Healthcare identifiers and privacy: Discussion paper on proposals for legislative support

Issued by the Australian Health Ministers' Advisory Council
July 2009

ISBN:

Online ISBN:

Publications Number: P3 -5371

Contents

EXECUTIVE SUMMARY

This paper describes and seeks comment on legislative proposals to support the establishment and implementation of national healthcare identifiers and enhanced arrangements for the privacy of health information.

E-Health

All Australian governments recognise the potential benefits of changing how information is accessed and shared across the healthcare system through the use of electronic communication and information technology to ensure that information is available when it is needed to provide patient care.

The adoption of this technology, commonly described as e-health, is expected to transform the way in which healthcare providers practise and consumers interact with the health system and improve the safety and quality of healthcare and patient outcomes.

To achieve the most from e-health, a national approach is needed to ensure that the frameworks and key infrastructure components are coordinated and aligned across Australia[1].

Two elements that are regarded as central to the successful implementation of a national e-health system are the establishment of national healthcare identifiers for consumers and providers and the establishment of robust regulatory arrangements to ensure appropriate safeguards for patient health information and encourage participation in e-health initiatives.

Considerable work has been undertaken by all governments in relation to both the development of national healthcare identifiers and to address health information privacy issues nationally.

National healthcare identifiers

In 2006, the Council of Australian Governments (COAG) agreed to a national approach to developing, implementing and operating systems for individual and healthcare provider identifiers as part of accelerating work on electronic health records to improve the safety of patients and improve efficiency for healthcare providers.[2]

The design and development of national infrastructure for national healthcare identifiers is being undertaken by the National E-Health Transition Authority (NEHTA), a company established by governments to develop better ways of electronically collecting and securely exchanging health information.

---

1 Australian Health Ministers' Conference, *National E-Health Strategy, Summary*, December 2008
2 Council of Australian Governments (COAG) Communique (Attachment D), 10 February 2006

A Healthcare Identifiers Service (HI Service) is to be established to assign, issue and maintain the identifiers. It is proposed that Medicare Australia will be the initial service operator.

Three unique identifiers will be issued. An Individual Healthcare Identifier (IHI) will be assigned to all individuals receiving health services in Australia. Individual healthcare providers will receive a Healthcare Provider Identifier - Individual (HPI-I) and Healthcare Organisations will be assigned a Healthcare Provider Identifier – Organisation (HPI-O). The service will also hold other personal demographic details for identification purposes. The HI Service will not hold or provide access to a patient's clinical information.

Once healthcare identifiers are issued by the HI Service they are designed to be used by individuals and organisations as part and parcel of delivering healthcare services. It is expected that the identifiers will be added to a healthcare organisation's patient administration and medical records systems. More specifically, the identifiers are designed to facilitate accurate and secure electronic recording and communication of patient health information between a patient's healthcare team.

The design of the HI Service and proposals for legislation and governance arrangements to support it are detailed in Part A of the paper. In considering legislative requirements, information flows associated with the HI Service have been mapped against general information privacy requirements reflected in existing Commonwealth, state and territory privacy laws.

The proposals for Healthcare Identifiers legislation:

- establish arrangements for operating the HI Service
- specifically authorise their use for healthcare identification, health information management and communication purposes
- appropriately recognise the risks that healthcare identifiers present
- do not mandate the use of healthcare identifiers by healthcare provider organisations
- do not require individuals to declare their identifier in order to receive healthcare services
- recognise that the HI Service will also be supported by other laws and through means other than legislation, for example standards and education
- establish processes for participation
- establish processes for inquiry and complaint.
- recognise that there are existing regulatory frameworks in place to support the appropriate flow of health information for healthcare and other public interest purposes

As Medicare Australia is a statutory agency, the functions that it is to undertake as the initial service operator will be set out in the legislation. These functions include assigning, collecting, using and disclosing identifiers and related information for healthcare identification, information management and communication purposes. Medicare Australia will be authorised to use information from its Consumer Directory Maintenance Service (CDMS) to assign IHIs to individuals. HPI-Is will be the able to be assigned by trusted data sources such as registration boards under the National Registration and Accreditation Scheme (NRAS), other trusted sources and directly by the service operator.

Because the healthcare identifiers will be associated with health information about an individual it is proposed that existing privacy and other laws that currently apply in each jurisdiction to the

collection, use and disclosure of health information will continue to apply. Specific authority will be given to private sector healthcare provider organisations to adopt, use or disclose an IHI or HPI-I for health information management and communication purposes. This is to overcome a restriction in the present Commonwealth *Privacy Act 1988*.

Health Information Privacy

The regulation of health information privacy across Australia is generally regarded as a patchwork of inconsistent and overlapping requirements. The mix of Commonwealth, state and territory legislation and administrative arrangements has resulted in:

- increased compliance costs, particularly where businesses are conducted across jurisdictional boundaries or public and private sectors
- confusion about which regimes regulate particular businesses
- forum shopping to exploit differences in regulation
- uncertainty among consumers about their rights.[3]

There have been a number of recent reviews proposing action to address these inconsistencies. The most recent is a review by the Australian Law Reform Commission (ALRC). The ALRC recommended that a single set of high-level Unified Privacy Principles (UPPs), covering all types of personal information including health information, be adopted across Australia as part of a nationally consistent privacy framework.

Health Ministers have agreed that national health information privacy arrangements should be implemented on a uniform national basis as part of that framework, but have identified a number of key requirements that would need to be addressed for this to be achieved. These include a clear role for Health Ministers in oversighting health information requirements, an appropriate balance in health privacy regulation between availability for legitimate purposes and privacy protections, a high level of uniformity and implementation in a timeframe to support e-health implementation and investment.

It is expected that most of these requirements will be able to be addressed through discussions between governments about how a national privacy framework is implemented and specific technical amendments to the UPPs and definitions. Part B of the paper describes the amendments that are proposed and the rationale for these against the recommended privacy principles set out in the UPPs.

Timeframes

The HI Service is expected to be operational by mid 2010. Discussions between governments about a national privacy framework across all jurisdictions and its implementation may not be completed by that time. Until revised privacy arrangements are implemented it is proposed that existing health information regulation and administrative arrangements will apply to the handling of healthcare identifiers to underpin the specific legislative proposals outlined in Part A of the paper.

---

3 Office of the Privacy Commissioner, *Getting into the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), pp. 66–8.

1 INTRODUCTION

1.1 Purpose and scope

This discussion paper outlines and seeks feedback on two important and interrelated issues:

1. A proposed legislative framework to support the establishment and implementation of a national HI Service (HI Service). Each healthcare consumer and each healthcare provider (individual and organisation) will be assigned a unique identifier for healthcare purposes. Healthcare identifiers are considered fundamental to effective, secure and efficient electronic storage and communication of health information. Section A of this paper describes the approach to establishing healthcare identifiers, explains how they would benefit healthcare stakeholders and sets out the regulatory issues for discussion.
2. Proposed national privacy regulation changes that focus on the specific privacy needs of Australia's health system, including to adequately support advances expected from e-health developments. Section B of this paper presents these regulatory proposals building on the recommendations made by the Australian Law Reform Commission (ALRC) in August 2008. These additional health privacy proposals address key issues not currently included in the ALRC recommendations.

The purpose of this paper is to encourage discussion and feedback on the two regulatory issues outlined above. The paper has been developed by a collaborative working group of representatives from Commonwealth, state and territory health departments. As such it represents a collection of issues identified by that working group rather than a concluded policy position of governments.

A list of key definitions used throughout the paper can be found at Appendix 1.

It is expected that public consultation will identify new issues and approaches for addressing regulation of healthcare identifiers and health information privacy.

1.2 Issues not in scope

The scope of this paper is limited to the legislative issues relating to the establishment of a national HI Service and to the national health information privacy regulation. While a number of other national and local e-health initiatives, including proposals for Individual Electronic Health Records (IEHRs), are expected to build on the implementation of national healthcare identification arrangements and a national privacy framework, those initiatives and any required regulatory support are not in the scope of this discussion paper and associated stakeholder consultation.

1.3 Other laws and obligations

Other laws, as well as privacy laws, may regulate health information sharing. These include laws that may prohibit specific information flows or authorise information flows that would otherwise be a breach of privacy legislation. Examples include:

- health services legislation
- Freedom of Information (FOI) legislation
- public health notifications required under law
- child protection legislation
- HIV AIDS legislation
- mental health legislation
- power of attorney and guardianship legislation.

The legislative proposals set out in this paper are intended to integrate with rather than override existing statutory and service delivery regimes such as those listed above.

1.3.1 Common law duty of confidentiality

The common law duty of confidentiality that healthcare providers owe to patients when personal information is collected as part of a healthcare interaction will continue to operate.

1.3.2 Professional requirements and standards

Requirements are imposed on certain healthcare providers under the various healthcare registration schemes. Healthcare and clinical standards are also issued by a range of expert bodies. These requirements and standards will continue to operate and are integral to the effective use of national healthcare identification arrangements at the local level by health service organisations.

1.4 How to make a submission

Submissions are invited from interested stakeholders on the legislative proposals for healthcare identifiers as set out in part A of this document, and national health privacy arrangements set out in part B. The paper raises questions to stimulate discussion on particular issues. These questions are not intended to limit the range of any submission.

Submissions must identify the names of the parties and/or organisations they represent, as well as contact details, including email addresses, if applicable.

Submissions may be:

1. Forwarded to:

   Healthcare Identifiers and Privacy Submission
   Primary and Ambulatory Care Division (MDP 1)
   Department of Health and Ageing
   GPO Box 9848
   CANBERRA ACT 2601

Or

2. Emailed to: ehealth@health.gov.au

Submissions will not be made publicly available but will be shared with relevant government agencies to inform jurisdictional consideration of national privacy arrangements. Please note that submissions or comments will generally be subject to freedom of information provisions.

The closing date for comments and submissions is **5pm (Australian Eastern Standard Time), 14 August 2009.**

2 BACKGROUND AND CONTEXT

Australia's Commonwealth, state and territory governments, healthcare providers and an increasing number of consumers recognise the potential benefits of using secure information and communication technologies in the delivery of healthcare services. Broader social trends have increased demand for, and acceptance of, the use of information technology to meet personal and community needs.[4]

Healthcare is an information-intensive industry with information being central to all aspects of clinical decision-making, care planning, management, service delivery and resource allocation. All governments are working to reform outdated communications and record-keeping practices in the health system.

The Australian healthcare sector is a complex of public and private interests, hospital and community facilities, GPs, laboratories, health funds, professional associations, special interest groups and individual consumers. All stakeholders have interests in health information and in the privacy and security of that information. Many stakeholders have invested in systems and equipment to enable them to manage their information and maintain its privacy.

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

Lack of accurate patient identification at the point of care can result in risks to patient safety from not being able to correctly associate health information from a single or multiple episodes of care to the correct patient. Errors can include medication errors, incorrect surgical interventions and diagnostic testing errors.

A national approach to healthcare identifiers was agreed by the Council of Australian Governments (COAG) in February 2006 as part of accelerating work on electronic health records to improve patient safety and increase efficiency for healthcare providers. In November 2008, COAG re-affirmed its support. It agreed to assignment of an Individual Healthcare Identifier (IHI) as a universal identifier and requested public consultation on national health privacy legislative proposals with a report back to COAG on the outcomes later in 2009. These decisions were announced by Health Ministers on 5 March 2009.[5]

A Healthcare Identifiers Service (HI Service) is being designed and developed by the National E-Health Transition Authority Limited (NEHTA) on behalf of all governments. NEHTA is a company established in July 2005 by the Commonwealth, state and territory governments to develop better ways of electronically collecting and securely exchanging health information.

---

4 Australian Health Ministers' Conference, *National E-Health Strategy, Summary, December 2008*, p. 3, www.ahmac.gov.au

5 Australian Health Ministers' Conference Communique, 5 March 2009

The HI Service will be a fundamental starting point for secure, reliable electronic exchange of information for healthcare purposes.[6] Legislation is required to support the establishment of the HI Service, and it must operate within a national privacy environment suited to the particular privacy needs of health information

2.1 National healthcare identifiers

The accurate identification of individuals and healthcare providers is vital when communicating electronically. Unique healthcare identifiers will minimise the likelihood of information being sent to the wrong healthcare provider or being assigned to the wrong patient.

Individuals are familiar with the need or expectation to identify themselves as part of their interactions with a range of different services and organisations, including healthcare services. Identifiers are given to individuals by a service or organisation to manage interactions with those individuals. Depending on the context, names, passwords and tokens (such as passports and cards) can be used by an individual to assert who they are.

Unique identifiers can facilitate more seamless and convenient interactions between service organisations and consumers, they can also make it significantly easier to match or link personal information that has been collected in different contexts and for different purposes. Such linkages can facilitate a range of functions, such as more targeted (and potentially intrusive) direct marketing through to data surveillance of how individuals go about their lives.[7]

In the healthcare context, unique patient and healthcare provider identification (both for individuals and organisations), supported by a common national legislative and policy framework, is expected to result in improvements to the secure communication and management of patient health information and reduce adverse events associated with mismatching.

2.2 Actions to date

In 2006, NEHTA was commissioned to develop a national HI Service. This involved developing a technical design as well as taking a collaborative and consultative approach with clinicians and consumers, with a strong focus on privacy and security measures.[8]

In 2007, NEHTA contracted the scoping, design, build and testing of the HI Service to Medicare Australia. At present, Medicare Australia's involvement is limited to these four areas.

Subject to the legislative proposals discussed below, Medicare Australia will also provide the trusted initial dataset[9] for individual identifiers. Other elements of existing Medicare Australia

---

6 Australian Health Ministers' Conference *National E-Health Strategy, Summary*, December 2008, www.ahmac.gov.au

7 Office of the Privacy Commissioner, *Submission to the ALRC Review of Privacy – Issues Paper 31*, 8 March 2007, pp132.

8 Privacy is an issue of great importance and concern to Australians – particularly in the health sector. A broad overview of NEHTA's position on privacy is set out in NEHTA's *Approach to Privacy* (available from www.nehta.gov.au).

9 Trusted initial dataset refers to the personal information needed to uniquely identify an individual, which has been verified by an accepted evidence of identity process. Medicare Australia's Consumer Directory Management Service contains personal information about individuals that has been obtained directly from individuals and supported by documentation such as passports to provide a level of certainty about the quality and accuracy of that information.

infrastructure are being used in the design of the HI Service, including information policies and customer services, such as shop front and online services. For these reasons, it is proposed that Medicare Australia will be the initial operator of the HI Service. These arrangements are expected to be in place for the first two years of HI Service operation.

A final decision has not been made about the arrangements for managing the HI Service and will be influenced by broader national e-health development being overseen by Health Ministers as part of the National E-Health Strategy (NEHS).

Many members of the veteran community receive all their healthcare through the Department of Veterans' Affairs (DVA), not through the Medicare system. As a consequence they are registered with DVA rather than Medicare Australia and will not be part of the initial dataset used to establish individual healthcare identifiers. However, DVA is working with NEHTA so that all members of the veteran community are automatically assigned an individual healthcare identifier in the same way as individuals enrolled with Medicare Australia. DVA is developing a specific proposal to enable this, and the veteran community will be consulted on this proposal through DVA's established veteran consultation forums.

