that they are interacting with the legitimate UHI Organisation's website through the individual web portal access; and
- the UHI Organisation can be certain that only those healthcare providers entitled to access UHI records gain access.

NEHTA is currently examining existing e-health authentication processes as well as a broad range of available alternatives, including jurisdictional, agency and industry solutions with and beyond health.

NEHTA will support a scalable and sustainable interoperability approach to Digital Identity Management services including their specifications and dependencies. Conformance criteria will be identified within these specifications and representative solution designs outlined. Where no jurisdictional or national solution is able to meet the conformance specification, NEHTA will propose a solution and call for expressions of interest from industry to develop it.

NEHTA has identified that, at this stage, healthcare individuals will require one-factor authentication (subject to the level required by Australian Government e-Authentication Framework (Individuals) framework); and providers will require two-factor authentication (ie. digital certificates delivered on smartcards). NEHTA may need to test whether these levels of authentication strike the right balance.

An Identity Management Blueprint will be released for public consultation purposes in mid 2007. It will outline further detail around NEHTA's identity management initiative. In summary:

- NEHTA is in the process of examining the scope for national e-health user authentication services, to control access to e-health systems such as that managed by the UHI Organisation. A user authentication service will form one of the basic building blocks for interoperable and service-oriented national e-health systems.
- An identity management service will authenticate identity, manage other claims made about identity (such as their role) and require the secure presentation of a validated identifier claim in order to allow access to the UHI records.

Further detail about NEHTA's security policies will be assessed during the full PIA of the UHI Service in 2007 and the results published in the Identity Management Blueprint.

3.8 Openness

The openness principle ensures that organisations are transparent in their data collection and handling activities. As part of the openness principle, the UHI Organisation will need to develop privacy policies that clearly outline how personal information will be collected and handled.

At this stage of the UHI Service's development, it is too soon to develop privacy policies and privacy notices. However, as discussed in Chapter 5, prior to implementation of the UHI service the development of privacy tools will be required including privacy policies, collection notices, participation agreements, communication tools such as brochures and posters, etc. The full PIA process will also produce relevant content for a wide range of UHI privacy documentation.

Privacy policy development is scheduled to commence in February 2007.

3.9 Access and correction

The access and correction principle provides that individuals have the right to seek access to, and correction of, information held about them.

As it is proposed that individuals will have access to their own UHI records via a number of mechanisms including online, shop front and call centre, this aspect of the principle will be fully complied with. Mechanisms will be in place for individuals to update and either directly correct themselves, or request that corrections be made to their own information contained in UHI records.

Individuals acting as authorised representatives will likewise be able to access and correct the records of the people they represent although they will need to establish that a legitimate authorised representative relationship exists. Authorised representative issues are discussed further in Chapter 4.

It is not envisaged that any information contained in the IHI record would be withheld from, or invisible to, the individual. There is likewise a commitment to enabling people to correct information held in the UHI Service. In this sense, the UHI Service is likely to comply fully with the requirements of the access and correction principle.

3.10 Identifiers

Organisations create and use identifiers for a range of purposes to manage interactions with large numbers of individuals. Unique identifiers that 'sit behind' tokens such as drivers' licences, EFTPOS bank cards and video borrowing cards improve administrative efficiency but also assist organisations to authenticate the individuals that they are dealing with.

NEHTA will assess the effect of the various Australian privacy laws, which contain prohibitions and/or restrictions governing the creation and adoption of unique identifiers. These restrictions aim to prevent function creep of identifiers, discouraging their development as almost universal identity numbers. NEHTA's analysis will depend on knowing whether the UHI Organisation is a public or private entity.

For example, if a Commonwealth agency were to create and implement a unique identifier, such practice would require alignment with the identifier-specific provisions in National Privacy Principle 7 of the *Privacy Act 1988* (Cth). The NPPs prevent private sector organisations from adopting identifiers assigned to individuals by Commonwealth agencies unless they have been authorised to do so by regulation. The circumstances in which the organisation could use or disclose the identifiers are also restricted.

3.11 Anonymity

The anonymity principle promotes the ability for individuals to conduct transactions anonymously where lawful and practical.

Clearly, the UHI Service's primary objective is to uniquely and accurately identify individuals – both as individual consumers and as healthcare providers – within the Australian healthcare sector. This means that, on the whole, there is no meaningful role for anonymity in the UHI Service. The ability or desirability of the UHI Organisation to provide for masking or pseudonymous transactions is another matter and is discussed further in Chapter 4.

NEHTA is committed to developing appropriate masking or pseudonymity functionality in the UHI Service.

A number of health services are provided on an anonymous basis to promote important public health objectives. For example, this includes sexual health clinics and alcohol and drug facilities. These health services would not use the IHI in their dealings with clients.

3.12 Transborder data flows

This principle is designed to limit flows of personal information to jurisdictions without equivalent or adequate privacy protection measures in place. Prior to implementation of the UHI Service, the adequacy of Australian jurisdictions' privacy protection measures will be assessed.

It is considered at this point that a combination of existing legislative or administrative arrangements in tandem with appropriate contractual controls

will be used to ensure compliance with transborder data flow provisions within Australia.

All collection and handling of personal information associated with the UHI Service will be undertaken in Australia. There will be no offshore processing of data.

3.13 Governance

While not a privacy principle in its own right, the governance arrangements developed for the UHI Service are both an essential component of the UHI Service and a means of ensuring ongoing engagement with the privacy tenets developed by NEHTA for national e-health infrastructure involving the collection and handling of personal (including health) information.

Development of a suitable e-health governance model is a key dependency for privacy compliance and will be critical in establishing the legal connections (and therefore risk allocation) between not only the Data Sources and the UHI Organisation but also between the users of the personal information and the UHI Organisation. Governance issues will require analysis of policy issues and also of legal structures.

Key tools for managing and mitigating trust and control risks are governance processes that include failure prevention and failure handling mechanisms such as responsive and consumer friendly complaints systems. Appropriate governance mechanisms are a crucial requirement for a system that individuals trust and are willing to participate in.

Emphasis should be as far as possible on the prevention and detection mechanisms built into the system (for example, internal business processes and audit supported by external accountability and audit systems). The governance system will have a corresponding focus.

