



Australian Government

Department of Health and Ageing

**Personally Controlled Electronic
Health Record System:
Legislation Issues Paper**

© Commonwealth of Australia 2011

This work is copyright. You may download, display, print and reproduce the whole or part of this work in unaltered form for your own personal use or, if you are part of an organisation, for internal use within your organisation, but only if you or your organisation do not use the reproduction for any commercial purpose and retain this copyright notice and all disclaimer notices as part of that reproduction. Apart from rights to use as permitted by the *Copyright Act 1968* or allowed by this copyright notice, all other rights are reserved and you are not allowed to reproduce the whole or any part of this work in any way (electronic or otherwise) without first being given the specific written permission from the Commonwealth to do so. Requests and enquiries concerning reproduction and rights are to be sent to the Communications Branch, Department of Health and Ageing, GPO Box 9848, Canberra ACT 2601, or via e-mail to copyright@health.gov.au.

Minister's introduction



The Australian Government is establishing electronic health records to deliver benefits for patients and clinicians across Australia.

The personally controlled electronic health record (PCEHR) system will enable better access to important health information currently held in dispersed records around the country. It will mean that patients will no longer need to unnecessarily repeat their medical history every time they see a doctor or other health professional.

I am pleased to seek your feedback on the legislation that will underpin that system by releasing publicly this *PCEHR System: Legislation Issues Paper*.

As part of our \$467 million program, we have already released the *Draft Concept of Operations – Relating to the introduction of a PCEHR system*, public consultation on which has just closed. We also are establishing 12 lead sites around the nation to test and apply e-health systems prior to the national launch from July next year.

As well as the technology, it is important that we also establish a strong legal framework that will help to make the new system work.

This will include creating a system that places the patient at the centre of the system – with strong access and privacy controls over their own information.

On the basis of this paper and the feedback we receive, the Government will be drafting legislation for introduction this year. This legislation will also be released for public consultation prior to being presented to Parliament.

This document includes 41 proposals for public comment about the content of the legislation, as well as asking 34 questions to the community to help test the views of the clinicians, health consumers, the ICT industry and the broader public.

The proposals in this paper are developed on the foundations of Australia's existing privacy legislation, as well as the privacy provisions in place as part of the *Healthcare Identifiers Act 2010* which was passed by the federal Parliament last year.

I welcome your feedback so that we can design the most robust legislation as possible to establish these records and so that Australians can receive the benefits that e-health will offer.

A handwritten signature in black ink, appearing to read 'Nicola Roxon'. The signature is fluid and cursive, with a long horizontal stroke at the end.

The Hon Nicola Roxon MP

Minister for Health and Ageing

Table of contents

Executive summary	1
1 Introduction	3
1.1 Purpose and scope of paper	3
1.2 What is not in scope.....	3
1.3 How to make a submission.....	3
2 Background and context	5
2.1 Health reform	5
2.2 Purpose of the PCEHR system.....	5
2.3 Design fundamentals – how the PCEHR will work.....	5
2.4 Design fundamentals – person-centred care and personal control	7
2.5 Benefits and improvements	9
2.5.1 Key benefits for patients	9
2.5.2 Key benefits for healthcare providers	9
2.5.3 Key benefits for the healthcare system.....	10
2.6 Implementation.....	10
2.7 Timeframes	10
2.8 Consultation of the PCEHR system	10
3 Legislative proposals to support the PCEHR system	12
3.1 Summary of the proposed legislative framework	12
3.2 Participation.....	12
3.2.1 Individuals	13
3.2.2 Healthcare provider organisations.....	18
3.2.3 PCEHR system operator	20
3.2.4 Repository operators	21
3.2.5 Trusted data source providers.....	22
3.2.6 Portal providers	23
3.2.7 Intellectual property.....	23
3.2.8 Health records management.....	24
3.3 Access	25
3.3.1 Individuals	25
3.3.2 Healthcare provider organisations.....	27
3.4 Privacy – coverage.....	28
3.4.1 Privacy – use and disclosure of information.....	31
3.5 Security	31
3.5.1 Offences and penalties.....	32
3.6 Governance	36
3.6.1 Principles for long-term governance.....	36
3.6.2 Complaints handling scheme	37
4 Next steps	39
Appendix 1: Acronyms and key definitions	40
Appendix 2: E-health and national healthcare identifiers	41
Appendix 3: Privacy laws in Australia	43
Appendix 4: State/territory general medical record retention requirements	44