The development and design of the HI Service has been subject to an overarching and ongoing Privacy Management Framework that draws upon legislation, governance principles, technological solutions and community consultation to consider how privacy can be built into the design of the service [10].

Consultations to date with consumers, healthcare professionals, regulators and other interested stakeholders have identified a number of challenges to implementing healthcare identifiers on a national basis within the current privacy environment. They have also confirmed the need to ensure that confidence in the development and implementation of a national HI Service is supported by legislation, governance, accountability and technology. A wide cross-section of stakeholders has been consulted by NEHTA.

Personal demographic information held by Medicare Australia (including name, date of birth) will be used to assign unique healthcare identifiers to individuals who receive healthcare in Australia. This information has been collected by Medicare Australia for the purpose of administering healthcare benefits programs. To use this information for the new purpose of healthcare identification requires appropriate legislation to comply with Commonwealth privacy and health laws[11].

In November 2008, based on development work by NEHTA in consultation with key stakeholders and governments, COAG agreed that authorising the use of existing personal information held by Medicare Australia to universally assign a healthcare identifier to individuals through Commonwealth legislation is the preferred approach. Other options such as assigning healthcare identifiers on a voluntary basis would create numerous implementation problems and complexities, placing increased burden on healthcare providers and consumers, and resulting in poor uptake.

Limited or inconsistent uptake will mean that many of the efficiency gains for health care providers and important quality and safety benefits for patients will not be realised.

---

10 NEHTA's Approach to Privacy (July 2006) www.nehta.gov.au

11 Medicare Australia's administration of healthcare benefits programs is regulated by the *National Health Act 1953* and the *Health Insurance Act 1973*. These acts include restrictions on how information collected to support administration of these programs is disclosed.

2.2.1 Need for specific enabling legislation

There is broad consensus that specific national e-health initiatives such as healthcare identifiers will require specific enabling legislation in addition to the application of an adequate national privacy framework[12].

Legislation specific to national healthcare identifiers will deal with issues such as the management and operation of the HI Service, assignment of identifiers to individuals and healthcare providers (individuals and organisations), tailored safeguards and limits on the collection, use and disclosure of personal information necessary to operate the service.

Section A of this document proposes a legislative framework for the HI Service.

2.3 Developing a regulatory framework for health information and e-health

Law underpins governance and accountability by defining the purpose of an initiative, defining purposes that are out of scope, setting out rights and responsibilities and where necessary allocating appropriate penalties.

In the e-health context, an appropriate policy and regulatory framework will support improvements in health policy and service delivery through better information sharing, while maintaining privacy and security. This framework should have governance arrangements that will permit flexibility to deal with changes as they emerge.

2.3.1 Health information privacy

Privacy is a fundamental principle underpinning quality healthcare, and Australian's expect their health information to be secure and used appropriately. Health information is traditionally protected by ethical and legal duties of confidentiality such as professional codes of conduct and, more recently, health service providers are subject to health information privacy laws.

The right to privacy is not absolute and in some circumstances it must be balanced with the rights of others and with issues that benefit society as a whole. Well accepted public interest examples include arrangements for mandatory public health reporting, medical and public health research and management of health services. These arrangements are clearly set out in legislation in line with the community expectation that any exceptions to health privacy protections are well considered and transparent.

Consumer's trust that their sensitive personal health information is handled appropriately within the healthcare sector must be maintained with the uptake of new technologies so that consumers can reap benefits from improved information flows at the point of care, knowing that their privacy will still be protected.

Without a clear framework for health information, patients may withhold information important to their treatment, and healthcare providers may be unsure of the circumstances for passing on information to other healthcare providers, even though this may be beneficial for coordinating a patient's healthcare.

---

12 Australian Law Reform Commission, *Review of Australian Privacy Law - Discussion Paper 72*, September 2007 and ALRC 108, *For Your Information: Australian Privacy Law and Practice*, August 2008

A number of major reviews of the *Privacy Act 1988* (Cth) (Privacy Act) have made recommendations about regulating health information. These include the Office of the Federal Privacy Commissioner, *Getting in on the Act: The Review of Private Sector Provisions of the Privacy Act 1988* (2005); the Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005); and the Australian Law Reform Commission (ALRC), *For Your Information: Australian Privacy Law and Practice (Report 108)* (2008).

The 2008 ALRC privacy report contained 295 recommendations, many of which focused on the simplification and streamlining of privacy arrangements across Australia. A key ALRC recommendation is the development of a consistent national privacy framework and adoption of a single set of high- level privacy principles (the Unified Privacy Principles or UPPs) covering all types of personal information, including health information.

Safeguards and arrangements for health information reflected in many current arrangements would continue, such as:

- the general requirement to obtain consent from the individual about how their health information is handled or to only use that information for directly related reasons that the individual would reasonably expect
- ensuring relevant health information is available where this is needed to provide health services to individuals or to lessen serious threats to health, life or safety
- ensuring patients have a right to access their own personal health information in a safe and effective way
- ensuring that important quality assurance, monitoring, planning and health service management activities can be undertaken efficiently and effectively.

Current problems can also be addressed such as to ensure that patients can access their medical records for ongoing treatment purposes when a healthcare practice closes or is sold or if the patient changes healthcare providers and ensure comprehensive family and social medical histories can be collected by healthcare providers in the course of providing treatment.

The ALRC noted that the collection of health information into electronic systems and the use of electronic systems to share information among health providers do not raise new or unique issues. In general, these systems do not require specific legislative control provided privacy principles remain technology neutral.

In general terms, the recommendations made by the ALRC seek to continue the high level of consumer control over, and protection for, health information reflected in current Commonwealth and state and territory privacy arrangements. If common arrangements are implemented on a national basis it is expected that there will also be greater clarity for healthcare consumers and providers about how these protections apply in practice and when it is appropriate to share information for healthcare and other public interest purposes.

Section B of this document sets out a number of additional proposals to those put forward by the ALRC to ensure that Australia's national privacy framework provides clear and practical guidance to support healthcare delivery either in paper or electronic environments.

PART A: NATIONAL HEALTHCARE IDENTIFIERS AND REGULATORY SUPPORT PROPOSALS

A.1 The approach

Commonwealth, state and territory health ministers are committed to working together to enable an e-health environment that will provide Australian health consumers with immediate improvements to patient care.

The release of the Australian Health Ministers' *National E-health Strategy* in late 2008 confirmed the fundamental importance of an identification and authentication regime as a foundation for e-health.

Progressing the development of national e-health systems requires:

- developing, implementing and operating systems for an individual consumer health identifier and healthcare provider identifiers for individuals and organisations using agreed terminologies; and
- promoting compliance with nationally-agreed standards in future government procurement related to electronic health systems and in areas of healthcare receiving government funding.

A.2 Healthcare identification – the problem

Australia's healthcare system has no single method of accurately and reliably identifying healthcare individuals, healthcare providers or organisations.

GPs, clinics, pharmacies, pathology laboratories, private and public hospitals all have separate and different methods and systems to identify patients.

The Medicare numbers printed on Medicare cards are not suitable for use as a patient identifier because they are not unique (family members are often on the same card) and are designed to assist in demonstrating eligibility for, and payment of, medical benefits rather than unique identification of individuals receiving healthcare services. Further, consumers who are not eligible or not registered for Medicare benefits do not have a Medicare card.

Similarly, Medicare provider numbers are allocated to individual providers and a range of numbers are allocated to organisations to support payments and claims through government schemes including, but not limited to, the Medicare Benefits and the Pharmaceutical Benefits Schemes. Health service providers who are not eligible to bill Medicare may not have a Medicare Australia issued provider number. Moreover, the format of the Medicare numbers was not intended for use in the electronic environment as an identifier.

Healthcare provider information is stored across multiple information directories, maintained by various registration bodies, private medical imaging, pharmacy and pathology services and public and private hospitals, making it difficult to locate individual providers. Many healthcare providers work for more than one organisation at the same time, making it difficult to send patient information to the right service location (e.g. a specialist may work in a hospital and a private practice).

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. These problems include:

Preventable errors

- Up to 18 per cent of medical errors are attributed to inadequate availability of patient information.[13]
- Medication prescribing errors are estimated to cost $380 million per year in the public hospital system.[14]

Reduced productivity

- 25 per cent of a clinician's time is spent collecting information[15]. Current health information systems are disjointed which often results in healthcare providers operating with incomplete or incorrect information[16].

Costly misuse of resources

- 17 per cent of referrals to hospitals could be avoided by improved communication of health information.[17]

A.3 What is being developed to improve healthcare identification?

A national approach to healthcare identification involves building foundation infrastructure, including a HI Service. The Service will assign, issue and maintain three sets of unique healthcare identifiers for individuals, individual healthcare providers and healthcare organisations.

1. Individual Healthcare Identifiers (IHIs) will increase the integrity of identification of electronic health information records and communications. They will enable accurate retrieval, discovery and recording of health information as part of delivering healthcare. Each individuals receiving consumer of health services in Australia will have a unique IHI.

---

13 Thom Rubel, *Electronic Health Information: The Key to Evidence-Based Medicine and Improved Patient Care*, Government Insights White Paper, sponsored by BEA/Oracle, October 2008, p.6.
14 Australian Institute of Health and Welfare, *Australian Hospital Statistics 1999-00* (2002a).
15 Audit Commission, *For Your Information: a study of information management and systems in the acute hospital*, London, HMSO (1995).
16 National Health and Hospitals Reform Commission, *Person-controlled Electronic Health Records*, 20 April 2009
17 GJ Elwyn & NCH Stott, *Avoidable Referrals? Analysis of 170 connective referrals to secondary care*, BMJ 309, 3/9/1994

2. Healthcare Provider Identifiers- Individual (HPI-Is) will accurately identify the people involved in providing healthcare. They will enable accurate transmission of communications between healthcare providers and more accurate identification of who accesses or otherwise handles an individual's health information. HPI-Is will also support development of a directory style listing of provider details. Having a HPI-I will be a pre-requisite, in combination with an organisation identifier, to accessing national e-health infrastructure and participating in national e-health services. They are also expected to be used in local electronic health information systems.
3. Healthcare Provider Identifiers - Organisation (HPI-Os) will accurately identify the locations where healthcare is provided. They will enable accurate transmission of communications between healthcare provider organisations, and support development of a directory style listing of healthcare organisation details. Having a HPI-O will be a pre-requisite to accessing national e-health infrastructure and participating in national e-health services. They are also expected to be used in local electronic health information systems.

The Healthcare Provider Identifiers (HPI-Is and HPI-Os) on their own will not provide enough information to authorise access to national electronic health information systems. A National Authentication Service for Health (NASH) is also being designed by NEHTA to provide a Public Key Infrastructure (PKI) system for the health sector. The service will issue digital certificates and tokens (e.g. smartcards) to individual and organisational healthcare providers. As part of its functions, NASH will provide the appropriate e-authentication of healthcare providers and healthcare organisations to enable them to access the HI Service.

Healthcare providers and organisations issued with national healthcare identifiers will have the option of being included on a national Healthcare Provider Directory. The Healthcare Provider Directory Service (Directory Service) will enable the search and location of healthcare providers and facilitate communication and information exchange between them, such as referrals, test orders and results.

Each of the three healthcare identifiers will be a unique 16-digit number that complies with International Standards Organization requirements and Australian standards for healthcare identifiers.[18] They will not replace Medicare numbers, or change the way Medicare and Pharmaceutical Benefit Schemes operate.

Each number will be associated with the minimum amount of personal demographic information required to uniquely identify the individual consumer or healthcare provider or organisation. No clinical information is required or will be maintained by the HI Service.

Once issued, healthcare identifiers may be included as part of:

- electronic health and clinical records – e.g. those created and maintained by healthcare providers and organisations, as well as any future IEHR
- electronic health information transactions – e.g. prescriptions, discharge summaries, referrals, and health test results.

18 *Healthcare Provider Identification* (AS4846 – 2006) and *Healthcare Client Identification* (AS5017 – 2006)

A.3.1 Key design and implementation features of healthcare identifiers

Individual Healthcare Identifiers (IHIs):

- **will be** provided to all individuals who receive healthcare in Australia
- **will not** need to be declared to obtain health services
- **will be** automatically allocated to everyone who is currently enrolled with Medicare Australia in the Medicare program
- **will not** be the identifier on the current Medicare card
- **will be** able to be generated as 'interim numbers' in situations where an individual cannot be identified at the point of care (e.g. emergency situations) or is not entitled to Medicare benefits (e.g. tourists)
- **will be** linked to demographic information contained in Medicare Australia's Consumer Directory Maintenance System (CDMS)
- **will be** able to be accurately and seamlessly retrieved by healthcare providers by use of an individual's Medicare card and number as an initial token. Retrieval of an individual's IHI will be based on an exact match and the use of a token provides significant privacy and efficiency benefits
- **will be** able to be retrieved by healthcare providers via a demographic search where a Medicare card is not available. The demographic search will be based on an exact match using name and date of birth. In some situations, address and sex details may need to be used to obtain an exact match
- **will not** alter the way in which anonymous health services are currently provided
- **will be** 16-digit unique identifiers based on national and international standards.

Healthcare Provider Individual Identifiers (HPI-Is):

- **will be** issued to any individual involved in providing healthcare who requires one[19]
- **will be** used to identify the individual healthcare provider associated with accessing health information and electronic health information transactions and communications
- **will be** issued to an individual healthcare provider through their professional or registration body where one exists, or by the HI Service in circumstances where a professional or registration body does not exist
- **will be** listed with the consent of the individual provider in a Healthcare Provider Directory Service
- **will be** a 16-digit unique identifiers based on national and international standards
- **will not** provide automatic access to the Identifiers Service on its own
- **will be** linked with an identified Healthcare Provider Organisation in order to obtain access to the HI Service.

---

19 Initial allocation of HPI-Is will be to healthcare professionals registered on a national basis through the National Registration and Accreditation Scheme (NRAS) and will occur automatically as part of the registration process. NRAS is expected to register approximately 400,000–500,000 healthcare professionals. Over time, allocating HPI-Is will be extended to all healthcare providers as required.

Healthcare Provider Organisation Identifiers (HPI-Os):

- **will be** issued to any organisation that employs or contracts one or more health providers or sole trader that provides a health service
- **will be** issued when an organisation signs a participation agreement with the HI Service
- **will be** listed in a Healthcare Provider Directory Service
- **will be** required, together with an HPI-I, to access the HI Service.

A.4 Benefits of a Healthcare Identifiers Service

Mismatching of patients with their records and results is a documented problem for the health system and a clear link has been established between avoidable harm to patients and poor medical records management [20].

If healthcare providers can accurately and confidently identify the individual they are treating and communicate with providers who have treated or are treating that person they may be able to:

- find details of previous care related to the current healthcare event
- more reliably communicate with each other both electronically and manually.

Over time, healthcare consumers may have improved portability of their clinical records.

The IHI will establish the means by which all individuals receiving healthcare in Australia can be uniquely identified within the healthcare system. The healthcare provider identifiers (HPI-I and HPI-O) will establish the means by which healthcare providers and organisations in Australia can be accurately and uniquely identified.