There must be adequate sanctions and remedies in case of failure to comply with privacy protection measures. Such enforcement measures must take account of Australia's federated structure and the current legal framework governing information and health privacy. Potentially, sanctions and remedies may need to be developed in addition to the privacy-specific ones; these may be criminal or civil.

Governance issues also require an understanding of 'clinical culture' and analysis of the alignment between the expectations and understanding of the health service provider and those of the individual about what will be done with personal information collected. Focus must be placed on identifying circumstances where expectations are not shared.

The preliminary PIA report recommended that complaints processes be integrated with the overall governance of the HPI and the IHI.

It is envisaged that a Governance Entity would set strategic directions and policies for the UHI Organisation and other national e-health infrastructure services such as an Identity Management Service. It will need to have the capacity to provide national leadership, coordination and oversight of the UHI Organisation.

For example, should governments decide that a potential broadening of users within the definition of 'healthcare administrator' and the approach to defining 'healthcare' and the 'health sector' is desirable (e.g. aboriginal health workers or aged care workers), care would need to be exercised in relation to identifying who these additional participants may be; why they require access to UHI records; and where they should be placed within that system. In essence, a Governance Entity would need to develop a clear policy position that is broadly acceptable to all stakeholders.

NEHTA will act in an interim capacity as the Governance Entity, however a long-term entity will be required to carry out the governance role. Governance in the interim is proposed to be handled contractually.

4 Key issues

4.1 Overview

NEHTA's privacy analysis must balance the improved practice and security that a more systematic approach to healthcare identification brings, against the potential privacy risks that arise from the UHI approach.

A number of privacy risks raised by unique identification are already present in the Australian health services system. A significant amount of personal information is already held within healthcare organisations such as GP clinics and hospitals. Medicare Australia holds large amounts of personal information in an electronic and centralised form. Secondary uses of personal information are increasing for both academic and commercial research purposes.

In establishing a new identification system with proper privacy protection NEHTA aims to include mechanisms that mitigate (where possible) these pre-existing risks, as well as to develop privacy-positive approaches wherever possible.

Potential privacy benefits to an individual arising from the UHI approach are also considered in a risk analysis. Some of these protections (such as audit of provider access and a greater ability to update one's own information) are much less feasible in a paper-based system.

The governing frameworks or standards for privacy in Australia are the various privacy principles legislated in statutes across Australia as well as any other laws that regulate the collection and handling of personal information. The privacy principles are intended to provide a framework for the responsible collection and handling of personal information, rather than a prescriptive set of rules to be obeyed.

Just as for managing other legal compliance issues, complying with privacy law can prompt the application of tests of reasonableness or practicality. Decisions on what is reasonable or practical in relation to a particular e-health initiative are essentially threshold decisions. These decisions may use a test of balancing an individual's right to privacy against competing public interests in the free flow of information.

Some of the threshold privacy issues raised by the UHI Service include:

- The nature of consent required for collection of personal information for the UHI Service (eg. express vs. implied);
- The nature of access and updating mechanisms required for individuals to their own information held by the UHI Organisation;
- The extent of secondary uses that should be supported by the UHI Service; and
- The scope or extent of activities that can be reasonably characterised as 'healthcare' related.

These threshold issues represent areas where there is significant scope to promote privacy-positive approaches rather than simply meeting minimum privacy principle requirements. In the previous chapter, a summary of the UHI Service's likely compliance with privacy principles and key issues around governance were provided. This chapter shows NEHTA's current thinking in relation to key threshold issues and seeks specific feedback from readers.

These issues will be adjusted in line with feedback received through the UHI Privacy Blueprint consultation process and policy positions finalised prior to the commencement of the full PIA process in 2007.

4.2 Consent and notification

Consent in the health context has proved to be one of the most intractable policy and legal issues faced by Australian e-health initiatives. Numerous debates about the respective merits of 'opt in' v. 'opt out'; confusion about the plethora of privacy laws in operation in Australia; and the risk of failing to meet all relevant compliance requirements (particularly meeting the test of 'informed consent') have deeply affected the debate to date.

Consent – put simply, “the voluntary agreement of a person or a person’s authorised representative about a proposed action” – is one key element of a privacy compliance regime. However, it is not the only element to consider. NEHTA’s approach to consent has been to ensure that it is considered in context, alongside all of the other privacy principles. It should also be considered in relation to the requirements of specific initiatives rather than in the abstract.

NEHTA must ensure that the UHI Service complies with all relevant privacy requirements and that the privacy approach adopted is supportive of identified business requirements. In other words, it is not acceptable to develop a UHI model that contravenes Australian consent requirements regarding the collection and handling of personal (including health) information. But neither is it acceptable to develop a 'perfect' privacy compliance regime if it results in sub-optimal participation rates. NEHTA’s main concern is to ensure that the twin goals of privacy and an effective UHI Service are met.

Consent occupies a further, less compliance-based, role in relation to the introduction and ongoing operation of e-health initiatives, in particular as a means of ensuring individual participants feel that they exercise a degree of control over the collection and handling of their personal information and that there is transparency about proposed uses and disclosures of that information.

NEHTA expects that ongoing work will be required to develop a comprehensive consent model for the UHI Service and that a full range of consent issues, including use and disclosure of the identifiers, will be considered in the full PIA. At this stage, NEHTA is seeking specific feedback around one particular consent circumstance, as outlined below.

The UHI Service is based on the premise that the initial data-set for the IHI will be drawn from Medicare Australia’s pre-existing collection of data.

The consent issues surrounding obtaining this data are different to those that apply to the collection of new information once the IHI is operational. In this circumstance, the initial collection of data would be obtained through a third party – Medicare Australia. The intention is that the UHI Organisation would impose requirements on Medicare Australia to ensure that applicable consent and notification requirements are met. Once the IHI is operational, these responsibilities would lie with the UHI Organisation.

Regardless of whether existing information or new information is involved, clear consent and notification policies will need to be in place.

The particular issue that NEHTA has identified for consultation purposes concerns the initial creation of the IHI from Medicare Australia’s information systems. In summary, Medicare Australia holds information collected for specific purposes, as authorised by its governing legislation. The IHI proposal involves using that information for another purpose – the creation of a national identification service for individuals.

KEY QUESTIONS

The key privacy issues that NEHTA has identified for consultation purposes from the above include:

1. How best to manage consent requirements around the initial use of Medicare Australia's information systems?
2. Whether certainty around the legitimacy of that use is best achieved through seeking to meet current consent requirements or whether legislative support is preferred?