Executive summary

The personally controlled electronic health record (PCEHR) system is a key element of the Australian Government's national health reform agenda. The PCEHR system and other health reform programs are designed to improve the delivery of health services and healthcare outcomes for all Australians.

The Department of Health and Ageing is responsible for managing the design and implementation of the system in association with consumers, the National E-Health Transition Authority, states and territories and key market partners. This paper is intended to promote discussion within the community about the legislative framework required to support implementation of the design and operation of the PCEHR system as described in the *Draft Concept of Operations—Relating to the introduction of a PCEHR system*¹ ('draft Concept of Operations'). The draft Concept of Operations was released by the Minister for Health and Ageing, the Hon. Nicola Roxon MP, for public comment on 12 April 2011 and is also available online at the <www.yourhealth.gov.au> website. The period for making submissions on the draft Concept of Operations closed on 7 June 2011.

This legislation issues paper sets out:

- introductory issues including the context and how to make a submission;
- the purpose, scope, key design features and information flows of the PCEHR system; and
- the proposed legislative framework to support the PCEHR system and particular questions about the proposals.

The legislative proposals are structured under five headings:

Participation: The most likely participants in the system are identified to include individuals, healthcare provider organisations, information service providers, the PCEHR system operator, repository providers, trusted data sources and portal providers. The participation model, registration, identification and verification of participants are canvassed.

Access: The PCEHR system revolves around the notion of personal control which extends to the capacity of individuals to have access to their own health information and to have choices about how access by healthcare provider organisations to their PCEHR is managed by the system.

Privacy: Health information within the PCEHR system will be protected through a combination of legislation, governance, and security and technology measures. The regulation of health information privacy across Australia varies, with Commonwealth privacy legislation covering the Commonwealth and private sector, and state and territory legislation or administrative arrangements covering the state and territory public sectors. The Australian Government is working to establish a revised privacy framework for personal and health information that will apply to Commonwealth agencies and private sector organisations. Health Ministers from the Commonwealth, states and territories have endorsed the goal of uniform health privacy legislation, which is likely to flow from the revised Commonwealth system over time. Current consultation with jurisdictions is focused on achieving a clear, workable arrangement to support implementation of the PCEHR system.

Security: Security of information held within the PCEHR system will include accurate authentication of individuals and organisations accessing the system, robust audit trails that can be accessed by individuals, proactive monitoring of

¹ The draft Concept of Operations is available at <www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/pcehr>

access by the system operator to detect suspicious and inappropriate behaviour, security testing, education and training of users, and requirements that the system operator and healthcare provider organisations only access the PCEHR when authorised. Not all elements of the security framework require a legislative response. However, this paper proposes offence and penalty mechanisms to deter or punish inappropriate behaviours or misuse.

Governance: The PCEHR system will be a key piece of national health infrastructure, as is the Healthcare Identifiers Service. E-health governance arrangements were considered as part of the National E-Health Strategy agreed by all Health Ministers in December 2008. The governance model 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 take a role. In addition to proposed legislation for the PCEHR system and application of a range of existing regulatory frameworks this model relies on competition and use of funding and compliance mechanisms to encourage participation. The governance framework for the PCEHR system would provide for three key functions:

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

The three key functions of governance in relation to the PCEHR system are described in further detail within the document.

1 Introduction

1.1 Purpose and scope of paper

This paper outlines the proposed legislative framework to support the establishment and implementation of a national personally controlled electronic health record (PCEHR) system. It describes the approach to establishing the system, explains how a PCEHR will benefit consumers and healthcare providers, and sets out the legislative framework and proposals for discussion.