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

Removing technological and organisational impediments to the effective sharing of health information, such as poor patient and provider identification, will result in:

- more secure, convenient and coordinated interactions across the many different parts of the health system
- better consumer access to health information
- more informed and efficient care and treatment decision-making by healthcare providers
- better understanding of what is happening in the health system and more informed population health surveillance, policy development, service planning and management.

Strong privacy and security protections and policies will continue to underpin how health information is handled. Secure electronic systems provide opportunities not present in current paper based and fragmented electronic information systems to improve patient privacy and accountability for information management.

---

20 Australian Commission on Safety and Quality in HealthCare, *Windows into Safety and Quality in Health Care 2008*, p 15.

A.5 Proposed legislative support for the Healthcare Identifiers Service and associated personal information flows

If consumers and providers are to actively participate in e-health systems, including the HI Service, there must be a high level of trust and confidence in their operation. Legislation that provides clear, transparent and flexible oversight of the operation of e-health systems as they develop and evolve is required, supported by administrative and technological processes. This section outlines key legislative requirements for the operation of the HI Service. Arrangements for governance of the HI Service are discussed at Section A.6.

Healthcare identifiers will be included with the health information of individuals. For this reason, it is appropriate that the handling of these identifiers be subject to existing health information privacy laws. This section discusses where additional legislation is required to establish the HI Service Operator and set out rights and responsibilities of health sector participants and individuals who use the service.

Your feedback is sought on whether the proposals for legislation:

- **are fit for purpose and support the objectives of the HI Service**
- **will raise any significant issues for stakeholders if they are implemented as proposed**
- **need modifying or adding to in order to support implementation of the HI Service and participation by individuals, healthcare providers and healthcare provider organisations.**

Additional questions for healthcare provider organisations:

- **What impact do you consider that participation in the HI Services would have on your current business practices? Please include both positive and negative impacts.**
- **In light of the legislative proposals to support the establishment and operation of the HI Services, do you consider that significant changes would need to be made to your current business practices should you choose to participate?**
- **Do you consider that these changes would be a substantial cost for you to incur, financial or otherwise? If so, do you see the potential benefit of participating outweighing the cost?**

A.5.1 The Healthcare Identifiers Service Operator

To establish the HI Service, a body must be allocated the role of operating the service. The HI Service Operator will have a range of functions in relation to IHIs, HPI-Is and HPI-Os.

It is proposed that the key functions of operating of the HI Service will be to:

- assign IHIs to individuals
- collect and adopt HPI-Is that are issued to providers through trusted data sources, such as professional or registration bodies, together with associated identifying information

- assign HPI-Is to other providers where no trusted data source exists,
- assign HPI-Os to provider organisations
- maintain the IHI, HPI-I and HPI-O datasets
- disclose IHIs and HPI-Is for authorised purposes to authorised users
- respond to complaints and inquiries about the HI service.

More specifically, it is proposed that the HI Service Operator will need to:

- be responsible for managing personal and other information about Australian healthcare consumers (the IHI, approx. 20 million) and Australian healthcare providers (the HPI-I, approx. 600,000[21]) and healthcare provider organisations (HPI-O)
- maintain the service so that it complies with relevant legal requirements, including health information privacy law
- develop and maintain agreed methods, standards, protocols and guidelines for use of the service
- develop and maintain procedures for assignment of identifiers to healthcare providers, organisations and individuals
- develop and maintain mechanisms for users to access their own records and correct or update details
- deal with legal liability issues for any loss or damage arising from participant reliance on inaccurate information
- manage participation arrangements for individuals, providers and provider organisations
- develop and maintain procedures for system audit, financial audit, performance evaluation and compliance with legislation
- provide feedback to strategic and regulatory oversight bodies regarding outcomes, compliance and design issues
- respond to enquiries and complaints (in the first instance) from participants about the HI Service and its operation
- ensure appropriate involvement of identified stakeholders, through agreed consultative mechanisms.

Initial establishment and operation of the HI Service will also require the use of personal demographic information that has been collected by Medicare Australia for the purposes of administering healthcare benefits programs.

To ensure sufficient protections and public confidence in the HI Service it is considered necessary for the operation of the Service to be undertaken under statutory arrangements that provide a similar level of accountability and scrutiny as apply to Medicare Australia. This could be achieved by establishing a new statutory authority or agency or by allocating the functions to an existing statutory authority or agency.

In considering whether a new body should be established, the extent to which there are synergies with any existing body and compatibility with existing functions has been considered.

---

21 Australian Institute of Health and Welfare *Australia's health 2008*, 24 June 2008, Table 8.23.

Because Medicare Australia's existing information and service infrastructure is being used to establish the individual and healthcare provider identifiers and because of its experience and trusted status in delivering national health related services to providers and consumers, it is proposed that Medicare Australia will be the initial HI Service Operator. It is intended that this decision will be reviewed by Health Ministers once the HI Service is fully operational and to take account of further national e-health developments.

All jurisdictions have an interest in ensuring that the HI Service supports health policy and service delivery functions. It is proposed that the interests of jurisdictions would be ensured through proposed governance arrangements. Consumer and healthcare provider confidence in the operation of the HI Service will be supported through arrangements for independent regulatory oversight. Further details of the proposed national governance arrangements for the HI Service are set out at Section A.6.

Medicare Australia is a statutory agency and can only undertake functions assigned to it by or under law. It will be necessary for the scope of the functions listed above to be provided for in legislation. Specific authorisation will be provided for Medicare Australia to use information collected for the purposes of administering healthcare benefits programs for assigning identifiers.

Proposal 1: Provide Medicare Australia with functions, in or under Commonwealth legislation, to establish and operate the HI Service for the purpose of accurately and uniquely identifying healthcare individuals, healthcare providers and provider organisations and enable communication between individuals, healthcare providers and provider organisations.

The functions would be conferred on the Chief Executive Officer of Medicare Australia and cover:

- assigning, collecting and maintaining identifiers to individuals, individual healthcare providers and organisations including by using information it already holds for existing purposes
- developing and maintaining mechanisms for users to access their own records and correct or update details
- collecting information from individuals and other data sources
- use and disclosure of these identifiers and associated data, including personal information, for the purposes of operating the HI Service.

Key Stakeholder Questions about providing functions to operate the HI Service:

Q1. Do you agree that the functions to be conferred on the Medicare CEO are sufficient?

A.5.2 Regulatory support for activities to be undertaken by the HI Service Operator and health sector participants

Activities that are undertaken by the HI Service Operator and those authorised to use the HI Service will involve the handling of personal information about individuals and individual healthcare providers. The individual and individual healthcare provider identifiers (IHIs and HPI-Is) will also be Commonwealth assigned unique identifiers, which are regulated by privacy law. The identifier for healthcare provider organisations (HPI-Os) will involve collection and handling of business rather personal information and application of privacy laws is not expected to be relevant. The HPI-O will not be a unique identifier subject to privacy law.

A.5.2.1 Application of general privacy and other laws

The way in which personal information and health information is collected, used or disclosed is currently regulated by privacy laws that have been put in place by Commonwealth, state and territory governments. To require health information that is accompanied by a healthcare identifier to be subject to additional restrictions would impose a further layer of complexity to the already complex patchwork of privacy legislation. It may also inadvertently restrict or impede the appropriate handling of health information in providing healthcare to individuals.

It is intended that where an IHI or an HPI-I is included with an individual's health information it will be treated in the same way as that health information by healthcare organisations.

The collection, use and disclosure of personal information by private sector healthcare organisations will continue to be subject to the Privacy Act. State or territory privacy laws will continue to apply to their public sector healthcare providers.

In some jurisdictions public health sector privacy arrangements have been put in place through administrative arrangements, specifically in South Australia and Queensland[22]. In Western Australia there are no specific privacy arrangements for the public health sector.[23]

These laws and arrangements operate in conjunction with health information requirements that are set out in other legislation, including health records legislation and other obligations, such as confidentiality.

To determine the extent to which additional legislative support is required beyond that provided through existing health privacy laws and administrative arrangements, the proposed information flows associated with the HI Service have been mapped against general privacy requirements.[24]

Proposal 2: Where an IHI or HPI-I is associated with health information about an individual, the collection, use and disclosure of an IHI or an HPI-I will be subject to the privacy and health information laws applicable to that health information.

Misuse of an IHI or HPI-I by a healthcare provider will be able to be pursued as a breach of privacy in jurisdictions with privacy laws or will be subject to other penalties set out in relevant health records or health service legislation.

Key stakeholder questions about application of general privacy and other laws:

Q2. Are there significant issues raised by regulating the handling of healthcare identifiers by public and private health sector organisations through existing privacy and health information laws with some additional regulatory support through specific enabling legislation for healthcare identifiers?

Q3. Are there circumstances where penalties for misuse of a healthcare identifier and associated information that is held by a healthcare provider will be inadequate?

22 On 19 May 2009, the Information Privacy Bill 2009 was introduced in Queensland. The Bill sets out privacy principles for the handling of personal information in the public sector in Queensland.

23 In March 2007, the Information Privacy Bill 2007 was introduced in Western Australia. The Bill sets out Health Privacy Principles for the handling of health information by public and private sector organisations.

24 Key requirements of the National Privacy Principles (NPPs) set out in the *Privacy Act 1988* (Cth) have been used as the basis for mapping privacy requirements of the Identifiers Service. These requirements are generally common to privacy principles set out in state or territory laws. There are differences, however, that have not been specifically mapped in this analysis.

A.5.2.2 Definitions

Healthcare identifiers are to be used to by individuals and organisations involved in providing healthcare services to ensure the integrity and accuracy of records of patient information and in the communication of health information in connection with treatment of the patient.

To support the allocation of identifiers it will be necessary for the healthcare providers who will be using the identifiers to be clearly defined.

Privacy legislation has addressed the same issue in providing protection for the privacy of health information by defining the term 'health service'. In amendments to the Privacy Act recommended by the ALRC, this term is defined as:

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the service provider to:

(i) assess, predict, maintain or improve the individual's physical, mental or psychological health or status;

(ii) diagnose the individual's illness, injury or disability; or

(iii) prevent or treat the individual's illness, injury or disability or suspected illness, injury or disability;

(b) a health-related disability, palliative care or aged care service;

(c) a surgical or related service; or

(d) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

In Part B of this document it is also proposed that the term 'health service provider' be defined as:

An organisation that provides health service to the extent that it provides a health service.

It is expected that the definitions of healthcare service and healthcare service provider in identifier legislation will be similar to those that apply to health information under privacy law.

Not all specific process requirements are expected to need to be set out in legislation. The HI service operator will have authority to undertake appropriate administrative steps that are necessary for the administration of the HI Service, such as establishing the processes under which a healthcare provider might seek an identifier.

Proposal 3: Definitions of healthcare service and healthcare service provider will be included in the legislation.

Key stakeholder questions about definitions:

Q4. Is it appropriate that definitions contained in privacy law are adopted?

Q5. Are there other specific terms that should be defined?

A.5.2.3 Collection

Privacy principles provide that collection of personal information must be necessary for an organisation to carry out its functions and require lawful authority for that collection.

Additional protection may also apply to the collection of sensitive information, such as health information.

Data collection for IHIs

The IHI Service will use demographic data held within Medicare Australia's Consumer Directory Maintenance System (CDMS). The CDMS currently holds demographic information about approximately 98 per cent of Australia's healthcare consumers, which allows for the majority of IHI numbers and records to be created without having to re-collect this demographic information, or collect additional information, from individuals. Assignment of IHIs will be authorised by legislation and individual consent will not be sought.

In privacy terms this involves the use of existing information by Medicare Australia, in its role as the initial HI Service Operator, rather than a collection (see Section A.5.2.3 below).

Collection of personal information to assign an IHI to an individual will only need to occur in limited circumstances. Where an individual's personal demographic details are not available from the Medicare Australia CDMS (e.g. because the individual is not enrolled in Medicare) only information required for the identification of healthcare individuals will be collected by the HI Service and will include [25]:

- name including title, family name, given name [26]
- date of birth
- date of birth accuracy indicator
- birth plurality (where relevant and for a designated period)
- birth order (where relevant and for a designated period)
- date of death (if applicable)
- date of death accuracy indicator.

Two additional data fields may be collected to assist in identification purposes where a token (e.g. Medicare card or other approved token) is not available. The additional fields are Address[27] and Sex[28].

The function provided to the HI Service Operator (see Proposal 1 above) will authorise the collection of personal information necessary to assign an IHI to individuals. Authorising the use of existing Medicare Australia CDMS information to assign an IHI to individuals is discussed below (see Section A.5.2.3 Use and disclosure)

Data collection for HPI-Is

Any individual healthcare provider in the health sector who needs a persistent, unique healthcare provider identifier (HPI-I) will be issued with one.

---

25 These fields are based on the Australian Standard *Healthcare client identification* (5017-2006)

26 Name includes the following fields: name title, family name, given name, given name sequence number, name suffix, name usage, name usage start date, name suffix sequence number, preferred name indicator, name conditional use flag, name start date and name finish date (if applicable).

27 Address includes the following fields: unit type, unit number, address site name, level number, level type, street number, lot number, street name, street type code, street suffix code, suburb, postal delivery type code, postal delivery number, state, postcode, delivery point identifier, international address line, international state/province, international postcode.

28 Sex includes the following fields; male, female, intersex or indeterminate, not stated/inadequately described.

A HPI-I may be assigned through a healthcare provider's registration body acting as a trusted data source (TDS). At this point registration bodies participating in the National Registration and Accreditation Scheme (NRAS) are recognised as a TDS.

All providers registered with NRAS will be assigned an HPI-I as part of the registration process. This is expected to be underpinned by law and will enable the disclosure and use of the identifier allocated through that scheme for the purposes of the HI Service.[29]

A number of trusted data sources may be utilised by the HI Service although other specific sources are still to be determined.

Demographic and professional information about healthcare providers will be collected by the HI Service Operator via a TDS. Trusted data sources will be the authoritative source for data they supply to the HPI Service, and will be the only party able to modify such data.

In those instances where no TDS exists for a healthcare provider individual, the HI Service Operator will be authorised to collect relevant information and assign a HPI-I to the individual healthcare provider (see Proposal 1).

The HI Service will include mandatory and optional data fields. Only information that is necessary for the purposes of the HI Service will be collected. The collection of the following information will be required to accurately and uniquely identify an individual healthcare provider and assign an HPI-I:

- name
- address
- sex
- date of birth
- provider individual type
- provider individual specialty
- registration identifier
- registration status [30].

The collection of the following information to support a Healthcare Provider Directory Service will be optional:

- business name (that is, the healthcare provider organisation name at which the Healthcare Provider Individual is employed or practices)
- electronic communication details
- provider Individual specialisation
- professional registration start date
- professional registration end date
- date of death (if applicable).

---

29 Legislation to support the NRAS is currently being developed by all Australian jurisdictions. A consultation paper on the proposed arrangements for information sharing and privacy was released for public consultation in November 2008. This outlined the proposals for use of a unique identifier for registration and HPI-I use. Exposure draft legislation further outlining these proposals was released for comment on 12 June 2009. See www.nhwt.gov.au/natreg.asp

30 Please note that the two points referred to as 'Registration Identifier' and 'Registration Status' reference refer to the number allocated through a trusted data source to a registrant (e.g. linked to the individuals type of health profession) and the status of the registrant (e.g. registered or conditional registration) respectively.