There are three options for managing initial consent requirements for participating in the IHI aspects of the UHI Service:

1. An "opt in" system whereby each individual provides express consent to participate in the IHI. This would require individual consent before any identifiers could be created. Medicare Australia would need to contact every individual concerned and explain the IHI in sufficient detail so that they could make an informed decision about whether or not to participate. In this case, responsibility for meeting informed consent requirements would lie with individual Australians rather than Medicare Australia although, conversely, Medicare Australia would not be able to create any identifiers until individuals provided express consent. This involves a considerable compliance effort and may result in low rates of take-up.
2. An "opt out" system whereby each individual is presumed to participate in the IHI but is given an opportunity to opt out. Identifiers would be created and distributed to individuals but their use would be conditional on individuals choosing to participate in the IHI scheme, in particular, agreeing to a range of clearly defined uses and disclosures. This too, would require that Medicare Australia communicate with all affected individuals but includes the additional requirement that Medicare Australia demonstrates that informed consent requirements have been met. It is known that this is very difficult to achieve under an opt-out model as responsibility for meeting the informed consent requirements lies with the organisation (i.e. Medicare Australia) rather than the individuals themselves. However, if Medicare Australia were able to demonstrate that informed consent requirements have been met, it could proceed to create and distribute the IHI. This involves a considerable compliance effort with a high degree of risk but may result in higher rates of take-up.
3. "Lawful authority and notice", whereby specific legislation is developed to support the IHI, enabling the creation and distribution of the identifiers in accordance with the requirements of that law. In this case, the new law would authorise the creation and distribution of the IHI, removing uncertainty around whether or not informed consent requirements have been met, minimising compliance efforts on the part of Medicare Australia and focusing attention on the specific uses and disclosures which the IHI would support.

NEHTA's view is that legislative support for the UHI Service will provide the greatest level of legal certainty around meeting consent requirements but that this approach needs to be tested. NEHTA is not in a position to develop UHI legislation as it sits outside of government and has no ability to progress legislative proposals. At the same time, NEHTA is interested in ensuring that the UHI Service is appropriately supported, including through legal mechanisms.

It is clear that any consideration of legal support by governments would be likely to consider a wider range of issues than consent alone, including, for example, governance arrangements and potential sanctions and/or remedies for misuse of the UHI Service. At this stage, however, NEHTA is seeking feedback on the specific consent issues outlined here.

Are there any other issues NEHTA should take into account in relation to this topic?

4.3 Who is authorised to access UHI records?

4.3.1 Individual access

As discussed above, individuals will not have access to HPI-I or HPI-O records. Individuals will, however, have access to their own IHI and IHI record and the corresponding provider audit log. Individuals will be able to update their details through different access points, for example, by visiting a shop front, through online web portal access, calling a national call centre or by requesting a provider or provider organisation to process an update.

Some data fields may not be able to be changed by an individual without a higher level of verification, for example, changes to name or date of birth. A trade-off will occur between allowing an individual to update their personal information easily and the objectives of ensuring data quality and integrity.

4.3.2 Provider access

Access to IHI records will be triggered by healthcare events. Providers will have general access to either update an IHI record on behalf of an individual or to access the most up-to-date IHI record for healthcare purposes. Search protocols and audit measures for provider and provider organisation access are discussed below.

In addition to IHI access, providers will have access to an HPI Provider Directory in order to route communications and locate other healthcare providers for referrals and healthcare communications.

4.3.3 Non-healthcare provider access

On the whole, the UHI approach is predicated on direct clinical relationships between providers and individuals. However, on a practical level, a category of access is required for 'healthcare administrators'. Healthcare administrators include roles such as practice receptionists, emergency desk clerks and filing staff. As discussed above, access by administrators to IHI records will be managed through the HPI-Os. The UHI Organisation will attribute access by administrators to the provider organisation's HPI-O. As discussed earlier, in order to audit HPI-O administrator access, an authentication mechanism will be required to ensure that only those entitled to gain access to the UHI records gain access.

In some respects, the proposed design reflects the principles of an employer organisation's vicarious liability for the acts of its employees.

The 'administrator' category was initially developed to accommodate the fact that most of the administrative work relating to the UHI Service is undertaken by practice manager or receptionist employees rather than providers. NEHTA's approach to this area needs to be tested.

Appropriate role-based access control policies will be required to provide mechanisms for access to the UHI records, particularly IHI records. These policies will establish:

- What type of healthcare related staff should have access through the HPI mechanism; and
- Secondly, the appropriate method for enabling that access, reflecting the distinction between clinical and administrative workers and as a result, whether that access should be through an HPI-I or HPI-O mechanism.

A trade-off will occur between allowing ready access to IHI records that are genuinely required by providers for healthcare purposes, whilst ensuring that accountability attaches to a provider or administrator accessing a particular IHI record.

In allowing appropriate access to the UHI records and determining the policies that should apply, it is useful to distinguish between the business processes that will prompt a request for access, that is:

- Where demographic information is provided in order to determine an individual's IHI; and
- Where an IHI is provided in order to obtain the details contained in an individual's IHI record.

Access management strategies include:

- Audit functionality (see discussion on audit below), privacy policies and business protocols for searching
- Participation agreements detailing the rights and obligations of providers, provider organisations and individuals
- An ability for individuals to block providers and provider organisations from accessing their IHI record (see discussion below on masking and pseudonym functionality); and
- Clear and transparent governance and complaints processes to ensure accountability for access.

KEY QUESTIONS

- Are these policies and strategies adequate?
- NEHTA is specifically seeking feedback on the appropriate balance to be struck for the breadth of HPI-O access rights for healthcare activities. Issues under consideration include:
 - The trade-off between the accountability and transparency of UHI Service scope widening – perceptions of function creep versus the workability/flexibility of the UHI Service (noting the sheer scale of the 'administrators'/other types of not strictly clinical workers)
 - The growth in larger, and more complex, care teams. Modern approaches to government service delivery tend to emphasise coordinated care - connecting as many aspects of health and social services that are relevant to an individual. Increasing complexity in healthcare also requires a comprehensive 'picture' of an individual, in order to provide the highest quality healthcare.
- Other issues requiring consideration for non-healthcare provider access policies include:
 - Certification processes for the HPI-O, requiring an authentication mechanism to enable audit function for access by healthcare administrators. It should be noted that administrators must meet the same authentication requirements as will be required for providers.
 - Clear allocation of liability and responsibility for the acts of administrators and the development of a privacy protective culture in provider organisations that wish to take part in the UHI Service.
- Are there any other issues that NEHTA should take into account in relation to this topic?