The purpose of this paper is to encourage discussion and feedback on the proposed framework. It is expected that public consultation will identify new issues and approaches for consideration in the further development of the legislative framework for the PCEHR system.

The paper has been developed by the Commonwealth in consultation with a working group of representatives from Commonwealth, state and territory health departments. The Commonwealth will continue to work closely with the jurisdictions in developing the legislative framework for the PCEHR system.

Acronyms and terms used in this paper are described at [Appendix 1](#).

1.2 What is not in scope

This paper puts forward a proposal for the legislation which might be developed to support a PCEHR system, the design of which is described in the *Draft Concept of Operations—Relating to the introduction of a PCEHR system*² ('draft Concept of Operations'). The draft Concept of Operations was released by the Minister for Health and Ageing, the Hon. Nicola Roxon MP, for public comment on 12 April 2011 and is available online at the <www.yourhealth.gov.au> website.

In this paper, the Commonwealth is seeking feedback on how well the legislative proposals support a PCEHR system as described in the draft Concept of Operations.

Feedback about the design of the PCEHR system itself, rather than its legislative framework, is not the intent of this phase of the consultation. Comments about the design of the system have already been sought in the public consultation on the draft Concept of Operations which closed on 7 June 2011.

1.3 How to make a submission

Submissions are invited from interested stakeholders on the legislative proposals for the PCEHR system as set out in this paper. The paper raises questions to stimulate discussion on particular issues. The questions provided 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.

² The draft Concept of Operations is available at <www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/pcehr>

Submissions may be:

1. Forwarded to:
PCEHR Legislation Issues Feedback
Department of Health and Ageing
GPO Box 9848
CANBERRA ACT 2601

OR

2. Provided at:
<www.yourhealth.gov.au>

OR

3. Submitted to:
<ehealth.legislation@health.gov.au>

Submissions will be made public and shared with relevant Commonwealth, state and territory government agencies to inform consideration of the PCEHR legislative framework.

Submissions that are intended to remain confidential should be clearly marked as such and submitters should be aware that confidential submissions may still be subject to access under Freedom of Information law.

The closing date for comments and submissions is **5 p.m. (Australian Eastern Standard Time), Wednesday 3 August 2011.**

Public notice: Readers are to note that submissions or comments will generally be subject to freedom of information provisions which includes being provided in response to a freedom of information request and subject to the provisions of the *Freedom of Information Act 1982*.

2 Background and context

2.1 Health reform

Australia's economic growth, productivity and long-term prosperity are underpinned by the health of its population. A healthy population is influenced by strong social and physical infrastructure and an accessible, safe and high quality health system.

Recent health reform reports³ recognise that the health system is facing challenges which are driving increased healthcare service demands and costs. The need to reform the healthcare system has been recognised by all governments.

The Australian Government is therefore implementing a range of health reforms which are underpinned by improvements to the operation of e-health in Australia. Some of the building blocks for e-health are, or have been, established following Health Ministers endorsing the National E-Health Strategy in 2008.

One of the key building blocks that has been established is the Healthcare Identifiers Service ('HI Service'), which commenced operation on 1 July 2010 to allocate unique identifiers to healthcare consumers, healthcare providers and healthcare provider organisations. The use of healthcare identifiers to more accurately identify and match healthcare information is an integral part of the proposed PCEHR system. Further information on the HI Service is at [Appendix 2](#).

As a key element of health reform, in 2010 the Australian Government announced a \$467 million investment over two years in the key components of an electronic health record system so that all Australians have access to a PCEHR if they choose to have one. The PCEHR system is the next step in using e-health to enhance the provision of healthcare and healthcare outcomes.

2.2 Purpose of the PCEHR system

The purpose of the PCEHR system is to address information fragmentation by allowing a person to more easily access their own health information and make their health information securely accessible to different healthcare providers involved in their care.