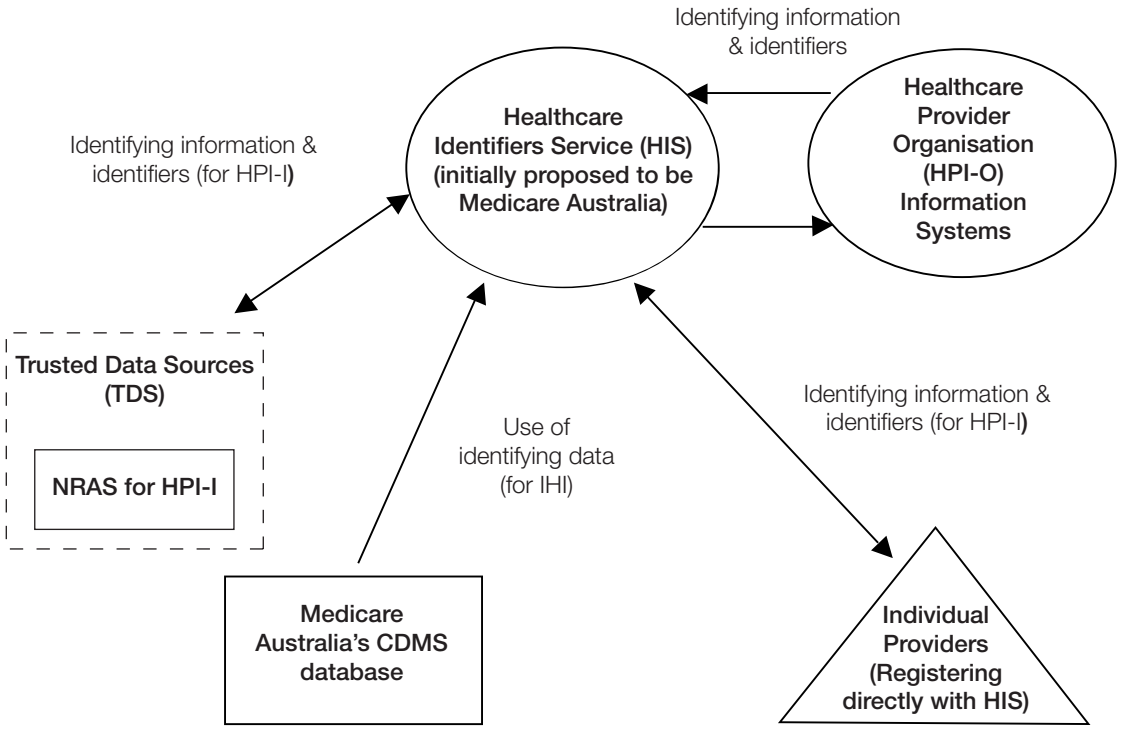
A.5.2.4 Use and disclosure

The use and disclosure principle allows agencies and organisations to use and disclose information they hold for the primary purpose for which it was collected and for authorised secondary purposes. Authorised secondary uses include where the individual consents, where the secondary use is directly related to the primary purpose and the individual reasonably expects the use and other specified public interest purposes.

The key objective of the HI Service is to provide a national capability to accurately and uniquely identify healthcare individuals and healthcare providers to enable reliable communication between healthcare individuals, providers and provider organisations.

Figure 1 below provides an overview of the uses and disclosures of Healthcare Identifiers and associated personal information between the HI Service Operator and healthcare participants.

Figure 1: Information flows – use and disclosure



Note: Identifying data for individuals (IHIs) can include Name, Date of Birth, Address, Sex or subsets of that information. Identifying data for individual healthcare providers (HPI-Is) can include Registration number, Name, Date of Birth, Address (residential and/or business), Provider type and Speciality.

In most circumstances, the amount of identifying information which is disclosed to the HIS will be greater than the identifying information which is disclosed back to the user accessing the HIS. The only new information which will be disclosed to user accessing the HIS will be the identifier itself.

Using and disclosing IHIs

Existing information held in Medicare Australia's CDMS will be used for the purposes of assigning an IHI to individuals. There will be an ongoing link between the CDMS demographic information and the IHI to provide authorised healthcare providers a facility to match the healthcare consumer with the IHI number for healthcare identification purposes and to update common demographic details.

There will be a number of restrictions on the disclosure of identifiers and personal information by the HI Service Operator.

The HI Service Operator will only be able to disclose identifiers and personal information to the extent that this is within the scope of the functions set out in Proposal 1 (see above).

Information held by the HI Service Operator will only be disclosed to individual providers who have an HPI-I and when the information is sought as part of health information management and communication activities undertaken on behalf of an organisation that has an HPI-O.

Searching for an IHI within the HI Service

The disclosure of information by the HI Service Operator will be limited to a number of data fields that are required to achieve the purpose of unique identification. These fields include name, date of birth, IHI number and date of death (if applicable) [31].

The results of a search for an IHI number must be a single exact match. The majority of searches undertaken by healthcare providers to obtain an individual's IHI will use the individual's Medicare card. IHIs will be linked with a healthcare individual's unique Medicare consumer ID in Medicare Australia's CDMS data store. Presentation of a Medicare card by an individual to a healthcare provider will enable the IHI to be looked up on the HI Service by swiping the Medicare card or keying in the Medicare card number.

In cases where an individual does not have their Medicare card with them a demographic search may be conducted. A demographic search will generally use the individual's name and date of birth. The HI Service Operator will not disclose information in response to a request from a healthcare provider that does not include this minimum set of demographic information.

If a single exact match cannot be found using the information provided by a healthcare provider, additional information can be provided until an exact match is located. The additional demographic information that may be provided is address and sex. These fields will not be disclosed by the HI Service Operator in response to a request.

Who will be able to search for an IHI?

It is proposed that a healthcare provider will be identified by an HPI-I and a HPI-O in order to request an IHI from the HI Service.

Staff involved in operating the HI Service will be able to search for an IHI within the Service in order to carry out the Service Operator's functions.

---

31 Other system related data fields may also be disclosed such as a date of birth accuracy indicator.

Using and disclosing HPI-Is and HPI-Os

Individual healthcare provider and provider organisation identifiers and associated information will be used for:

- the accurate identification of the people providing healthcare services and the locations where those services are provided and
- development of a Healthcare Provider Directory Service (the Directory Service) to enable secure communication of health information between healthcare provider individuals and organisations.

Individual healthcare providers will be asked to consent to having their professional and business contact details made available through the Directory Service. The Directory Service will contain a sub set of information held by the HI Service.

Searching for a HPI-I within the HI Service

Individuals nominated by a healthcare provider organisation and who have an HPI-I linked to an HPI-O will be able to search the HI Service to establish a link between the organisation and other individual healthcare providers who perform functions within the organisation.

Staff involved in operating the HI Service will be able to search for a HPI-I within the HI Service in order to carry out its functions.

Healthcare providers with an HPI-I linked to an HPI-O will be able to search the Directory Service to support healthcare communications. The information available to be searched will be limited to relevant business contact and professional details. Sensitive details such as a healthcare provider's home address which may have been collected for identification purposes will not be able to be searched.

The Directory Service may also be used by healthcare provider organisations to help maintain their existing local provider index systems. Some of these existing systems are available to the public to assist them in locating appropriate healthcare services.

Disclosure of HPI-Is and associated personal information for Professional Registration purposes

The range of healthcare professions that are to be covered by the NRAS is expected to be extended over time and will include healthcare providers who have been previously allocated an HPI-I by the HI Service Operator. The HI Service Operator needs to be authorised to disclose the HPI-I and relevant data fields collected for HPI-I purposes to NRAS for registration purposes.

Penalties for unauthorised disclosure

Secrecy provisions currently apply to disclosure of information by Medicare Australia staff in the course of administering other health programs under the *Health Insurance Act 1973* or the *National Health Act 1953*. It is proposed that similar provisions would apply to information obtained in administering the identifiers function. Breaches of the secrecy provisions in the above Acts can lead to civil or criminal penalties ranging to fines of up to $5000 and/or 2 years imprisonment.

Secondary uses

Consistent with the key objective of the HI Service, the use and disclosure principle will allow personal information obtained from the HI Service to be used by healthcare providers for purposes other than the primary purpose. In the health context, the existing privacy regulations provide for a number of secondary use provisions. These secondary use provisions are only allowed if they are authorised. Authorised secondary use provisions include:

- uses and disclosures with the consent of individuals
- secondary use purposes where this is directly related to the primary use and the individual would reasonably expect this use to occur, for example in connection with referrals to a specialist
- for management, funding and monitoring of health services
- for research that is in the public interest
- in lessening or preventing threats to health, life or safety
- other public interest purposes such as law enforcement, and the protection of public revenue.

Guidance on secondary uses of health information by private sector organisations that are permitted under the Privacy Act is available on the website of the Office of the Privacy Commissioner.[32]

Proposal 4: The HI Service Operator will only disclose an individual's IHI and the minimum personal information required to identify an individual to an authorised healthcare provider. Requests for an IHI must be supported by a minimum set of personal information.

Proposal 5: Healthcare providers will be authorised to use or disclose an individual's name, date of birth, sex and address details in order to request an IHI from the HI Service Operator.

Proposal 6: The HI Service Operator will disclose information held in the Service only to authorised users. The term 'authorised user' will be defined in the legislation.

Proposal 7: The HI Service Operator will be authorised to disclose the HPI-I and relevant data fields for professional registration and other purposes to bodies set up in legislation establishing the NRAS.

Proposal 8: Secrecy provisions similar to those set out in the Health Insurance Act or the National Health Act would apply to the disclosure of information by staff in undertaking the HI Service Operator function.

Proposal 9: Existing Commonwealth, state and territory health information regulation and administrative arrangements will apply to secondary uses and disclosures of HI Service information.

32 www.privacy.gov.au

Key stakeholder questions about use and disclosure:

Q6. Do the limits on disclosure set out in Proposal 4 provide adequate protection for an individual's personal information?

Q7. Is the authorisation for healthcare providers set out in Proposal 5 required to provide certainty to healthcare providers, noting that the use or disclosure could occur under existing privacy arrangements as a directly related and reasonably expected secondary use or disclosure of health information?

Q8. Does the limit on disclosure set out in Proposal 6 provide adequate protection for a healthcare provider's personal information?

Q9. Does the proposal to apply secrecy provisions similar to those set out in the Health Insurance Act or the National Health Act provide sufficient protection for personal information held by the HI Service Operator?

Q10. Is there a need to apply a specific penalty to unauthorised use or disclosure of healthcare identifiers by health sector or other participants who hold the healthcare identifier in association with health information?

Q11. Do you agree that existing health information regulation and administrative arrangements will provide sufficient secondary use requirements for organisations handling healthcare identifiers?

A.5.2.5 Data quality

The data quality principle requires that information is accurate, complete and up to date. A data quality framework will be put in place to support the HI Service and ensure that information meets these standards. Key design elements of the HI Service have been developed to ensure data quality of personal information required to support the Service.

Managing data quality for IHIs

The use of existing Medicare Australia information allows for the creation of IHI numbers and records using verified, up to date demographic information that has been subject to Medicare Australia's data quality procedures. IHI numbers created using Medicare's CDMS data will be deemed verified at the point of creation, providing data quality for the IHI.

Medicare Australia's evidence of identity policies will ensure that new IHI records added to the HI Service will undergo verification processes. It is proposed that data quality will also be managed through the use of common core Medicare demographic information. If an individual changes their name with Medicare Australia, the name change will be automatically available to the HI Service. This will minimise the need for individuals to make changes in multiple locations and ensure greater likelihood of maintaining up to date information.

Managing data quality for HPI-Is

Trusted data sources (TDS) will maintain data quality for the HPI-Is in the HI Service. If an individual healthcare provider is registered with a TDS, the HPI-I record will be updated upon notice of a change to information from the TDS. This will ensure that up to date information is maintained in the HI Service and available for use by authorised users.

The HI Service will also implement a standard process for verifying the identity of healthcare providers assigned an HPI-I by the HI Service rather than a TDS.

Proposal 10: Existing Commonwealth, state and territory health information regulation and administrative arrangements will apply to data quality.

Key stakeholder questions about data quality:

Q12. Do you agree that existing health information regulation and administrative arrangements will provide sufficient data quality requirements for organisations handling healthcare identifiers?

A.5.2.6 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. Key design elements of the HI Service have been developed to ensure data security of personal information.

An information security framework will be implemented for the Identifiers Service. The information security framework will:

- minimise the risk of unauthorised access to the Identifier Service and the information it contains
- enable detection of unauthorised information access or modification, and any other breach of information security (including privacy)
- facilitate appropriate response to, and investigation of, any such breaches
- assure the continued availability of HI Service
- provide a means to continually improve security protections (including protection of privacy, confidentiality, integrity and availability).

National Authentication Service for Health (NASH)

Strong authentication mechanisms for healthcare providers are being developed by NEHTA and will provide one of the fundamental building blocks for a national e-health system, as well as providing security credentials for use at the organisational and individual level.

Healthcare providers and organisations will be provided with smartcards or other certificates that will authenticate them for access into local and national e-health systems, including the HI Service. It is anticipated that appropriate authentication services will be ready for operation in conjunction with the HI Service.

Audit logs

The HI Service will have a system log that stores all transactions and access attempts in relation to the IHI or HPI-I record (e.g. the HPI-I and HPI-O and associated information). Mechanisms to allow individuals access to relevant details of the system log for their IHI and HPI-I record will be in place. Requests for access to audit logs may be made by individuals via a web-based portal, or other service channels such as a shop front. An increasing level of detail may be provided where the individual suspects that their record has been accessed inappropriately.

The system log will be regularly audited by the HI Service Operator and may also be subject to independent audit by relevant government regulators.

Use of an IHI or HPI-I within a healthcare provider organisation will be subject to audit arrangements that are in place in that organisation.

Proposal 11: Existing Commonwealth, state and territory health information regulation and administrative arrangements will apply for data security.

Key stakeholder questions about data security:

Q13. Do you agree that existing health information regulation and administrative arrangements will provide sufficient data security requirements for organisations handling healthcare identifiers?

A.5.2.7 Openness

The openness principle ensures that organisations are transparent in their data collection and handling activities. This involves ensuring the policies that govern the collection and handling of personal information are made available to the public. Once the IHI and HPI services are operational, all policies relating to data handling will be available via the online portal to allow easy access for all users.

Proposal 12: Existing Commonwealth, state and territory health information regulation and administrative arrangements will apply to openness.

Key stakeholder questions about openness:

Q14. Do you agree that existing health information regulation and administrative arrangements will provide sufficient openness requirements for organisations handling healthcare identifiers?

A.5.2.8 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. Freedom of information laws also provide an access framework for public sector health services in each state and territory.

Providing access to the HI Service

To provide individuals and healthcare providers with the ability to easily interact with the HI Service, Medicare Australia's customer service channels will be used in the operation of HI Service.

These channels are well established within Medicare Australia and include shopfronts, call centres and mail services. A web-based portal will provide online services for individuals. Individuals will have the ability and opportunity to maintain updated records through these channels both for existing Medicare Australia claiming functions and for healthcare identification functions.