4.4 UHI data fields

Data fields define what categories of personal information may be collected about an individual or a provider for inclusion in the IHI or HPI record. Sufficient information is required in order to ensure accurate identification. However, from a privacy perspective, it is also necessary to protect against excessive collection of personal information. The challenge for NEHTA is to ensure that the design of the demographic record associated with the IHI or HPI identifier is both sufficient and proportionate. It involves testing the degree to which particular pieces of information (data fields) are necessary, and being able to explain concisely why they are needed. It may require mediating between the specific functional needs and priorities identified by health informaticians and the expectations of the wider community, including privacy advocates.

Consistent with international and Australian standards, the proposed data fields for the IHI record currently include: first name, surname, date of birth, sex, home address, home telephone number, mother's original surname, birth plurality, birth order, date of death and three entries of home address history.

Likewise consistently with international and Australian standards, the proposed data fields for the HPI record currently include: first name, surname, date of birth, sex and current work address. Additional 'professional' information may also be collected for providers – for example the types of specialisation medical practitioners might be qualified in and whether they are currently practicing that specialisation. The HPI will also record which particular provider organisations a provider might be associated with.

NEHTA must demonstrate that the specified data fields are necessary and proportionate for UHI purposes. Excessive collection of personal information via poorly designed forms or extraneous data fields will result in a privacy breach. Further, the ad hoc collection of a vast range of data fields would also be detrimental to data quality objectives. The success of the UHI Service relies on the usefulness of the HPI and IHI records which, in turn, must contain reliable and good quality data.

NEHTA must justify any collection of personal information directly in relation to the specific requirements to ensure accurate identification of individuals. One of the means of doing this is by introducing functional limitations for the amount of data returned. As discussed above, [3.5.2] the IHI and HPI-I records will consist of three parts – a summary record, an identification record and a demographic record. This acts to 'segregate' elements of the record, promoting the release of the minimum amount of information required for matching purposes. This privacy protective mechanism will not prevent providers accessing the full record should it be required for matching purposes. There will also be limitations on the number of records returned on each search.

Currently, NEHTA's management strategy for the UHI data fields comprises:

- Data fields analysis from a healthcare identification standards perspective;
- Alignment of this analysis with identified privacy requirements;
- Consultation to test the proportionality of the data fields to the required healthcare purposes (including through this Privacy Blueprint);
- Consideration of data quality requirements and alignment with the UHI Service's data quality framework and strategy; and
- Development of mitigation strategies for additional privacy protection.

NEHTA has engaged an independent healthcare standards expert to undertake an analysis of the data fields proposed for the IHI and HPI records and to explain the relevance of items categorised as 'mandatory' for identification

purposes. The results of this analysis will be considered during the full PIA process.

In addition to the data fields analysis, NEHTA has also developed a number of essential protective mechanisms designed to further assist privacy protection. These include:

- Audit functionality enabling individuals to see what providers have accessed their IHI records;
- Segregation or compartmentalisation of groups of data fields so that the minimum amount of personal information is revealed; and
- The UHI Service accommodates special requirements around masking, restricting access or highlighting the sensitivity of certain categories of information (e.g. address details where an Apprehended Violence Order is in place).

KEY QUESTIONS

- Will the proposed data fields be capable of meeting privacy requirements around necessity and proportionality?
- Do any of the proposed data fields raise specific privacy problems that will not be mitigated by NEHTA's approach as outlined above?
- Are the proposed mitigation strategies sufficient? Are there any other positive steps that could be taken to enable access to information while ensuring that 'sensitive' information is protected?
- Are there any other issues NEHTA should take into account in relation to this topic?

4.5 Audit functionality and policy

One of the clear privacy benefits arising from the UHI Service is the ability to audit access to personal information. Appropriate audit functionality and supporting policies are a means of demonstrating that participants in the UHI Service are complying with applicable laws and policies and to detect violations. It is important to note that audit alone is not a sufficient oversight mechanism and NEHTA is not proposing that individual audit of the UHI Service forms the primary means of establishing whether or not that system is being used appropriately.

When information is held or transmitted in electronic format it leaves data trails that can give information about the activities of the person who has accessed it. In relation to the UHI Service, two types of data trails will be created: those left by providers and delegates (administrators) of provider organisations when they access the UHI Service, and those left by individuals who access their own IHI record.

The UHI Service audit function is primarily focused on recording provider and administrator access to individual IHI records. The main objectives of the audit function are:

- To provide an essential safeguard to ensure the UHI Service is being used appropriately; including the ability to deter, detect and prove violations of UHI Service policies and procedures; and
- To increase transparency of the UHI Service by allowing individuals to check their own IHI records to determine whether their IHI has been accessed inappropriately. Individuals themselves will be able to check how/when their IHIs have been accessed.

Auditing is viewed as a privacy-positive measure because it provides an important mechanism to monitor whether the UHI is being appropriately accessed and used and promotes confidence and trust in an otherwise opaque system.

Although audit functionality introduces privacy benefits to a system, negative implications can arise from an audit capability. Extensive auditing practices can slow down systems, resulting in performance issues that might outweigh any privacy benefits gained. Audit records can also be used to intrude on privacy, if they are used to monitor the way individuals may access their own records.

A trade-off will occur between the level of audit required to track use and access of UHI records and the burden placed on business processes to manage and record audit data generated. Clearly audit protocols should always be capable of picking up suspicious searching behaviour as a proactive risk management strategy.

NEHTA recognises that while access to audit trails is an important mechanism for monitoring whether the UHI Service is being appropriately accessed and used, this should focus on the data trails created by providers and administrators, not individual consumers. As a result, NEHTA will explore options to mitigate the negative privacy consequences that may arise from UHI Service audit trails. These options include limiting access to consumers' audit trails and exploring how to avoid creating data trails at all where such data is not needed for the management of the UHI Service.