2.3 Design fundamentals – how the PCEHR will work

The PCEHR system will allow clinical data and records to be stored, so that they can, with the consumer's consent, be retrieved by healthcare providers involved in providing treatment. The individual will be able to decide what clinical records about them will be uploaded to the system, and will have some choices about how to provide healthcare provider organisations involved in their care with access to their information.

Individuals and healthcare providers participating in the system will need to use healthcare identifiers issued by the HI Service. The healthcare identifiers will be used to ensure that the right health information is associated with the right record as part of the indexing of patient records, and to identify

³ *A Healthier Future For All Australians—Final Report of the National Health and Hospitals Reform Commission*, National Health and Hospitals Reform Commission, June 2009; *Primary Health Care Reform in Australia—Report to Support Australia's First National Primary Health Care Strategy*, Department of Health and Ageing, 2009; and *Australia: the healthiest country by 2020, National Preventative Health Strategy—the roadmap for action*, National Preventative Health Taskforce, 2009

healthcare providers that access and contribute information to the PCEHR system.

The PCEHR system services will be delivered to individuals and healthcare providers through the coordinated efforts of a number of organisations working together to perform specific roles to support the system. These roles are:

- **System operator** – the system operator is responsible for providing key services which integrate the PCEHR system, like registering participants, indexing records coming into the system, and maintaining an audit trail of access to the information available through the PCEHR system. The system operator will be the focal point of the system where various components are pulled together to provide an integrated, effective service to consumers and health provider organisations;
- **Repository operators** – repositories are operated by organisations that hold health information which is available for retrieval by the system operator, when the system operator receives a request for access from an authorised individual or healthcare provider organisation; and
- **Portal operators** – individuals and healthcare providers will be able to access records in the PCEHR system via conformant portals.

These roles are likely to be filled by a range of public and private sector organisations that demonstrate they can perform the roles to a sufficiently high standard and can meet the standards to operate with the PCEHR system.

Key design features of the PCEHR system

The PCEHR system:			
is	opt in – if an individual or healthcare provider wants to participate, they need to register with the system to do so.	and not	compulsory – both individuals and healthcare providers choose whether or not to participate.
is	an enhancement to medical treatment – the PCEHR system will allow an individual's health information to be shared as and when it is needed to support the best possible care.	and not	a requirement for medical treatment – if a person does not wish to participate in the PCEHR system, this has no impact on their eligibility for treatment or Medicare benefits.
is	a source of selected clinical data and documents – in addition to a health summary in each PCEHR which contains basic health data about an individual, clinical documents may be added to that person's PCEHR only with their agreement.	and not	a substitute for normal clinical records – an individual's healthcare providers will continue to maintain their own records of each person's health and wellbeing. Those will continue to be the primary records of a person's treatment and care.

is	a source of information to assist enquiry – a person's PCEHR is intended to be the start of the conversation between a person and their healthcare provider. It will hold basic data which can inform the kinds of questions the healthcare provider might ask.	and not	a replacement for normal sharing of information between an individual and their healthcare provider – as currently occurs in medical practice, existing medical records are used as the starting point for the discussion about the patient's health, rather than as the complete and authoritative source of current information.
is	aligned with current privacy obligations – healthcare providers will have the same privacy responsibilities in relation to information in PCEHRs as they currently do in relation to other clinical information.	and not	immune to current sharing and reporting rights and obligations of providers – healthcare providers currently have rights and obligations in relation to disclosure of health information which will continue. These include the ability to access health information in life threatening situations and the obligation to report to government authorities about a range of disease and child welfare matters.
is	a distributed system of service providers working in concert – government and private sector organisations will work together to deliver the PCEHR system to individuals and healthcare providers. The proposed legislative framework is intended to impose appropriate controls and standards on all the delivery bodies.	and not	a single government store of personal information – while public sector bodies may provide some of the repositories which hold information for the PCEHR system, other private sector organisations may also participate as repositories where they meet relevant standards.