Authorised representatives

Authorised representatives are individuals who have a legal authority to act on behalf of someone else and can include parents and legal guardians.

Individuals may also wish to nominate a family member, friend or carer to be a substitute or assisted decision-maker although no legal authority exists.

The IHI services will use Medicare Australia's well established processes in this area.

Proposal 13: Existing Commonwealth, state and territory health information regulation and administrative arrangements will apply to access and correction. No additional legislative requirements will be developed for access and correction.

Key stakeholder questions about access and correction:

Q15. Do you agree that existing health information regulation and administrative arrangements will provide sufficient access and correction capability for individuals?

A.5.2.9 Identifiers

Organisations create and use identifiers for a wide range of purposes to maintain interactions with large numbers of individuals.

Currently, the Privacy Act prevents private sector organisations from adopting identifiers that have been assigned to individuals by a Commonwealth agency unless they have been authorised to do so by law. There are also restrictions on using or disclosing Commonwealth identifiers other than to meet obligations of the issuing agency. These requirements are set out in National Privacy Principle 7 (NPP 7) of the Privacy Act.[33]

NPP 7 would prevent the adoption, use and disclosure by private sector organisations of IHIs and HPI-Is that are assigned by Medicare Australia in its role as the initial HI Service Operator.

As a large proportion of the Australian healthcare sector is comprised of private sector entities, legal authorisation is required to allow these organistions to use healthcare identifiers for legitimate healthcare identification, health information management and communication purposes.

Medicare numbers

Healthcare providers currently use and disclose Medicare numbers for the purposes of processing medical claims and are entitled to provide these to Medicare Australia to meet their obligations to that agency.

To assign and locate an IHI, Medicare Australia's CDMS database will be searched to find the individual using the individual's existing Medicare number supplied by a healthcare provider organisation. This will involve use and disclosure of a Commonwealth identifier (the Medicare number) by private sector health providers for a new purpose. The use or disclosure of the Medicare number in the private sector is restricted by NPP 7 of the Privacy Act, subject to limited exceptions, or authorisation. Legal authorisation is needed to overcome this restriction.

33 *Privacy Act 1988*, Schedule 3.

Proposal 14: It is proposed that Commonwealth legislation provide that NPP 7 does not apply to the adoption, use and disclosure of the IHI or the HPI-I by private sector healthcare provider organisations for the purposes of accurately and uniquely identifying individuals and individual healthcare providers respectively for health information management and to enable communication between individuals, healthcare providers and provider organisations.

Proposal 15: It is proposed that Commonwealth legislation will provide that NPP 7 does not apply to the use and disclosure of Medicare numbers to Medicare Australia by private sector healthcare provider organisations for the purposes of the retrieval of individual identifiers.

Key stakeholder questions about identifiers:

Q16. Will the proposals to overcome current identifier restrictions on private healthcare providers effectively enable participation in the HI Service?

Q17. Do these proposals raise any significant issues in relation to the handling of identifiers?

A.5.2.10 Anonymity

The anonymity principle promotes the ability for individuals to conduct transactions with organisations and agencies anonymously where that is lawful and practical. Current practice within the healthcare sector allows for treatment and services to be provided to individuals on an anonymous basis. The introduction of IHIs will not affect these arrangements. Key design elements of the HI Service have been developed to ensure data security of personal information held by the service.

Pseudonymity

Within the HI Service, vulnerable individuals (such as victims of domestic violence etc.) will be able to request that a pseudonym is used in connection with their IHI. This will involve issuing a new IHI number and association of that new IHI with a pseudonym and other demographic details. Access and control will be restricted to specified staff of the HI Service Operator.

These arrangements will align with the emerging international standard to support individuals accessing healthcare services using a pseudonym.[34]

In some circumstances healthcare providers will need to have their identities protected. This may include those providers who work in sensitive medical areas, such as family planning clinics or psychiatry.

Work on designing the HI Service to include provisions to protect the privacy of these types of healthcare providers is underway.

Proposal 16: Existing Commonwealth, state and territory health information regulation and administrative arrangements will apply to anonymity.

Key stakeholder questions about anonymity:

Q18. Do you agree that existing health information regulation and administrative arrangements will provide sufficient anonymity requirements?

34 ISO Document ISO/IECTC 215/SC N (Draft) 2006-12-20

A.5.2.11 Trans-border data flows

This principle is designed to limit flows of personal information to jurisdictions without equivalent or adequate privacy protection measures in place. As has been discussed earlier, Australia's current privacy landscape is fragmented and complex.

Under the federal Privacy Act the principle relates to the transfer of information outside of Australia. For state and territory privacy laws it refers to transfers outside of their borders. This is relevant where a state or territory has no privacy law. Differences between states and territories in the definition of health information have also contributed to uncertainty in determining whether another state or territory's privacy arrangements are adequate or equivalent.

There is no direct impact on a state or territory public sector healthcare provider being able to obtain an identifier.

Until common privacy arrangements are put in place in all jurisdictions, organisations subject to state or territory law may be required to consider whether the laws applying to an organisation in another state are comparable or provide adequate privacy protection before the organisation transfers health information or other personal information in which an identifier is embedded.

The establishment of common health information privacy arrangements across Australia, discussed in Part B of this paper, would enable providers subject to state or territory trans-border requirements to be assured that equivalent arrangements apply to other Australian bodies to whom they might transfer health information.

Proposal 17: Existing Commonwealth, state and territory health information regulation and administrative arrangements will apply to transborder data flows.

Key stakeholder questions about transborder data flows:

Q19. Do you agree that existing health information regulation and administrative arrangements will provide sufficient requirements for transborder data flows?

Q20. Does this proposal raise any significant issues in relation to the handling of identifiers?

A.6 Governance arrangements

A.6.1 Background

The HI Service is a key piece of national e-health infrastructure. E-health governance arrangements were considered as part of the National E-Health Strategy endorsed by Health Ministers in December 2008.

The governance structure recommended as part of that strategy is referred to as a guided market model – that is, central coordination in areas of national significance, combined with greater flexibility in areas where the market is positioned to play a role. In addition to proposed legislation and regulatory support for key initiatives, this model also relies on competition and the use of incentives, funding and compliance mechanisms to achieve the desired outcomes.

A.6.2 Key governance functions

E-health governance arrangements must provide for three key governance functions:

- strategic oversight
- management and operation
- independent regulatory oversight.

These functions are described below in relation to the HI Service.

A.6.2.1 Strategic oversight

It is proposed that overall responsibility for the national HI Service will rest with a Ministerial Council of Health Ministers. Strategic oversight of the initiative could be provided through meetings of the existing Australian Health Ministers' Conference (AHMC). In fulfilling these responsibilities, AHMC would be supported by its existing advisory committee, the Australian Health Ministers' Advisory Council (AHMAC).

Key responsibilities will be to determine national policies and strategic direction of the HI Service, including its scope and authorised participants, the required regulatory and institutional arrangements and monitoring of those arrangements to ensure they continue to be suitable.

Possible future expansion of functions

It is anticipated that, over time, some expansion of the currently proposed use of the HI Service may be required, particularly as other local and national e-health services which rely on healthcare identifiers are implemented. The expansion may be of:

- the features of the HI Service, e.g. data fields, search features
- the authorised uses of the HI Service, such as for other purposes related to healthcare or
- authorised users, to enable new agencies or organisations to use the HI Service.

Proposal 18: The role of the Ministerial Council would be set out in an intergovernmental agreement. Key elements would be set out in legislation, including any processes for future consideration by the Ministerial Council about the operation or expansion of functions of the HI Service.

Proposal 19: Establish a process for controlling the expansion of the future uses of the HI Service. This could be done by:

- providing for the Minister who is responsible for the legislation to determine future operation or expansion of the service subject to a requirement to undertake a privacy impact assessment and seek agreement from all state and territory Health Ministers.

Guidelines for the steps to be undertaken would be expected to be set out in the legislation.

A.6.2.2 Management and operation

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

- managing the issue and assignment of national identifiers
- managing access to and use/disclosure of national identifiers
- maintaining records of national identifiers
- managing relationships with participants and relevant data sources
- providing advice and information to the strategic oversight body on the performance of the system
- educating, training and informing healthcare providers and consumers about how the service operates
- responding to system/service complaints and enquiries (in the first instance).

Proposal 20: It is proposed that these functions would be undertaken by Medicare Australia in its role as the initial HI Service Operator (see Proposal 1 above).

AHMC may also decide to establish other consultation or contractual arrangements to ensure that the HI Service meets appropriate service levels to support public and private sector healthcare providers. There will also need to be clear communication or reporting arrangements between the HI Service Operator and other bodies responsible for developing e-health standards and other key infrastructure. At this stage it is not expected that these kinds of arrangements would require legislative support.

Final decisions about the detail of e-health governance arrangements are being developed by all jurisdictions in response to the National E-Health Strategy.

Participation agreements

It is proposed that as part of operating the HI Service participation agreements may be put in place between healthcare provider organisations and the HI Service Operator. It is envisaged that participation agreements would set out the responsibilities of the parties involved in the HI Services. This may include:

- defining the rules of participation, such as setting minimum I.T. security, equipment and data management standards
- establishing the consequences of breaching business rules.

Key stakeholder questions about participation agreements:

Q21. Do you think participation agreements are an appropriate mechanism for setting out the responsibilities of the parties involved (i.e. healthcare provider organisations and the HI Service Operator)?

Q22. If so, do you consider that legislation is necessary to underpin the participation agreements?

A.6.2.3 Independent regulation

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

Key functions include:

- handling complaints from consumers and providers about uses of personal information, with an associated complaints-handling model and appeal process
- monitoring handling of health information, including when associated with healthcare identifiers, through conducting audits or requiring reports to assess compliance with relevant health privacy and enabling legislation
- conducting investigations into certain acts or practices
- applying a range of sanctions or penalties commensurate with the seriousness of a breach including, but not limited to, pecuniary penalties, issuing notices to stop engaging in specific conduct and compelling public apologies
- maintaining a register of individuals and organisations against whom sanctions or penalties have been applied
- developing and issuing codes or guidelines in accordance with policy set by strategic governance bodies
- providing feedback and advice to strategic governance and infrastructure management bodies
- developing and issuing determinations to cover emerging issues
- general oversight powers such as to provide advice, education, and to conduct monitoring activities.

In line with current responsibilities, the Commonwealth Privacy Commissioner will provide independent oversight of:

- the operation of the HI Service by the HI Service Operator (initially Medicare Australia)
- how healthcare identifiers are handled by private sector healthcare providers.

Existing state and territory health services or information regulators will have responsibilities in relation to how healthcare identifiers are used and disclosed within public sector health services.

Proposal 21: It is proposed that existing Commonwealth, state and territory privacy and/or health information regulatory arrangements will apply.

A.7 Other issues

A.7.1 Implementation and transition arrangements

The design and build of the HI Service is expected to be completed by NEHTA and Medicare Australia by mid 2010.

As described in Section A.6, it is proposed that Commonwealth legislation will be put in place to enable the introduction and operation of the HI Service and to set limits on the handling of healthcare identifiers by healthcare organisations. It is anticipated that enabling legislation will be introduced in early 2010, and subject to passage through Parliament, will be in place by mid 2010.

Ideally, to support the use of healthcare identifiers by healthcare organisations on a national basis, common health privacy arrangements would be established by all jurisdictions as part of a national privacy framework. Recommendations made by the ALRC about how to establish a national privacy framework are currently being considered by the Commonwealth, in consultation with states and territories.

Part B of this paper sets out a number of proposed amendments or additions to the ALRC recommendations to support healthcare policy and service delivery.

Until revised privacy arrangements are implemented it is proposed that existing health information regulation and administrative arrangements in all jurisdictions will apply to the handling of healthcare identifiers in addition to specific Commonwealth legislative proposals. Commonwealth privacy law will apply to private sector healthcare organisations. To ensure the HI Service can operate as intended within public health systems there may also be a need for some amendment to state and territory legislation.

Before the HI Service is implemented in full, testing and evaluation of the service may be undertaken by NEHTA and Medicare Australia. These processes may involve the use of identifying information to test the operation of the Service in 'live' scenarios. NEHTA is also exploring collaborative options for undertaking early evaluation of the HI Service in the context of existing healthcare information systems such as discharge summary or referral services.

Consideration is to be given to the way in which the participation of individuals, healthcare providers and provider organisations in testing the operation of the HI Service prior to its full implementation can be undertaken. It is proposed that any testing or evaluation of the HI Service by Medicare Australia prior to introduction of proposed legislation would only be undertaken if it were authorised under a Ministerial Direction issued by the relevant Minister.

PART B: PROPOSED NATIONAL PRIVACY REFORMS

Privacy is recognised as one of the key building blocks needed to provide an effective regulatory framework to support the development and implementation of e-health initiatives.

While information privacy laws address a broader set of issues, clear, common national arrangements are critical to ensure the success of national initiatives including the implementation of unique healthcare identifiers for consumers and healthcare providers.

The ability of existing jurisdiction and sector-based privacy arrangements to adequately protect health information that is shared increasingly between public and private sector providers and across state and territory boundaries is a significant issue not only for national e-health initiatives but also for appropriate health information sharing more generally.[35] Inconsistent regulation results in confusion and undue complexity and adds significant compliance burdens and costs as well as impeding projects in the public interest. Table 1 below provides a summary of the range of different legislative and administrative arrangements in place to regulate the privacy and handling of health information.

Attempts to address this issue began in 2000 with discussion between health officials from all jurisdictions leading to proposals for a National Health Privacy Code. While there was agreement on the content of the code, no consensus was reached on how it would be implemented to achieve uniformity.

Table 1: Current health privacy arrangements

Jurisdiction	Public sector	Private sector
Commonwealth	*Privacy Act 1988* (Information Privacy Principles – IPPs)	*Privacy Act 1988* (National Privacy Principles – NPPs)
New South Wales	*Health Records and Information Privacy Act 2002* (Health Privacy Principles – HPPs)	*Health Records and Information Privacy Act 2002* (HPPs) *Privacy Act 1988* (NPPs)
Victoria	*Health Records Act 2001* (Health Privacy Principles – HPPs)	*Health Records Act 2001* (HPPs) *Privacy Act 1988* (NPPs)
Tasmania	*Personal Information Protection Act 2004*	*Privacy Act 1988* (NPPs)

35 The extent of the issues and difficulties they raise are discussed in the report by the Australian Law Reform Commission (ALRC), *For Your Information: Australian Privacy Law and Practice (Report 108)* (2008)

Table 1: Current health privacy arrangements (continued)

Jurisdiction	Public sector	Private sector
Australian Capital Territory	*Health Records (Privacy and Access) Act 1997* (The Privacy Principles) *Privacy Act 1988* (IPPs)	*Health Records (Privacy and Access) Act 1997* (The Privacy Principles) *Privacy Act 1988* (NPPs)
Northern Territory	*Information Act 2002* (Information Privacy Principles – IPPs)	*Privacy Act 1988* (NPPs)
Queensland	The *Information Privacy Act 2009* was passed by Parliament on 2 June 2009 and will commence on 1 July 2009. The Act sets out privacy principles for the handling of personal information in the public sector in Queensland.[36]	*Privacy Act 1988* (NPPs)
South Australia	Administrative arrangements have been put in place to require all public sector agencies to comply with a set of principles based on the Australian Government IPPs. A code of practice based on the Australian Government NPPs applies to the Department of Health and Department of Families and Communities.	*Privacy Act 1988* (NPPs)
Western Australia	No legislative or formal privacy protection, beyond the common law protection, exists in Western Australia. Policy documents guide the sharing of health information within the public health sector.	*Privacy Act 1988* (NPPs)

There have been a number of major reviews of the Privacy Act (Cth) in recent years which have considered and made recommendations about regulating health information both in electronic and paper form. The most recent of these is by the ALRC, *For Your Information: Australian Privacy Law and Practice (Report 108)* (2008).