While audit alone is not a sufficient oversight mechanism, individual audit is viewed as a privacy-positive measure that enhances transparency.

KEY QUESTIONS

- Clear business rules and privacy policies will be critical to the management of the UHI Service's audit and search functionality. Is this sufficient?
- Would it help promote confidence and trust in the UHI Service if **Audit & Accountability Checklists** were published, clearly outlining the UHI Organisation's approach to auditing?
- Are there any technical solutions available to mitigate the potential privacy risk associated with auditing individuals' use of the audit function?
- Are there any other issues NEHTA should take into account in relation to this topic?

4.6 Masking and pseudonym functionality

The key objective of the UHI Service is to uniquely and accurately identify individuals – whether as individual consumers or healthcare providers – within the Australian healthcare sector. As noted previously in 3.5.5 and 4.11, the primary purpose of the UHI Service is identification and there is no meaningful role for anonymity in this context except where health services are provided anonymously for public policy or legal reasons (e.g. needle exchange clinics; sexual health clinics).

However, NEHTA recognises that mechanisms for supporting special conditions and sensitivity tags for IHI and HPI records are required for circumstances where individuals are vulnerable to misuse of their personal information. Examples include individuals with protection or restraining orders in force who may be vulnerable to domestic violence or providers working in sensitive areas.

Unlike those who seek anonymous healthcare services, people in these situations may wish to gain the benefits of the improved safety and quality the UHI Service will bring as long as they can be assured that their identifying data is appropriately protected.

Masking or pseudonym functionality is one way of managing this issue as it can be used to meet the needs of people who, for a range of legitimate reasons, do not wish to be 'visible' in the UHI Service.

In these circumstances, the UHI Organisation must be able to address the needs of both individuals who require special treatment because of legal conditions (e.g. protection orders) as well as individuals who may have good reason to withhold partial/full details from general view (e.g. VIPs).

In practical terms this means it should not be possible to associate a particular person with a specific record without there being additional authorisations or particular procedures to follow. For example, the IHI record may be indirectly associated with a specific individual (pseudonymity) or, only people with particular access authorisations may view the full record.

The success of this approach is dependent on effective policies and technical protections being in place that clearly establish how, when and under what circumstances, the association between the individual and his/her record may be made. It also relies on appropriate audit and accountability protocols being in place.

KEY QUESTIONS

- NEHTA is examining current approaches to masking and pseudonymity in settings such as government administration of personal information databases and also the banking and finance sector to determine best practice approaches for the UHI Organisation to adopt. What model would best suit the requirements of the UHI Service?
- Requirements to manage sensitive circumstances for unique identifiers are interrelated with privacy management for any future Shared EHR services. It should be noted that the IHI will act as a key to an individual's Shared EHR and as such, will be directly associated with it. Does the relationship to a potential future Shared EHR service warrant additional consideration at this point?
- Are there any other issues NEHTA should take into account in relation to this topic?

4.7 A framework for dealing with authorised representatives

Central to the delivery of high quality healthcare is an environment where individuals can make informed decisions about their healthcare in conjunction with their providers. Of course, for individuals to effectively make these decisions, it is essential that they actually have the capacity to do so.

Individuals may have a range of disabilities, both in terms of the disability itself but also the severity or permanency of disability, and may have a diminished capacity to make such decisions as a result.

Although some individuals may not have the ability to understand or make decisions about how their health information is handled, their privacy must still be respected. Individuals with reduced decision-making capacity will need to compromise a reasonable level of their health information privacy in order to receive the most effective health services but this should be carried

out in a way that respects their right to privacy and where possible, promotes their individual human dignity and autonomy.

Similar issues of decision-making ability arise in relation to parental control over their children's health information. The ability of young people to keep health information from their parents or others may play an important part in their healthcare and should be taken into account in developing appropriate policies in this context. It is also the case that healthcare providers routinely make professional judgements about a child's capacity to consent to medical treatment now.

The concept of an 'authorised representative' is used to manage issues arising when individuals do not have the ability to make informed decisions themselves. Authorised representatives are individuals who have legal authority to act on behalf of someone else. For example a parent is the authorised representative of his/her children. A legal guardian is the authorised representative of the person he/she has been given guardianship over.

When a family member, carer or friend (referred to as an 'associate') serves as a substituted or assisted decision-maker although not formally appointed as an authorised representative, issues can arise due to the informal nature of the authority. An associate may not hold an express authorisation or formal legal document granting power to act on behalf of the individual concerned. It is therefore difficult to prove conclusively that the individual actually authorised their associate to carry out particular acts. NEHTA does not intend to provide a formal mechanism to accommodate associates within the UHI Service.

NEHTA recognises that current laws regulating how individuals can act on behalf of another for the purpose of accessing health information and making healthcare decisions are complex and problematic. Nevertheless, the UHI Service must ensure that mechanisms for authorised representatives are provided for in a clear and accountable way.

In order to allow an authorised representative to have access and possibly make changes to an individual's IHI record, there must be a process of validating that a genuine authorised representative relationship exists. A balance must be struck between providing a flexible mechanism that does not create an unreasonable burden, whilst also ensuring that some proof or evidence of the relationship has been confirmed.

NEHTA's authorised representatives' framework will manage the requirements for authorised representatives of individuals. Some evidence of the authorised representative relationship will need to be demonstrated in order to allow an individual to access or make changes to another's IHI record.

KEY QUESTIONS

- What processes and evidence could be reasonably required to support an application to be an authorised representative?
- Do current policies in place in similar healthcare settings manage requirements for authorised representatives adequately? If not, what are some of the issues associated with these policies?
- Should the level of access and permissions allowed distinguish between the type of authorised representative and the circumstances in which they seek to act? For example, should a higher level of proof be required to make changes to an IHI record compared to simply accessing an IHI record? Should a parent's level of access be the same regardless of the circumstances?
- Is there a need for the UHI Organisation to be able to manage

associates in addition to authorised representatives?

- Is parental consent an issue dealt with adequately by healthcare providers in the course of professional judgement used in provider decision-making?
- Are there any other issues NEHTA should take into account in relation to this topic?

4.8 Secondary uses

As discussed in 3.5.4, use of the UHI Service is to be restricted to the Australian healthcare sector. Enforcement of such a restriction is directly related to (and will rely on) the governance arrangements established for the UHI Service and/or any legislative support that may be developed for the UHI Service. It will also have an impact on the types of secondary uses that may be undertaken by the UHI Organisation.