2.4 Design fundamentals – person-centred care and personal control

The PCEHR system will enable key information currently stored in dispersed health records across the healthcare system to be accessible online, making the PCEHR person-centred. An individual's key health information can travel with them through the healthcare system, making their important health information available to support their end-to-end healthcare needs regardless of where they seek care or assistance – even when away from home or seeing new healthcare providers.

Central to the PCEHR system is the concept of personal control.

Individuals will have a number of controls over their PCEHR, including the ability to set some access controls at the point of registration, and will be able to access the service in a number of ways to monitor access to their PCEHR.

The following controls have been designed to provide at least the same kinds of choices individuals currently have over how their health information is accessed and shared with healthcare providers, and provides enhanced methods for individuals to access their own health information and be informed about how healthcare providers are accessing their information.

The controls on which individuals will make decisions about access to their electronic health record will include the ability to:

- *Decide whether or not to have an active PCEHR*

The PCEHR system will operate as an opt-in model, where individuals elect to register and create a PCEHR. Individuals may deactivate their PCEHR at any time and subsequently reactivate their PCEHR at any time.

- *Access information in their PCEHR*

Individuals will be able to view all health information contained in their PCEHR.

- *Set controls around healthcare provider access*

Individuals may determine and change settings controlling access to their PCEHR by participating healthcare provider organisations involved in their healthcare. Individuals may choose from a range of approaches to setting and managing controls that will give general or limited access.

- *Authorise others to access their PCEHR*

Individuals may nominate other persons (such as carers and family members) to access their PCEHR.

- *Choose which information is published to and accessible through their PCEHR*

Individuals may request that healthcare providers withhold certain information from their PCEHR.

- *View an activity history for their PCEHR*

The PCEHR system will provide an audit trail whereby individuals can view a history of actions on their PCEHR.

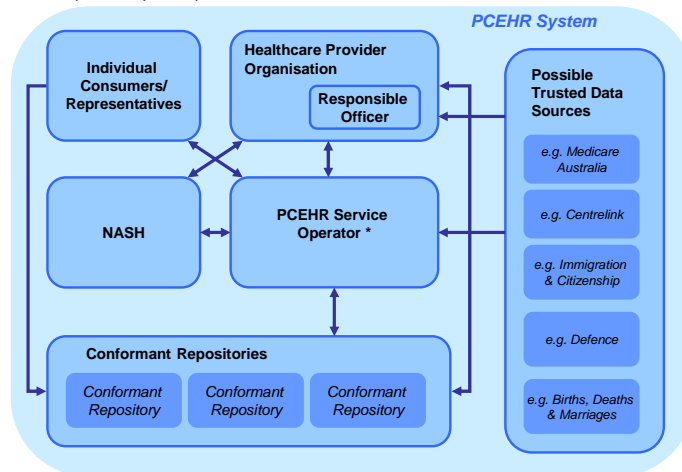
- *Make enquiries and complaints*

Individuals will be able to make enquiries and complaints about the management of information in their PCEHR and the PCEHR system.

Appropriate information and support will be available to individuals to clearly describe the options available for managing the access controls to their PCEHR and for accessing their own information. Establishment and maintenance of these controls will be available via a range of channels.

Healthcare providers who are given access by a consumer to the consumer's PCEHR will be able to download the health information from the PCEHR system into the healthcare provider's local system, where the information will be subject to the existing protections and controls covering that particular healthcare provider.

Participants and information flows in a PCEHR System
(Draft: 19 April 2011)



* Includes national repository, index, view, audit and participation/authorisation services, consumer and provider portals

2.5 Benefits and improvements

2.5.1 Key benefits for patients

Poor availability of health information across healthcare settings can be frustrating and time consuming for patients and healthcare providers alike. It can also have damaging effects on a patient's health outcomes through, for example, avoidable adverse medication events or lack of communication between healthcare providers following discharge from hospital or where multiple providers are involved in a patient's care.

The PCEHR system will enable patients to have easy-to-access information about their medical history, including medications, test results and allergies, allowing them to make informed choices about their healthcare and be active participants in their healthcare.