In August 2008, the ALRC publicly released the final report of its review. One of the key recommendations is for the development of a consistent national privacy framework and adoption of a single set of high-level privacy principles (the Unified Privacy Principles or UPPs) covering all types of personal information, including health information, supplemented by additional health privacy regulations. In relation to health privacy, the ALRC has included many proposals originally developed as part of the National Health Privacy Code.

The Commonwealth has announced that it will be responding to the ALRC report in a two stage process.[37] The first stage will include UPPs and recommendations relating to credit reporting and health information privacy. The intention is that legislation to implement these reforms will be in place within 12 to 18 months of the release of the final report, ie by mid 2010.

36 The Act sets out principles for the handling of personal information by public sector agencies based on the Commonwealth IPPs, with a set of principles based on the NPPs applying to the Queensland Department of Health.

37 See joint media release by the Cabinet Secretary, Senator, the Hon. John Faulkner and the Attorney-General, Robert McLelland, MP, 11 August 2008 http://www.smos.gov.au/media/2008/mr_262008_joint.html

Consultations have been undertaken by the Australian Government and exposure draft legislation to give effect to the first stage reforms is expected to be released by the end of 2009.

The Australian Government also announced that it would be consulting with state and territory governments about proposals to harmonise Commonwealth, state and territory privacy regulation. These consultations are expected to commence in the second half of 2009.

A number of other jurisdictions are also considering proposals for reform to their privacy arrangements including Western Australia and NSW.

Health Ministers have considered the ALRC recommendations in the context of making recommendations to the COAG about e-health investment and implementation.

They have agreed to the implementation of uniform national health privacy arrangements as part of a national privacy framework by incorporating health-specific principles into the UPPs. However, a number of health specific requirements that would need to be addressed for this to be achieved have been identified.

How a national privacy framework is implemented within each jurisdiction, taking into account current legislative arrangements and reform proposals that are already underway in some jurisdictions, eg Queensland and the Commonwealth will need to be discussed between governments.

Key requirements for national privacy regulation to support e-health and health privacy more generally are set out below.

B.1 A national privacy framework (incorporating health-specific requirements)

Key requirements for national health privacy regulation are:

- recognition of the need to provide specific regulation for health information to appropriately balance the particular sensitivities of this type of information with the benefits of its availability for healthcare and other public interest purposes
- support for national e-health initiatives by a national health privacy framework that is, to the greatest extent possible and appropriate, uniform
- involvement of Health Ministers in decision-making processes in recognition of their responsibility for health policy and service delivery
- implementation of a national health privacy framework in a timeframe that supports national e-health investment and implementation, in particular healthcare identifiers.

These requirements can be addressed through arrangements that are established for implementation of the national framework, its oversight and administration, coverage of the law, definitions that relate to health information and some technical amendments to the UPPs.

Your feedback is sought on the potential impact on people who deliver and receive healthcare of the changes proposed in the areas of coverage, definitions and amendments to the UPPs.

B.1.1 Implementation

B.1.1.1 Health provisions as part of the UPPs

The ALRC recommended that an individual's health information would be regulated through the general provisions of the Privacy Act, and a combination of the UPPs with health-specific regulations to modify or add to those principles.

This recommendation is not supported. The combination of privacy laws with regulations that might add to or modify those principles will add to confusion and uncertainty for providers and patients.

A patient's trust that their personal health information will be protected appropriately is at the core of their relationship with their healthcare provider(s). If patients lack confidence around privacy protection they may not seek treatment or may withhold information, resulting in harm to themselves or others. At the same time the community expects that health information will be shared for important, albeit limited, reasons other than healthcare and that these arrangements will be clearly set out in privacy laws.

To ensure that provisions that affect rights and impose responsibilities are set out in the primary legislation and subject to appropriate parliamentary oversight, Health Ministers have agreed that specific health privacy provisions should be incorporated into the UPPs as opposed to supplementary regulations proposed by the ALRC.

B.1.1.2 National applied law scheme

The ALRC concluded that the most appropriate way to implement the national privacy framework would be to have federal legislation that regulates the handling of personal information in the Commonwealth public sector and the private sector, and state and territory legislation that applies key uniform elements to regulate the handling of personal information in their public sectors.

The ALRC examined two options for rolling out legislation across Australia: through an applied law scheme, using either mirror legislation where a law in one jurisdiction is enacted in similar terms in other jurisdictions; or incorporation by reference, where the law in one jurisdiction is picked up by other jurisdictions.

A decision on how a national privacy framework is implemented is a matter to be decided between all jurisdictions.

To ensure a high level of uniformity is maintained over time, arrangements for modifications to the law (e.g. coordinated control over amendments to the legislation) will need to be established. This would be expected to be provided through the establishment of an intergovernmental agreement (IGA) between jurisdictions.

B.1.1.3 Timeframes

Privacy is a critical dependency for a national approach to electronic health records, in particular the current development and implementation of unique healthcare identifiers for consumers and healthcare providers. Ideally, to provide support, common privacy arrangements would be established by all jurisdictions as part of a national privacy framework. However, national

healthcare identifiers are expected to be rolled out in mid 2010 and this is likely to be ahead of implementation of national privacy arrangements by all jurisdictions.

As noted in section A.7, until revised privacy arrangements are implemented it is proposed that existing health information regulation and administrative arrangements in all jurisdictions will apply to the handling of healthcare identifiers, in addition to specific Commonwealth legislative proposals. There may also be a need for some amendment to state and territory legislation to ensure the HI Service can operate as intended within public health systems. Commonwealth privacy law will apply to private sector healthcare organisations.

B.1.2 National oversight arrangements

The ALRC has recommended that the Standing Committee of Attorneys-General (SCAG) take responsibility for providing oversight for the national privacy framework. In addition it has recommended that Health Ministers be consulted by SCAG only on the proposed supplementary health privacy regulations.

If health privacy provisions are incorporated into the UPPs, as proposed above, the UPPs as a whole will regulate the way in which health information is handled by public and private sector healthcare providers. It is important that health information protections are not compromised in relation to other policy imperatives and that health information privacy provisions continue to support health policy and service delivery activities.

To address these issues and ensure that newly emerging health care issues are able to be responded to appropriately a higher level of involvement of Health Ministers than proposed by the ALRC will be required.

The role of Health Ministers and the extent to which they are to share responsibility for privacy legislative and regulatory decisions that may have an impact on health policy and health service delivery will be discussed by governments.

B.1.3 Administration

The ALRC has recommended that wherever possible, existing Commonwealth, state and territory regulators should be responsible for administering privacy laws (e.g. ensuring compliance with the privacy framework and enforcing compliance). The recommendations contained in the ALRC review for the Commonwealth Privacy Commissioner provide a starting point for jointly developing common requirements for compliance and enforcement between all jurisdictional regulators.

To ensure that privacy laws are applied in a consistent and practical way, national coordination between regulators is needed, particularly in relation to compliance and enforcement of the national framework.

Required modification:

The national legislation should include requirements such as: conciliation being the first step in resolving complaints; an independent administrative or judicial mechanism; the length of time consumers have to lodge a complaint; powers of regulators; and sanctions for breaches of the law by organisations or agencies.

Guidelines including minimum standards are required to ensure that there is a consensus in the way in which privacy laws are to be applied across Australia. Jurisdictional regulators would need to determine a common approach to applying these minimum standards. Arrangements under which they might coordinate their activities to help achieve a consistent approach to practical application of the laws and compliance and enforcement activities would need to be developed. This might be achieved by establishing a council of privacy regulators. The arrangements for developing or enforcing jointly agreed directions or guidelines may need to be supported by legislation.

Proposal 22: National legislation include requirements such as: conciliation being a critical element in the approach to resolving complaints; an independent administrative or judicial mechanism; the length of time consumers have to lodge a complaint; powers of regulators; and sanctions for breaches of the law by agencies or organisations.

Guidelines including minimum standards be developed and agreed to by regulators to ensure that there is a consensus in the way in which privacy laws are to be applied across Australia.

Jurisdictional regulators be empowered to jointly determine a common approach to applying these minimum standards.

Key stakeholder questions about administration of a national privacy framework:

Q23. Are there any other requirements that should be specified in legislation?

Q24. Is it necessary that arrangements for and enforceability of directions or guidelines that are jointly agreed by privacy regulators to be supported by legislation?

B.1.4 Coverage

The national framework will apply to all personal information, including health information, wherever it is held by a public agency or private sector organisation and whether in paper or electronic form. The framework will apply to the private sector on a national basis and the public sector in each jurisdiction, subject to agreement by states and territories.

As with existing privacy legislation, there will be full and partial exceptions and exemptions from coverage under the proposed law for certain organisations, information and activities as determined by governments. These include exemptions for national security or intelligence services, courts (in relation to their judicial activities) and news media in relation to journalism or news activities.

Where personal information is held by a public sector body, an individual's access to their own information may continue to be available under freedom of information legislation in the respective jurisdiction. However, it is proposed that an individual's access to their own personal information held by Commonwealth agencies will be provided under the Privacy Act.

B.1.4.1 Deceased persons

It is recommended by the ALRC that the national framework apply to the personal information of individuals who have been dead for 30 years or less where the information is held by a private

sector organisation. The personal information of a deceased individual which is held by public sector agencies will continue to be covered by freedom of information and public records legislation in the respective jurisdiction.

Issues raised in response to this recommendation include whether privacy law is the appropriate place in which to protect the information of deceased individuals when other arrangements may provide access to information about deceased persons, or if the protection should be limited to the health information of deceased persons because of its sensitivity and potential relevance to living relatives. Discussion about how the information of deceased persons is protected must be considered in a broader context. However, from a health perspective, if the information of deceased individuals is to be protected, the arrangements established for health information should be the same as the arrangements established for all other personal information of deceased individuals.

Proposal 23: Health information of deceased individuals should be subject to the same protection as other personal information about deceased persons whether this is through privacy law or other arrangements.

Key stakeholder questions about deceased persons:

Q25. Are there any reasons for the privacy of health information about deceased persons to be treated differently to other personal information about them?

B.1.5 Key definitions

To support health service delivery, a number of key definitions are important. These are definitions for: 'personal information', 'sensitive information', 'health information' and 'health service'.

The definitions of 'health information' and 'health service' are intended to be broad enough to cover personal information relating to an individual's health or that is collected about a person accessing a health service, while providing clarity about what constitutes health information or a health service. In order to be health information, such information must also be personal information.

'Sensitive information' is a subset of personal information that includes health information. As some principles apply only to health information while other principles apply to all sensitive information, this term is also critical.

The ALRC has recommended amendments to these terms in the Privacy Act. The definitions of these terms, as amended by the ALRC, are set out in Appendix 2. No change is proposed to the definitions of personal information, sensitive information, health information or health service.

Health Service Provider

There are some specific arrangements that will only be relevant to health service providers, such as the requirements for the transfer of health records or closure of a practice. To support these situations, a definition of 'health service provider' should be included.

Proposal 24: Include a definition of 'health service provider' as

'an organisation that provides a health service to the extent that it provides a health service'.

Key stakeholder questions about definitions:

Q26. Is the proposed definition of health service provider appropriate?

Q27. Are there any other terms that need to be defined to support a health information privacy protection as part of a national framework?

B.1.6 Unified Privacy Principles

The ALRC has recommended that a single set of privacy principles, the UPPs, be adopted on a national basis. The policy intent of each of the UPPs is outlined below and, where necessary, additional health-specific requirements or modifications to the UPPs recommended by the ALRC are proposed. A copy of the UPPs as proposed by the ALRC can be found at Appendix 2.

UPP 1: Anonymity and pseudonymity

This principle imposes an obligation on agencies and organisations to provide individuals with an opportunity, wherever it is lawful, practical and not misleading, to interact in an anonymous or pseudonymous capacity. Although these concepts are intended to apply beyond the healthcare sector, they are a valuable tool in supporting the delivery of healthcare services and handling of health information.

UPP 2: Collection

This principle specifies when agencies and organisations can collect personal information and how this information should be collected. Agencies and organisations are only permitted to collect personal information relevant to their functions and, wherever possible, this information should be collected from the individual to whom the information relates.

This principle also states that where an agency or organisation receives unsolicited information, it must either destroy it, if lawful and reasonable, or choose to keep the information and comply with relevant provisions in the UPPs.

In addition, an agency or organisation must not collect sensitive information unless (UPP 2.5):

(a) the individual has consented;

(b) the collection is required or authorised by or under law;

(c) the collection is necessary to prevent or lessen a serious threat to life or health of an individual;

(d) the information is collected by a non-profit organisation in the course of their activities and relates to their members;

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim;

(f) the collection is necessary for research in the public interest; or

(g) the collection is necessary for the purpose of a confidential alternative dispute resolution process.

Required modifications to UPP 2:

Addition to 2.5(c) to allow the collection of sensitive information where there is a serious threat to an individual's welfare: The exception under UPP 2.5(c), to allow collection where there is a serious risk only to 'life or health', does not provide the certainty needed by agencies and organisations who regularly assist some of the most disadvantaged members of the community (e.g. the homeless), to determine when they can collect sensitive information including health information to provide assistance. In most instances consent to collect this information will be obtained but in situations where there is a degree of urgency it should be clear that agencies and organisations are able to collect sensitive information to assist that individual or others, such as family members, to provide for their welfare. This rationale is also applicable to the similar exception to the Use and Disclosure Principle (UPP 5).

Deletion or modification to 2.5(d) to exclude the right for a non-profit organisation to collect health information about its members: It is not clear why non-profit organisations should be subject to different and lower requirements than other agencies or organisations when collecting sensitive information.

Modification to 2.5(f): Where the collection of sensitive information is necessary for research purposes, it must meet certain other specified conditions including that the purpose cannot be served by collection of information that does not identify the individual and it is unreasonable or impracticable to seek consent. In addition, the collection must comply with any guidance issued by the Privacy Commissioner. To ensure the specific needs of the healthcare sector are taken into account, the paragraph should specify that guidance issued by the Privacy Commissioner for this purpose should be developed in conjunction with input from other appropriately qualified individuals or organisations in the field of research. This rationale is also applicable to the similar exception to the Use and Disclosure Principle (UPP 5).

Additional collection exception (ALRC health regulations proposals): The ALRC has recommended that the Privacy Commissioner be empowered to issue rules that would need to be complied with by an agency or organisation where it is necessary to collect identifying health information for the purposes of funding, management, planning, monitoring or evaluation of a health service and consent is not obtained. Not all jurisdictions agree that advice issued for these activities should be binding, preferring development of guidelines rather than rules. To ensure that these rules or guidelines provide a balance between privacy and the needs of the health sector, they should be developed in conjunction with input from other appropriately qualified individuals or organisations in the health service management field. This rationale is also applicable to the proposed amendments to the exception to the Use and Disclosure Principle (UPP 5).