Currently, NEHTA's considerations of secondary uses (in particular, research and statistics for public interest purposes) are circumscribed by existing legislative requirements (particularly privacy). Privacy legislation sets out rules relating to the use and disclosure of personal information for secondary purposes. On the whole, these secondary uses are only permitted where there is legal authority; individual consent has been granted; or the specific secondary use is directly related to the primary purpose of collection. Wherever possible, personal information should be de-identified prior to its release to a third party.

In relation to possible secondary uses of IHI and HPI data, it is important to note that no clinical information is to be collected or disclosed as part of the UHI Service.

It was anticipated that secondary uses of IHI and HPI data by the UHI Organisation might include the following types of analysis:

- Public health – using the identifiers and associated record to support preventative medicine and public screening activities to create conditions under which people and populations can be healthy;
- Healthcare research – using the identifier and its demographic record to undertake statistical and healthcare planning activities by appropriately authorised personnel;
- Administrative research – ensuring that systems for the operations of organisations and/or individuals are designed and operated as effectively and economically as possible.

Analysis of secondary uses must also take account of any pre-existing lawful authority, for example, legislation relating to the Australian Taxation Office or in electoral legislation.

However, at this stage of the UHI Service's development, no decisions have been made about the type and scope of secondary uses to be supported.

NEHTA's initial policy position is that wherever equivalent data is held by other organisations, e.g. State/Territory registration bodies, researchers should approach those organisations first. Consideration of requests for research/statistical analysis will only occur where the UHI repository is the only organisation capable of providing the data. Any data will be provided in de-identified format.

NEHTA is interested in receiving feedback on what types of secondary uses the UHI Service should support and how best to manage these transparently and accountably.

Ongoing work will require NEHTA to develop recommendations on the processes for approval and oversight of potential secondary use of IHI and HPI data. Secondary uses policies must comply with existing obligations, for example, medical research guidelines set down by the National Health and Medical Research Council. Policies and legislation dealing with data-matching and de-identification may also be relevant.

KEY QUESTIONS

- What relationship should there be between the UHI Organisation and external researchers?
- Is NEHTA's preliminary position on de-identifying data appropriate?
- Should consideration be given to new models aiming to facilitate secondary uses such as the National Data Network?
- Are there any other issues NEHTA should take into account in relation to this topic?

5 Consultation and next steps

5.1 Privacy Blueprint

The UHI Privacy Blueprint has been published by NEHTA to establish a framework for discussion of privacy issues. The Privacy Blueprint is a key consultation tool for the UHI Service.

5.2 Consultation

5.2.1 Clinician and Consumer Discussion Forum

NEHTA runs discussion forums with a group of diverse clinicians and independently-selected consumer representatives, to examine the relationship between NEHTA's work and healthcare safety, quality and efficiency goals.

A discussion paper on the operating concepts for the UHI Service was provided to the Clinician and Consumer Discussion Forum in May 2006. The Discussion Forum identified, at a conceptual level, potential clinician and consumer issues (including privacy) with the proposed UHI Service. This input was used to inform the Blueprint prior to consultation with privacy experts, through a Privacy Roundtable meeting.

5.2.2 Privacy Roundtable

A Privacy Roundtable was convened on 17 November 2006 to examine key privacy issues raised by the UHI Service and provide feedback on privacy risks and proposed management strategies to NEHTA. Membership comprised privacy advocates and consultants with recognised expertise in health identification and privacy issues; senior health department (jurisdiction) representatives with specific expertise in e-health systems and/or privacy regulation; and a sub-group of the Clinician and Consumer Discussion Forum.

Privacy and Jurisdictional Participants

Facilitator: Mr Malcolm Crompton, Director, Information Integrity Solutions and former Federal Privacy Commissioner

Mr Andrew Solomon, Director - Policy, Office of the Federal Privacy Commissioner	Ms Robyn Cooke, Director, Corporate Information & Records Management, Northern Territory Dept of Health and Community Services
Ms Joanna Kelly, Director – Portfolio Management, Strategic Information Management Branch, New South Wales Health	Mr David Watts, Assistant Secretary (Legal Services), Australian Government Department of Health and Ageing
Ms Anna Johnston, Australian Privacy Foundation	Ms Helen Trihas, Registrar, Victorian Registry of Births, Deaths and Marriages
Mr David Jonas, Director, Convergence E-Business Solutions	Dr Moira Paterson, Senior Lecturer, Faculty of Law, Monash University
Mr Nigel Waters, Pacific Privacy Consulting	Ms Amanda Bresnan, Policy Manager, Consumers' Health Forum of Australia
Ms Stefanie Janiec, Principal Legal Adviser, Medicare Australia	Ms Nina Nordin, Senior Privacy Officer, Medicare Australia

Clinician and Consumer Discussion Forum Participants

Dr Michael Tooth	Mr Bernard Kealey
Mr Ben Horgan	Ms Heather Grain

Note: Ms Anna Johnston and Ms Amanda Bresnan are also members of NEHTA's Clinician and Consumer Discussion Forum.

NEHTA representatives

Dr Bridget Bainbridge, General Manager, E-Health Policy	Mr Roger Glenny, General Manager, Program Coordination
Ms Sophie Nevell, Senior Legal Policy Adviser, E-Health Policy	Mr Gil Carter, Manager, Identity Management

The Roundtable reviewed the Privacy Blueprint and discussed the key issues outlined in Chapter 4. Feedback received on the Privacy Blueprint through the Roundtable process informed the finalisation of the UHI Privacy Blueprint. It will continue to inform NEHTA's ongoing internal privacy analysis and detailed design and implementation of the UHI Service prior to undertaking a full PIA of the UHI Service in 2007.

NEHTA may convene further Privacy Roundtables at critical points of the UHI Service development if additional expert privacy input is required.

5.2.3 Jurisdictional and Project Reference Groups

In addition to fulfilling its primary reporting requirements through the NEHTA Board (composed of the CEOs of the nine Australian health jurisdictions), NEHTA also consults with the Australian, State and Territory Governments through a Jurisdictional Reference Group (JRG) and a number of Project Reference Groups (PRGs).