The system will allow an individual's key health information to travel with them through the healthcare system, making it available to support their end-to-end healthcare needs regardless of where they seek healthcare assistance.

Patients will no longer have to remember every detail of their care history and retell it to every healthcare provider they see. Parents will not have to remember the vaccinations their child has had and healthcare providers will not have to search through paper records.

2.5.2 Key benefits for healthcare providers

The PCEHR system will enable a better quality of health information to be available to healthcare providers at the point of care. Healthcare providers and organisations that choose, and are ready, to participate in the system will have the opportunity to:

- access health information more easily – the PCEHR system will provide secure, quick and easy access to a consolidated view of an individual's key health information supplied by other participating healthcare provider organisations;
- ensure safer healthcare – the system will provide easy access to key information about an individual such as their allergies and previous adverse reactions as well as their medicines and related healthcare conditions and provide a summary of relevant healthcare events; and
- deliver more effective healthcare – easier access to information can be crucial to improved prevention, early intervention and treatment.

2.5.3 Key benefits for the healthcare system

Like many other health systems worldwide, the Australian healthcare system is facing an increasing set of challenges which threaten the sustainability of current healthcare business practices.

The PCEHR system will be a key part of an agile and continuously improving 21st century health system.⁴

As a key workstream of the national health reform agenda, the PCEHR system will help manage healthcare costs and support sustainable quality care. The system will support improved healthcare decisions based on updated information:

- reductions in preventable hospitalisations through ready access to relevant information;
- delivery of better coordinated healthcare across distributed healthcare provider organisations;
- reductions in the number of avoidable adverse events and costly unnecessary treatment activities;
- improvement in health sector efficiency through streamlining healthcare information and testing processes; and
- allowing clinicians and clinical support staff to access patient information they need in a more timely, convenient and reliable fashion.

2.6 Implementation

Implementation of the PCEHR system will initially focus on key groups in the community likely to receive the most immediate benefit, including those suffering from chronic and complex conditions, older Australians, Aboriginal and Torres Strait Islander peoples, and mothers and newborn children. The methodology for focussing on these target groups will be developed initially through the guidance and directions gleaned from the lead implementation sites. The change and adoption partner will also identify care strategies to ensure that these target groups are given priority in the initial stage of the PCEHR system.

2.7 Timeframes

From July 2012 individuals will be able to register online for a PCEHR. As the PCEHR system is taken up by healthcare providers, registered individuals will be able to progressively reap the benefits of having a PCEHR.

2.8 Consultation on the PCEHR system

The consultation that has been undertaken in respect of the PCEHR system is outlined below in chronological order.

June 2008: The National E-Health Transition Authority (NEHTA) conducted two clinician and consumer roundtable sessions as part of the Individual Electronic Health Record proposal. A peak body summit was then held to present and validate the key recommendations from those sessions.

July 2008: NEHTA released its *Privacy Blueprint for the Individual Electronic Health Record* for public comment. It was distributed to a range of key stakeholders and published on the NEHTA website. A report of feedback was

⁴ For example, about 2-3 per cent of hospital admissions in Australia are linked to medication errors. This equates to 190,000 admissions each year and costs the health system \$660 million. Clear and promptly available information will reduce such incidents, avoid unnecessary tests and save scarce health resources.

released in November 2008 which provided a summary and analysis of the key themes that emerged from the submissions made on the Blueprint, and outlined NEHTA's next steps.⁵

August 2008: NEHTA undertook a quantitative survey and opinions were sought from 2,700 people across Australia on issues relating to implementation of an individual electronic health record.⁶

September 2009: A workshop was held with clinician and consumer representatives to discuss the Individual Electronic Health Record, test ideas and concepts, share ideas and capture feedback and concerns.

July 2010: NEHTA commenced consultation and engagement activities using its clinical leads and reference group members, leveraging the experience and skills in each of its existing reference groups. Each group has a mix of participants including clinical, consumer and state and territory representatives, and representatives with other backgrounds.