Proposal 25: Amendment of 2.5(c) to allow the collection of sensitive information where there is a serious threat to an individual's welfare.

Proposal 26: Deletion or modification to 2.5(d) to exclude the right for non-profit organisations to collect health information about their members.

Proposal 27: Amendment of 2.5(f) to provide that any guidance issued by the Privacy Commissioner in relation to the collection of sensitive information necessary for research purposes be required to be developed in conjunction with input from other appropriately qualified individuals or organisations in the field of research.

Proposal 28: Any rules or guidelines issued by the Privacy Commissioner in relation to the collection of identifying health information where it is necessary for the funding, management, planning, monitoring or evaluation of a health service be developed in conjunction with input from other appropriately qualified individuals or organisations in the health service management field.

Key stakeholder questions about UPP2 - Collection:

Q28. Do you agree that the amendments proposed above are appropriate?

Q29. Are there any other circumstances where the collection principle might require amendment in relation to health information?

UPP 3: Notification

This principle requires agencies and organisations to make individuals aware of circumstances where the agency or organisation has collected personal information about that individual. Notification is intended to inform the individual about specific things including why the information was collected, their right of access and potential disclosures to other organisations. As this increases consumers' awareness and control over how their information is used, it is appropriate for health information.

UPP 4: Openness

This principle requires agencies and organisations to develop and make publicly available a privacy policy which outlines their personal information-handling practices. This ensures a degree of transparency in their information-handling practices and enables consumers to make informed choices about who they disclose their personal information to. The principle is appropriate for health information.

UPP 5: Use and Disclosure

This principle covers when an agency or organisation can use and disclose personal information it has collected. Essentially, agencies and organisations can only use or disclose sensitive information (such as health information) for the primary purpose for which the information was collected unless (UPP 5.1):

(a) the secondary purpose is directly related to the primary purpose of collection and the individual would expect the use or disclosure of the information for the secondary purpose;

(b) the individual has consented;

(c) there is a reasonable belief that the use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety or to public health or safety;

(d) there is reason to suspect that unlawful activity has been or is being engaged in and the use of disclosure of the information is a necessary part of an investigation;

(e) the use or disclosure is required or authorised by or under law;

(f) there is a reasonable belief that the use or disclosure is necessary for an enforcement body to carry out functions;

(g) the use or disclosure is necessary for research purposes; or

(h) the collection is necessary for the purpose of a confidential alternative dispute resolution process.

Required modifications to UPP 5:

Addition to 5.1(c): To allow the use or disclosure of sensitive information where there is a serious threat to an individual's welfare. As with collection exception 2.5(c), including provision for information to be used or disclosed where there is a serious threat to welfare will provide clarity to agencies and organisations handling health information in these circumstances.

Modification to 5.1(g): As with the collection exception 2.5(f), where the use or disclosure of sensitive information is necessary for research, it must also meet specific conditions including that the purpose cannot be served by collection of information that does not identify the individual and it is unreasonable or impracticable to seek consent. In addition, the collection must comply with any guidance issued by the Privacy Commissioner. This guidance should also be developed in conjunction with input from other appropriately qualified individuals or organisations in the research field.

Additional exception (ALRC health regulations proposals): As with the additional collection exception, the ALRC has recommended that the Privacy Commissioner be empowered to issue rules that would need to be complied with by an agency or organisation where it is necessary to use or disclose identifying health information for the purposes of funding, management, planning, monitoring or evaluation of a health service and consent is not obtained. Not all jurisdictions agree that advice issued for these activities should be binding, preferring development of guidelines rather than rules. To ensure that these rules or guidelines provide a balance between privacy and the needs of the health sector, the rules should be developed in conjunction with input from other appropriately qualified individuals or organisations in the health service management field.

Additional exception: It is proposed that an exemption to allow personal information to be used or disclosed where an individual is known or suspected to be missing or deceased be included. This would provide greater clarity to agencies and organisations as to when the health information it holds can be used and disclosed in these types of circumstances. It is proposed that this exception be limited to circumstances where the use or disclosure is not contrary to any wishes expressed by the individual before they went missing or became incapable of consenting and disclosure would be limited to a law enforcement officer for the purposes of ascertaining the whereabouts of the person.

Proposed modification to defining authorised representatives: In addition to the other provisions of the Use and Disclosure Principle, the ALRC has proposed that an agency or organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual ('authorised representative'), if the individual is incapable of giving consent.

The concept of an authorised representative is particularly valuable in the context of health service delivery. Healthcare consumers are often supported by other people when accessing healthcare services and it is important that the provisions put in place are flexible enough to support the types of arrangements regularly encountered in the health sector, such as a neighbour or friend collecting a medical prescription.

Proposal 29: Amendment of 5.1(c) to allow the use or disclosure of sensitive information where there is a serious threat to an individual's welfare.

Proposal 30: Amendment of 5.1(f) to provide that any guidance issued by the Privacy Commissioner, in relation to the use or disclosure of sensitive information is necessary for research purposes, be required to be developed in conjunction with input from other appropriately qualified individuals or organisations in the field of research.

Proposal 31: Rules or guidelines issued by the Privacy Commissioner in relation to the collection of identifying health information where it is necessary for the funding, management, planning, monitoring or evaluation of a health service be developed in conjunction with input from other appropriately qualified individuals or organisations in the health service management field.

Proposal 32: An exception is proposed to allow personal information to be used or disclosed by an agency or organisation where an individual is known or suspected to be missing or deceased, subject to this not being contrary to any wishes expressed by the individual before they went missing or became incapable of consenting, with disclosure limited to a law enforcement officer for the purposes of ascertaining the whereabouts of the person.

Proposal 33: It is proposed that the definition of a 'person responsible for an individual' be altered to provide for:

- any person who has a personal relationship with the individual rather than only a person who has an intimate relationship, or
- a person who is responsible for providing support or care to the individual rather than only the person who is primarily responsible.

Guidelines could identify the grounds on which a personal relationship exists or that a person is responsible. These would include such things as whether there is a sufficient degree of intimacy or level of responsibility. Another alternative would be to set the list up as an inclusive rather than an exclusive list.

Key stakeholder questions about UPP5 – Use and disclosure:

Q30. Do you agree that the amendments proposed above are appropriate?

Q31. Are there any other circumstances where additional guidance about the use or disclosure of information would be helpful?

Q32. In relation to Proposal 32, should an agency or organisation be required to have a reasonable expectation that the person responsible for the individual will act in the best interests of the individual in receiving that information? Would guidelines provide sufficient certainty?

UPP 6: Direct marketing (organisations only)

The ALRC has recommended that an organisation may use or disclose personal information, including health information, about their existing customers (aged 15 years and over) for direct marketing purposes provided the individual would reasonably expect the information to be used for this purpose and the organisation provides customers with a simple method to opt-out of

future direct marketing communications. Health information about customers aged under 15 or any new customers could only be used or disclosed with their consent and the organisation must provide the opportunity to opt-out of the organisation's direct marketing activities.

Given the sensitive nature of health information, healthcare consumers should have an opportunity to choose whether they wish for their health information to be used for direct marketing purposes, regardless of whether they are new or existing customers. In both instances, obtaining consent to use health information for direct marketing purposes should be required.

Proposal 34: The consent of individuals is required to the use or disclosure of health information for direct marketing purposes.

Key stakeholder questions about UPP6 – Direct marketing:

Q33. Do you agree that the consent of the individual should be obtained for the use or disclosure of health information for direct marketing purposes?

UPP 7: Data quality

This principle imposes an obligation on agencies and organisations to take reasonable steps to ensure that the personal information they collect, use and disclose is accurate, up to date and relevant. Ensuring the quality of health information is essential in delivering appropriate and quality healthcare and is strongly supported.

UPP 8: Data security

This principle requires agencies and organisations to take all reasonable steps to protect the personal information they hold from inappropriate use. It also requires agencies and organisations to destroy or ensure that personal information they no longer need is de-identified.

Required modification to UPP 8:

Provision of guidelines outlining key requirements for retaining health information (e.g. minimum retention periods) would provide clarity to agencies and organisations who hold health information, particularly in a national e-health systems environment. In addition, the guidelines should clarify the obligations owed by a healthcare provider to an individual where a healthcare service has been sold, amalgamated or closed. The guidelines should describe how these circumstances are managed to assist healthcare providers to understand what is expected of them.

Records legislation in each jurisdiction may also specify a time period for which records are to be retained.

Proposal 35: Guidelines be developed by the Privacy Commissioner outlining key requirements for retaining health information (e.g. minimum retention periods and obligations owed by a healthcare provider to an individual where a healthcare service has been sold, amalgamated or closed).

Key stakeholder questions about UPP8 – Data security:

Q34. Are guidelines sufficient to ensure that health information is retained for a suitable period of time?

UPP 9: Access and correction

This principle sets out the obligations owed by an agency or an organisation to an individual where the individual wishes to access or correct their personal information held by the agency or organisation. These obligations include:

- responding within a reasonable time and providing access to the information requested, wherever possible
- not charging excessive fees for access where the personal information is held by an organisation
- providing access in the manner requested by the individual, wherever possible
- taking reasonable steps to correct personal information about the individual where it is incorrect, inaccurate or out of date and notifying other entities to whom the information may have been disclosed to
- where a request is refused, providing the individual with reasons for refusing access.

The ALRC has proposed that guidelines be issued by jurisdictional regulators to assist agencies and organisations to comply with this principle.

Access to health information held by public sector organisations may also be able to be accessed under freedom of information legislation in a jurisdiction.

Required modifications to UPP 9:

Exception to the Access and Correction Principle: The exception to providing access to information that would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations should be amended to ensure that negotiations about provision of health services are not included.

Clarification that organisations can provide access to information where it is possible to refuse access: A note should be included explaining that nothing in the principle compels an organisation to refuse to provide an individual with access to his or her health information. This will provide clarity for healthcare providers and organisations by assuring them that, although they may have grounds to refuse access, they may still provide access if they consider it appropriate.

Detailed guidelines: To provide clarity to healthcare consumers and providers about their respective rights and obligations, guidelines that include detailed information about the process which should be followed to gain access to personal information, including guidance on requests for access, responses to those requests, how information is provided, and fees, should be developed.

Proposal 36: It is proposed that the exception from providing access to health information where providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations does not include negotiations about provision of health services.

Proposal 37: A note be inserted into the Access and Correction Principle explaining that nothing in the principle compels an organisation to refuse to provide an individual with access to his or her health information.

Proposal 38: Guidelines be developed by the Privacy Commissioner that include detailed information about the process which should be followed to gain access to personal information, including guidance on requests for access, responses to those requests, how information is provided and fees.

Key stakeholder questions about UPP9 – Access and correction:

Q35. Do you agree with these proposals?

Q36. Are guidelines sufficient to ensure processes for access to health information are understood by agencies and organisations?

Q37. Are any other amendments to the access principle required?

UPP 10: Identifiers (organisations only)

This principle provides that organisations must not adopt identifiers (other than prescribed identifiers) assigned to individuals by Commonwealth, state or territory agencies for their own purposes. In addition, organisations must not use or disclose the identifier unless it is necessary to fulfil their obligations to the agency which assigned the identifier or one of the specified exceptions to the use and disclosure principle applies.

The restriction on the adoption, use or disclosure of identifiers issued by Commonwealth, state and territory agencies is contrary to the ALRC recommendation to allow the collection, use or disclosure of health information for funding, management, planning, monitoring, improvement or evaluation of health services and for research purposes. The restriction outlined in the identifiers principle would prevent use of information where an identifier is included, even if the information does not contain any other identifying details.

Required modification of UPP 10:

To support the appropriate handling of health information, the restriction on adoption, use or disclosure of identifiers should be amended to align with and complement the proposal to allow the collection, use or disclosure of health information for funding, management, planning, monitoring, improvement or evaluation of health services and for research purposes. If this does not occur in the context of the national privacy framework, it is expected that the restriction would need to be addressed in the legislation for the healthcare identifiers.

Proposal 39: The identifier principle should permit the use or disclosure of information that includes an identifier for funding, management, planning, monitoring, improvement or evaluation of health services and for research purposes in the public interest subject to the same limits that apply to health information being used or disclosed for those purposes.

Key stakeholder questions about UPP10 – Identifiers:

Q38. Do you agree with this proposal?

Q39. Are any other situations where the identifier principle might have an inappropriate effect on the use or disclosure of health information?

UPP 11: Cross-border data flows

This principle provides that where an agency or organisation transfers personal information outside of Australia it remains accountable for that personal information subject to limited exceptions. The exceptions include:

- where there is a reasonable belief that the recipient of the information is subject to a similar privacy law, binding scheme or contract
- the individual has consented, or
- the transfer is required or authorised by law.

Required modification of UPP 11:

An exception that allows an agency or organisation to use or disclose information outside Australia to lessen or prevent a serious risk to life, health, safety or welfare and not continue to be liable for any misuse of that information after it is transferred should be included. This would enable healthcare providers to transfer information to assist in overseas treatment without being overly cautious because of the risk of liability if that information were misused.

Proposal 40: An agency or organisation should be allowed to use or disclose information outside Australia to lessen or prevent a serious risk to life, health, safety or welfare without continuing to be accountable for any misuse.

Key stakeholder questions about UPP11 – Transborder data flows:

Q40. Do you agree with this proposal?

Q41. Are there any other exceptions for health information transferred outside Australia?

Appendix 1: Abbreviations, Acronyms and Definitions

Australian Health Ministers' Advisory Council (AHMAC)	The Council providing strategic and operating support to AHMC (see definition below). AHMAC membership comprises the Head (plus one other senior officer) of each of the Australian Government, State and Territory and New Zealand Health Authorities, and the Australian Government Department of Veterans' Affairs.
Australian Health Ministers' Conference (AHMC)	A forum for Australian Government, State and Territory Governments and the Government of New Zealand to promote and discuss health policy issues. AHMC is comprised of all Australian Government, State, Territory and New Zealand Ministers with direct responsibility for health matters, including the Australian Government Minister for Veterans' Affairs are Members of AHMC.
Audit Log	A history of all transactions in connection with a single IHI, HPI-I or HPI-O record
Authentication	The process of using a token, login, or other mechanism to validate access to the HI Service.
ALRC	Australian Law Reform Commission
CDMS	Medicare Australia's Consumer Directory Maintenance System
Council of Australian Governments (COAG)	The peak intergovernmental forum in Australia. COAG comprises of the Prime Minister, the State Premiers, the Chief Ministers of the Australian Capital Territory and the Northern Territory, and the President of the Australian Local Government Association.
Consumer	An individual receiving healthcare services
DVA	Department of Veterans' Affairs
Healthcare Identifiers Service	The Healthcare Identifiers Service (HI Service) will assign, issue and maintain identifiers to individuals, healthcare provider individuals and healthcare organisations.
Healthcare Provider Directory Service	A 'white pages' of Healthcare Providers and Provider Organisations - a provider individual or organisation will only be listed after providing consent for the publication of their details. It does not list Healthcare Individuals, and is not available for viewing by healthcare consumers or the general public.
Healthcare Provider Identifiers	The term to describe two unique identifiers – the Healthcare Provider Identifier for individuals (HPI-I) and the Healthcare Provider Identifier for organisations (HPI-O).