The JRG comprises senior executives representing the nine health jurisdictions nominated by NEHTA's Board. The JRG aims to:

- Promote awareness of and provide input into key NEHTA decisions;
- Provide advice on the most appropriate means of communicating NEHTA's work within their jurisdiction and assist with the implementation of these;
- Facilitate as requested whole of jurisdiction input to, and comment on, NEHTA's work program and deliverables.

PRGs are made up of nominated representatives within jurisdictions chosen by the JRG who each have expertise that can add value and assistance to respective areas of NEHTA's endeavour, including E-Health Policy.

The PRG process provides a conduit between NEHTA and the Australian governments with respect to project details, providing insight, particularly on a technical or policy basis. An E-Health Policy PRG meeting considered this Privacy Blueprint and the key policy issues raised on 22 November 2006 in order to provide input and advice to NEHTA.

5.3 Full Privacy Impact Assessment

NEHTA is committed to conducting both internal and external (independent) PIAs on relevant NEHTA initiatives, including the UHI Service.

PIAs aim to mitigate or avoid privacy risks but also take into account any overall benefits of an initiative. PIAs are focused on ensuring compliance with privacy legislation as well as meeting broader community expectations.

NEHTA has already undertaken a preliminary PIA of the UHI Service; the results have been factored into the UHI Privacy Blueprint and inform NEHTA's ongoing privacy consultations.

When the scope of the UHI Service is fully defined, a full PIA will be carried out. Successfully completing a full PIA ensures that it is safe to proceed to the implementation phase of a major IT initiative. Conversely, failure to embed appropriate privacy protection measures may result in a breach of privacy legislation and/or involve prohibitive costs in terms of a 'privacy retrofit' of the system. It may also result in a potential loss of community confidence if privacy issues become a source of public debate.

On current timeframes, it is envisaged a full PIA will be commissioned in the first half of 2007.

Importantly, this Privacy Blueprint is based on a generic Australian privacy analysis reflecting the fact that it was not known whether the UHI Organisation would be a public or private sector body. This is critical, as the nature of the organisation determines whether it is subject to the public or private sector provisions of the *Privacy Act 1988* (Cth). While the public and private sector privacy principles are similar, there are key differences in coverage and the way they are structured that will impact on the privacy analysis undertaken.

Once the nature of the UHI Organisation is confirmed, NEHTA's ongoing privacy work, including preparation for a full PIA, will immediately commence mapping UHI design and architecture requirements against the most relevant privacy principles, that is, either the Information Privacy Principles (IPPs) or the National Privacy Principles (NPPs).

5.4 Privacy Tools

Prior to implementation of the UHI Service, development of privacy tools will be required including:

- Privacy policies, collection notices, participation agreements, communications tools such as brochures and posters; and
- Ongoing privacy support and guidance, which will be closely related to governance and oversight of the UHI Service.

These materials cover topics such as the purpose of collection of information, access, correction and complaints processes. Privacy tools may assist the UHI Organisation to discharge fundamental privacy obligations, for example, collection notices that effectively communicate the primary purpose of data collection to an individual (at a point no later than at the time of collection). Others may help ensure that employees of the UHI Organisation are well placed to comply with broader privacy requirements such as promoting access or assisting with the resolution of complaints.

Development and use of such privacy tools assists in ensuring that data collection occurs in a fair and lawful manner and that there is openness and transparency accompanying UHI Organisation practices and policies.

5.5 Summary of next steps

Activity	Timing
Ongoing examination of secondary uses	Commenced in January 2006
Development of consent model recommendations	Commenced in September 2006
Development of recommendations on governance and complaints models for national e-health infrastructure	Commenced in September 2006
Development of Identity Management Blueprint	Commenced in October 2006
Development of authorised representative framework	Commenced in November 2006
Ongoing development of participation agreements and negotiation of legal arrangements with Data Sources such as professional registration bodies	Commenced in November 2006
Conduct public consultation	Privacy Blueprint released for public comment, December 2006 – February 2007. Full PIA to commence in March 2007 when scope of UHI Organisation is fully defined; further public consultation will be undertaken as part of this process.
Ongoing development of privacy policies and notices for the UHI Organisation	Commence in February 2007

It is anticipated in the current program that the above activities will be completed by mid-2007, for consideration by the NEHTA Board (noting that some activities, such as the development of privacy policies and negotiations with Data Sources, are ongoing). Outcomes will be included in subsequent privacy impact assessment publications, which will be presented for public comment.

Appendix A: Glossary

Key Terms (and shortened version)	
Consent	the voluntary agreement of a person to a proposed action or proposition
EHR	Electronic Health Record
Health information	personal information that is associated with information about an individual's health or is collected to provide a health service
HPP	Health Privacy Principle
Healthcare individual or consumer (individual)	an individual who is the subject of care in the context of a healthcare event
Healthcare Provider Identifier (HPI)	the generic term to describe two unique identifiers – the Healthcare Provider Identifier for providers (HPI-I) and the Healthcare Provider Identifier for organisations (HPI-O)
Healthcare Provider Identifier for providers (HPI-I)	the unique identifier assigned to an individual healthcare provider and is a number
Healthcare Provider Identifier for provider organisations (HPI-O)	the unique identifier assigned to a healthcare provider organisation and is a number
Healthcare provider organisation (provider organisation)	an organisation involved in the direct provision of healthcare activities
Information privacy legislation	The overarching legal framework for the protection of personal and health information in Australia. It may prohibit or facilitate information flows and is intended to provide individuals with some control over the way in which their information is collected and handled, to ensure that organisations collect and handle information responsibly and to encourage the free flow of data.
Individual healthcare provider (provider)	A health professional involved in the direct provision of healthcare activities
Individual Healthcare Identifier (IHI)	the unique healthcare identifier for individuals within the healthcare system and is a number
IPP	Information Privacy Principle
NEHTA	National E-Health Transition Authority
NPP	National Privacy Principle
Personal information	information or an opinion recorded about an individual whose identity is apparent, or can reasonably be ascertained
PIA	Privacy Impact Assessment
Shared Electronic Health Record (shared EHR)	a repository of information regarding the health status of an individual in computer processable form, stored and transmitted securely and accessible by multiple authorised users

Unique Healthcare Identifiers program (UHI Service)	the national initiative to establish two unique healthcare identifiers enabling reliable electronic communication; the IHI and the HPI
UHI Organisation	the entity that will establish and manage the UHI records and associated unique identifiers
UHI records	refer to the identification and demographic data records that are attached to the unique identifiers - the IHI, HPI-I and HPI-O

Appendix B: Privacy Materials

B.1 Privacy Checklist

A privacy compliance checklist provides a straightforward comprehensible method of testing projects for compliance with the primary tenets of privacy law. NEHTA has developed the following list of compliance questions using Module E of the Office of the Federal Privacy Commissioner's Privacy Impact Assessment Guide (OPC PIA Guide) and also examining areas where measures can promote and protect privacy more than at present.