August 2010: The Department of Health and Ageing selected three organisations as lead sites to deploy and test national e-health infrastructure and standards, demonstrate tangible outcomes and benefits from funded e-health projects, and build stakeholder support and momentum behind the PCEHR program. These three sites are part of the first wave of lead sites, aimed at supporting early adopters, and the second wave lead sites were selected in March 2011.

November 2010: The Department of Health and Ageing conducted a National E-health Conference. This was the beginning of public discussions and included a number of sessions to engage the community on the topic of the PCEHR. The various presentations, including the speech by the Minister for Health and Ageing, the Hon. Nicola Roxon MP, were streamed live to the public, and information regarding these discussions is available online at <www.yourhealth.gov.au>, including:

- a report on the key themes emerging from the conference and earlier roundtables; and
- all the support material including an animation, interviews and case studies.

March 2011: The Department of Health and Ageing selected nine organisations as part of the second wave of lead sites. One of the key objectives of the second wave is to achieve national demographic coverage.

April 2011: The Department of Health and Ageing released the draft Concept of Operations for the PCEHR system for public comment. That document provides an overview of what the PCEHR system is and how it is proposed to work. It was intended to elicit discussion on the proposed design and to highlight areas of uncertainty where further work is required. The period for making a submission on the draft Concept of Operations closed on 7 June 2011. The Concept of Operations is expected to be finalised in August 2011.

The Department of Health and Ageing and NEHTA will conduct additional rounds of consultation as the PCEHR program progresses.

⁵ Both documents are available at <www.nehta.gov.au>

⁶ The individual electronic health record was the precursor to the personally controlled electronic health record

3 Legislative proposals to support the PCEHR system

3.1 Summary of the proposed legislative framework

If consumers, healthcare providers and other organisations are to actively participate in the PCEHR system, there must be a high level of trust and confidence in its operation. A legislative framework that provides clear, transparent and flexible oversight of the operation of the system as it develops and evolves is required.

This section outlines the key legislative requirements for the operation of the PCEHR system and the rights and responsibilities of participants who use the system.

The proposals outlined in this paper propose that the legislative framework will:

- establish arrangements for operating the PCEHR system;
- establish processes for participation;
- establish processes for enquiry and complaint;
- recognise the risks that a PCEHR system will present;
- recognise that there are existing regulatory frameworks in place to support the appropriate flow of health information for healthcare and other public interest purposes; and
- recognise that the PCEHR system will also be supported by other laws and through means other than legislation, for example standards and education.

Health information is currently regulated by legislation, including privacy law (see [Appendix 3](#)). This includes laws that prohibit specific information flows or authorise information flows that would otherwise be prohibited. Examples include:

- *Healthcare Identifiers Act 2010* ('HI Act') and regulations;
- health services legislation;
- freedom of information (FOI) legislation;
- public health notifications required under national or international law;
- child protection legislation;
- HIV AIDS legislation;
- mental health legislation; and
- 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, wherever this is feasible for the effective and secure delivery of a PCEHR system.

It is proposed that the common law duty of confidentiality between healthcare providers and patients, and professional accreditation and registration requirements for healthcare providers, will continue to operate.

3.2 Participation

It is important in establishing any scheme to identify the key participants. It is also considered necessary that legislation establish these roles, set out

clear parameters for usage of the system and provide for the full range of enforceability measures, including criminal penalties if required.

Key participants in the PCEHR system are:

- individuals (i.e. healthcare recipients);
- healthcare provider organisations;
- individual healthcare providers;
- PCEHR system operator;
- repository providers, which include registries;
- trusted data sources, including the HI Service;
- portal providers; and
- the information technology (IT) industry, including software providers.

This is not an exclusive list of the participants in the PCEHR system since it is likely that there may be other organisations providing infrastructure services to the PCEHR system operator. At this time it is considered that the participation of service providers of this kind could be managed through contractual relationships with the system operator rather than by legislation.

Q1. Are there other potential participants in the PCEHR system and what is their role?