Healthcare Provider Identifier – Individual (HPI-I)	The unique identifier assigned to an individual healthcare provider to identify the individual providers involved in delivering healthcare services.
Healthcare Provider Identifier – Organisation (HPI-O)	The unique identifier assigned to a healthcare provider organisation to identify the organisations involved in delivering healthcare services.
Individual Electronic Health Record (IEHR)	An IEHR is a secure, electronic record of your medical history, stored and shared in a network of connected systems. An IEHR will bring key health information from a number of different systems together and present it in a single view.
Individual Healthcare Identifier (IHI)	The information technology services which will enable the unique identification of health care consumers in Australia.
National Authentication Service for Health (NASH)	A project being developed by NEHTA to deliver the first nationwide secure and authenticated service for healthcare organisations and personnel to exchange e-health information.
National E-Health Transition Authority (NEHTA)	A company established by governments to develop better ways of electronically collecting and securely exchanging health information.
National Registration and Accreditation Scheme (NRAS)	A COAG approved national professional registration and accreditation scheme for health practitioners, which will allow doctors, nurses and other health professionals to practice across State and Territory borders.
Public Key Infrastructure (PKI)	An electronic trust framework to provide Authentication and Confidentiality for online transactions through the use of digital Keys and Certificates.
Standing Committee of Attorneys'-General (SCAG)	SCAG is a national ministerial council. Its members are the Australian Attorney-General and the Minister for Home Affairs, the State and Territory Attorneys-General and the New Zealand Attorney-General. Norfolk Island has observer status at SCAG meetings. SCAG provides a forum for Attorneys-General to discuss and progress matters of mutual interest. It seeks to achieve uniform or harmonised action within the portfolio responsibilities of its members.

Seed Organisation	A senior healthcare provider organisation at the top of an organisational hierarchy or structure. A Seed Organisation is a separate legal entity that will participate in the HPI Services. A Seed Organisation can establish multiple relationships with Networked Organisations.
Trusted Data Source (TDS)	For HPI Services purposes, a specific type of data source external to Medicare Australia which is used to update information within the HI Services. TDSs will be authoritative sources, and the data they supply must meet formatting standards and have the highest standards of quality and accuracy.
Unified Privacy Principles (UPPs)	A set of 11 high level principles for the handling of personal information recommended by the ALRC in its report *For Your Information: Australian Privacy Law and Practice (Report 108)* (2008).

Appendix 2: Model Unified Privacy Principles (UPPs)

UPP 1. Anonymity and Pseudonymity

Wherever it is lawful and practicable in the circumstances, agencies and organisations must give individuals the clear option of interacting by either:

(a) not identifying themselves; or

(b) identifying themselves with a pseudonym.

UPP 2. Collection

2.1 An agency or organisation must not collect personal information unless it is necessary for one or more of its functions or activities.

2.2 An agency or organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

2.3 If it is reasonable and practicable to do so, an agency or organisation must collect personal information about an individual only from that individual.

2.4 If an agency or organisation receives unsolicited personal information about an individual from someone else, it must either:

(a) if lawful and reasonable to do so, destroy the information as soon as practicable without using or disclosing it except for the purpose of determining whether the information should be retained; or

(b) comply with all relevant provisions in the UPPs that apply to the information in question, as if the agency or organisation had actively collected the information.

2.5 In addition to the other requirements in UPP 2, an agency or organisation must not collect sensitive information about an individual unless:

(a) the individual has consented;

(b) the collection is required or authorised by or under law;

(c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual to whom the information concerns is legally or physically incapable of giving or communicating consent;

(d) if the information is collected in the course of the activities of a non- profit organisation—the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities; and

(ii) at or before the time of collecting the information, the organisation undertakes to the individual to whom the information concerns that the organisation will not disclose the information without the individual's consent;

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim;

(f) the collection is necessary for research and all of the following conditions are met:

(i) the purpose cannot be served by the collection of information that does not identify the individual or from which the individual would not be reasonably identifiable;

(ii) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the collection;

(iii) a Human Research Ethics Committee that is constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research* (2007), as in force from time to time, has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*; and

(iv) the information is collected in accordance with Research Rules issued by the Privacy Commissioner; or

(g) the collection is necessary for the purpose of a confidential alternative dispute resolution process.

2.6 Where an agency or organisation collects sensitive information about an individual in accordance with 2.5(f), it must take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.

Note: Agencies and organisations that collect personal information about an individual from an individual or from someone else must comply with UPP 3.

UPP 3. Notification

3.1 At or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual or from someone other than the individual, it must take such steps, if any, as are reasonable in the circumstances to notify the individual, or otherwise ensure that the individual is aware of, the:

(a) fact and circumstances of collection, where the individual may not be aware that his or her personal information has been collected;

(b) identity and contact details of the agency or organisation; rights of access to, and correction of, personal information provided by these principles;

(d) purposes for which the information is collected;

(e) main consequences of not providing the information;

(f) actual or types of organisations, agencies, entities or other persons to whom the agency or organisation usually discloses personal information of the kind collected;

(g) fact that the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information are set out in the agency's or organisation's Privacy Policy; and

(h) fact, where applicable, that the collection is required or authorised by or under law.

UPP 4. Openness

4.1 An agency or organisation must create a Privacy Policy that sets out clearly its expressed policies on the management of personal information, including how it collects, holds, uses and discloses personal information. This document should also outline the:

(a) sort of personal information the agency or organisation holds;

(b) purposes for which personal information is held;

(c) avenues of complaint available to individuals in the event that they have a privacy complaint;

(d) steps individuals may take to gain access to personal information about them held by the agency or organisation; and

(e) whether personal information is likely to be transferred outside Australia and the countries to which such information is likely to be transferred.

4.2 An agency or organisation should take reasonable steps to make its Privacy Policy available without charge to an individual:

(a) electronically; and

(b) on request, in hard copy, or in an alternative form accessible to individuals with special needs.

UPP 5. Use and Disclosure

5.1 An agency or organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection (the secondary purpose) unless:

(a) both of the following apply:

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; and

(ii) the individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose;

(b) the individual has consented to the use or disclosure;

(c) the agency or organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to:

(i) an individual's life, health or safety; or

(ii) public health or public safety;

(d) the agency or organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities;

(e) the use or disclosure is required or authorised by or under law;

(f) the agency or organisation reasonably believes that the use or disclosure is necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal;

(g) the use or disclosure is necessary for research and all of the following conditions are met:

(i) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the use or disclosure;

(ii) a Human Research Ethics Committee that is constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research* (2007), as in force from time to time, has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*;

(iii) the information is used or disclosed in accordance with Research Rules issued by the Privacy Commissioner; and

(iv) in the case of disclosure—the agency or organisation reasonably believes that the recipient of the personal information will not disclose the information in a form that would identify the individual or from which the individual would be reasonably identifiable; or

(h) the use or disclosure is necessary for the purpose of a confidential alternative dispute resolution process.

5.2 If an agency or organisation uses or discloses personal information under paragraph 5.1(f) it must make a written note of the use or disclosure.

5.3 UPP 5.1 operates in respect of personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

Note 1: It is not intended to deter organisations from lawfully cooperating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 5.1 does not override any existing obligations not to disclose personal information. Nothing in subclause 5.1 requires an agency or organisation to disclose personal information; an agency or organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: Agencies and organisations also are subject to the requirements of the 'Cross-border Data Flows' principle when transferring personal information about an individual to a recipient who is outside Australia.

UPP 6. Direct Marketing (only applicable to organisations)

6.1 An organisation may use or disclose personal information about an individual who is an existing customer aged 15 years or over for the purpose of direct marketing only where the:

(a) individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing; and

(b) organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications.

6.2 An organisation may use or disclose personal information about an individual who is not an existing customer or is under 15 years of age for the purpose of direct marketing only in the following circumstances:

(a) either the:

(i) individual has consented; or

(ii) information is not sensitive information and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure;

(b) in each direct marketing communication, the organisation draws to the individual's attention, or prominently displays a notice advising the individual, that he or she may express a wish not to receive any further direct marketing communications;

(c) the organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications; and

(d) if requested by the individual, the organisation must, where reasonable and practicable, advise the individual of the source from which it acquired the individual's personal information.

6.3 In the event that an individual makes a request of an organisation not to receive any further direct marketing communications, the organisation must:

(a) comply with this requirement within a reasonable period of time; and

(b) not charge the individual for giving effect to the request.

UPP 7. Data Quality

An agency or organisation must take reasonable steps to make certain that the personal information it collects, uses or discloses is, with reference to the purpose of that collection, use or disclosure, accurate, complete, up-to-date and relevant.

UPP 8. Data Security

8.1 An agency or organisation must take reasonable steps to:

(a) protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure; and

(b) destroy or render non-identifiable personal information if it is no longer needed for any purpose for which it can be used or disclosed under the UPPs and retention is not required or authorised by or under law.

8.2 The requirement to destroy or render non-identifiable personal information is not 'required by law' for the purposes of the *Archives Act 1983* (Cth).

Note: Agencies and organisations also should be aware of their obligations under the data breach notification provisions.

UPP 9. Access and Correction

9.1 If an agency or organisation holds personal information about an individual and the individual requests access to the information, it must respond within a reasonable time and provide the individual with access to the information, except to the extent that:

Where the information is held by an agency:

(a) the agency is required or authorised to refuse to provide the individual with access to that personal information under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents; or

Where the information is held by an organisation:

(b) providing access would be reasonably likely to pose a serious threat to the life or health of any individual;

(c) providing access would have an unreasonable impact upon the privacy of individuals other than the individual requesting access;

(d) the request for access is frivolous or vexatious;

(e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings;

(f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations;

(g) providing access would be unlawful;

(h) denying access is required or authorised by or under law;

(i) providing access would be likely to prejudice an investigation of possible unlawful activity;

(j) providing access would be likely to prejudice the:

  (i) prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

  (ii) enforcement of laws relating to the confiscation of the proceeds of crime;

  (iii) protection of the public revenue;

  (iv) prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

  (v) preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders; by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

9.2 Where providing access would reveal evaluative information generated within the agency or organisation in connection with a commercially sensitive decision-making process, the agency or organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: The mere fact that some explanation may be necessary in order to understand information should not be taken as grounds for withholding information under UPP 9.2.

9.3 If an agency or organisation is not required to provide an individual with access to his or her personal information it must take such steps, if any, as are reasonable to provide the individual with as much of the information as possible, including through the use of a mutually agreed intermediary.

9.4 If an organisation charges for providing access to personal information, those charges:

(a) must not be excessive; and

(b) must not apply to lodging a request for access.

Note: Agencies are not permitted to charge for providing access to personal information under UPP 9.4.

9.5 An agency or organisation must provide personal information in the manner requested by an individual, where reasonable and practicable.

9.6 If an agency or organisation holds personal information about an individual that is, with reference to a purpose for which it is held, misleading or not accurate, complete, up-to-date and relevant, the agency or organisation must take such steps, if any, as are reasonable to:

(a) correct the information so that it is accurate, complete, up-to-date, relevant and not misleading; and

(b) notify other entities to whom the personal information has already been disclosed, if requested to do so by the individual and provided such notification would be practicable in the circumstances.

9.7 If an individual and an agency or organisation disagree about whether personal information is, with reference to a purpose for which the information is held, misleading or not accurate, complete, up-to-date or relevant and:

(a) the individual asks the agency or organisation to associate with the information a statement claiming that the information is misleading or not accurate, complete, up-to-date or relevant; and

(b) where the information is held by an agency, no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth; the agency or organisation must take reasonable steps to do so.

9.8 Where an agency or organisation denies a request for access or refuses to correct personal information it must provide the individual with:

(a) reasons for the denial of access or refusal to correct the information, except to the extent that providing such reasons would undermine a lawful reason for denying access or refusing to correct the information; and

(b) notice of potential avenues for complaint.

UPP 10. Identifiers (only applicable to organisations)

10.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) an agency;

(b) an agent of an agency acting in its capacity as agent;

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract; or

(d) an Australian state or territory agency.

10.2 Where an identifier has been 'assigned' within the meaning of UPP 10.1 an organisation must not use or disclose the identifier unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency that assigned the identifier;

(b) one or more of UPP 5.1(c) to (f) apply to the use or disclosure; or

(c) the identifier is genetic information and the use or disclosure would be permitted by the new *Privacy (Health Information) Regulations*.

10.3 UPP 10.1 and 10.2 do not apply to the adoption, use or disclosure by a prescribed organisation of a prescribed identifier in prescribed circumstances, set out in regulations made after the Minister is satisfied that the adoption, use or disclosure is for the benefit of the individual concerned.

10.4 The term 'identifier', for the purposes of UPP 10, includes a number, symbol or biometric information that is collected for the purpose of automated biometric identification or verification that:

(a) uniquely identifies or verifies the identity of an individual for the purpose of an agency's operations; or

(b) is determined to be an identifier by the Privacy Commissioner.

However, an individual's name or ABN, as defined in the *A New Tax System (Australian Business Number) Act 1999* (Cth), is not an 'identifier'.

Note: A determination referred to in the 'Identifiers' principle is a legislative instrument for the purposes of section 5 of the *Legislative Instruments Act 2003* (Cth).

UPP 11. Cross-border Data Flows

11.1 If an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia and an external territory, the agency or organisation remains accountable for that personal information, unless the:

(a) agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to these principles;

(b) individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or

(c) agency or organisation is required or authorised by or under law to transfer the personal information.

Note: Agencies and organisations are also subject to the requirements of the 'Use and Disclosure' principle when transferring personal information about an individual to a recipient who is outside Australia.

Appendix 3: Key Definitions recommended by the ALRC

Personal information:

> 'Information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual.'

Health information:

(a) information or an opinion about:

  (i) the physical, mental or psychological health or a disability (at any time) of an individual; or

  (ii) an individual's expressed wishes about the future provision of health services to him or her; or

  (iii) a health service provided, or to be provided, to an individual; that is also personal information; or

(b) other personal information collected to provide, or in providing, a health service; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances; or

(d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

Health service:

(e) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the service provider to:

  (i) assess, predict, maintain or improve the individual's physical, mental or psychological health or status;

  (ii) diagnose the individual's illness, injury or disability; or

  (iii) prevent or treat the individual's illness, injury or disability or suspected illness, injury or disability;

(f) a health-related disability, palliative care or aged care service;

(g) a surgical or related service; or

(h) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

Sensitive Information:

(a) information or an opinion about an individual's:

  (i) racial or ethnic origin; or

  (ii) political opinions; or

  (iii) membership of a political association; or

  (iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual orientation and practices; or

(ix) criminal record;

that is also personal information; or

(b) health information about an individual; or

(c) genetic information about an individual that is not otherwise health information;

(d) biometric information collected for the purpose of automated biometric verification or identification; and

(e) biometric template information.