Although not a substitute for detailed legal compliance checking, the privacy compliance checklist is an analysis tool that can be readily applied throughout the design phase.

In a similar manner to the common privacy principles reproduced in Section 3.1 of this Privacy Blueprint, the following questions reflect an amalgam of requirements based on Australia's multiple privacy laws. Once it is known whether the UHI Organisation will be a public or private entity, NEHTA will refine the list, reflecting the privacy principles most relevant to the UHI Organisation.

B.1.1 Checklist for Privacy Compliance

- Is the information to be collected for a lawful purpose directly related to a function or activity of the collector?
- Will the information collected be necessary for or directly related to that purpose?
- Will the information be collected by lawful and fair means?
- Is consent to collect the information obtained, or is the collection authorised by or under law? Will a record be kept of whether the consent was express or implied?
- Is the personal information to be solicited by the collector directly from the individual concerned?
- Is it proposed that sensitive information be collected?
- Will reasonable steps be taken to inform the individual of the purpose of the collection and if the collection is to be authorised or required by law will the individual be so advised?
- Will the individual be advised about the usual disclosures?
- Have statutory limitations on the transfer of Commonwealth-held information been considered and complied with?
- Do any secondary purposes for collection either:
 - directly relate to the primary purpose and fall within the individual's reasonable expectations; or
 - has consent been obtained; or
 - is the secondary purpose required or authorised by law; or
 - is there a serious or imminent threat to any individual's life, health or safety?
- Will reasonable steps be taken to ensure that the personal information collected is accurate, complete and up-to-date (particularly before use)?

- Will reasonable steps be taken to ensure that the information will be collected in a way that does not unreasonably intrude on the individual?
- Are there sufficient protections against misuse, loss and unauthorised access, modification, and disclosure?
- Will there be reasonable technical and physical security in place to protect against loss, unauthorised access, use, modification or disclosure and against other misuse?
- Will information that is no longer necessary be destroyed or de-identified?
- Will there be work unit policies and procedures in place for the security of personal information during the handling (routine and ad hoc) of the information?
- Will controls and procedures be created for the authority to add, change or delete personal information?
- Will the system security include an ongoing audit process that can track use of the system including for back-up materials (eg. when and who accessed and if those processes collect personal information, will they themselves have privacy protections built in)?
- Will audit mechanisms identify inappropriate access to the system?
- Will the individual be allowed access to their personal health information?
- Will the individual (directly or indirectly) be able to correct their information?
- Will relevance be tested before use of the information?
- Have identifiers, if used, been used lawfully?
- Has anonymity been allowed to the extent practicable?
- Are appropriate contractual obligations and policies in place for transborder data flows and providing information to external parties, where transfer may occur?

B.1.2 Additional Privacy-Positive Measures

- Can individuals be described as being in control of their information throughout the process?
- Are the purposes of collection and use clearly explained and appropriately circumscribed?
- Where legal requirements call for judgements of 'reasonableness' and 'practicality', are NEHTA's positions on those issues clear and well documented?
- Has the community been consulted and privacy concerns addressed?

B.2 Privacy Impact Analysis

The privacy management tools included in the OPC PIA Guide set out key questions (Module D) to be answered through the privacy impact analysis phase of a PIA:

- Does the project comply with privacy legislation and organisation-specific legislative requirements?

- Do individuals have to give up control of information about themselves to any degree?
- Will the project require, or is it likely to result in, individuals changing their behaviour (eg. having to present identification in more circumstances) or incurring costs?
- Will decisions that have consequences for individuals be made on the basis of the personal information handled in the project (eg. decisions about services or benefits)?
- Is there provision for complaint-handling mechanisms, in the event that privacy breaches eventuate?
- Have emergency procedures been devised (including audit and oversight mechanisms) in the event that the system fails?
- Does the project have potential for function creep or other unplanned consequences?
- What is the value of the information to unauthorised users?
- Is any intrusion (physical or on property) or surveillance (covert or overt) fully justified and proportional to the outcome?
- How consistent is the project with community values about privacy (eg. does it involve new ways of identifying individuals, the creation of significant databases, or the use of genetic material)?
- How has privacy been factored in the project's cost-benefit analysis, and the analysis of the project's return on investment?

B.3 Privacy Management

The OPC PIA Guide (Module F) also sets out a range of matters to be taken into account when managing privacy risks.

- **Balancing interests** – providing an appropriate balance between the goals of the project, the interests of the agency and those of individuals who may be affected. How would ordinary individuals react?
- **Minimum standards** – ensuring a minimum standard of privacy protection for individuals affected by a project with consideration of transfer of personal information across public or private sectors and across jurisdictions, including the adequacy of privacy protection and regulatory oversight.
- **Proportionality** – ensure that any privacy infringement is proportional to, or appropriately balanced with any benefits gained from the infringement (and considering the likelihood of achieving the benefits).
- **Transparency and accountability** – ensure that measures affecting privacy are transparent to individuals, through adequate notice and availability of privacy policies, and that organisations are accountable for how they handle personal information, including through effective complaint-handling, audit and oversight.
- **Flexibility** – be sufficiently flexible to take account of the diversity of individuals affected by a project. Do some individuals have heightened sensitivities for example, about the personal information involved?
- **Deliverable promises** – ensure that privacy protections are followed through by including them in law or other binding obligations and by building them in to new technology.
- **Privacy Enhancing Technologies (PETs)** – carefully consider any available PETs, as well as the impact of implementing privacy invasive technologies.

- Review after implementation – did a project meet its primary objectives? How will a project's privacy impacts be assessed eg. in an internal audit, implementation assessment, an Australian National Audit Office or OPC audit, or scrutiny by a Parliamentary committee?