3.2.1 Individuals

Individuals, as healthcare recipients, will be able to register for a PCEHR in a number of ways.

It is expected that the primary registration channel will be to register using an online process. Assisted face-to-face registrations may be supported through government service offices or healthcare provider organisations. An option to register for a PCEHR by post will also be provided for those individuals who are unable to access online or face-to-face services.

Online registrations are expected to be supported by one or more consumer portals that could be provided by the PCEHR system, an existing government service provider or an existing health related service.

The registration processes for the PCEHR system are expected to leverage existing registration, verification of identity and authentication processes and standards to ensure that the right record is created for the right person. Individuals who wish to register for a PCEHR will need to have a verified Individual Healthcare Identifier (IHI) assigned by the HI Service. Newborns and infants under 12 months may not yet have a verified IHI and an alternative process will be put in place for these circumstances.

Individuals will need to provide sufficient identifying information to ensure that a single PCEHR is created for the individual. It is proposed that individuals will need to provide:

- full name;
- IHI, Medicare card number or Department of Veterans' Affairs (DVA) file number;
- date of birth;
- sex; and
- address, as registered with a trusted data source such as Medicare Australia.

Individuals who are enrolled with Medicare Australia⁷ or hold a DVA file number⁸ have been automatically allocated an IHI by the HI Service.

An IHI can be obtained from the HI Service by providing a combination of demographic details such as a birth certificate or passport and other identification documentation.⁹

Once the individual's PCEHR is active the individual would be able to establish a range of access controls and add information such as contact details and next of kin details.

Proposal 1: Legislation would specify that an individual would be entitled to be registered for a PCEHR if:

- he or she has a verified IHI; or
- in the case of individuals under 12 months who do not have a verified IHI, he or she has an unverified IHI; and
- the identifying information has been provided to enable registration.

Proposal 2: Legislation would enable the information flows necessary to verify the identity of individuals, and to create legally recognised rights and responsibilities for individuals.

Q2. Should portals for consumer registration be provided by organisations other than health related organisations, including government organisations?

It is proposed that legislation would provide the framework to allow an individual to participate in the PCEHR system in a range of ways, depending on the circumstances. These could include the participation of an individual:

- personally;
- by an authorised representative;
- by a nominated representative; and
- using a pseudonym.

To provide flexibility to accommodate the wide variety of personal circumstances which may arise, the legislation could provide a broad framework and be supplemented by administrative arrangements and policy. Authorised and nominated representative frameworks used by existing national service delivery agencies such as Medicare Australia and Centrelink will inform the detailed operational policy framework for the PCEHR system.

Authorised representatives

The concept of representation is particularly relevant to health service delivery. Individuals are often supported by other people when accessing

⁷ People who reside in Australia are eligible to enrol in Medicare if they hold an Australian or New Zealand citizenship, have been issued with a permanent visa or have applied for a permanent visa (excluding a parent visa).

⁸ A DVA file number is a unique personal identifier issued to a veteran by DVA. All veterans and veteran community clients are issued with a DVA file number. The veteran community may access many different benefits, ranging from pensions to health services, through their DVA file number. Veterans may have a Medicare card number **and** a DVA number or only a DVA number.

⁹ Persons who are not enrolled in Medicare Australia or DVA but receive healthcare in Australia, such as international tourists, are able to get an IHI by visiting a healthcare provider or by applying to the HI Service operator. Documentary evidence of identity will be required to verify the IHI (i.e. in order to register for a PCEHR).

healthcare services and it is important that the provisions put in place are flexible enough to support the types of arrangements that might be needed.

It is important that everyone in Australia have the option of having a PCEHR. There are, however, individuals who have limited or no capacity to make decisions in respect of their health and health information. These individuals would not be able to create and manage a PCEHR on their own behalf. The use of authorised representatives would ensure that these individuals could still have a PCEHR.

The Commonwealth, states and territories each have legislation providing that a person can be authorised by law to represent another person for healthcare purposes, such as through powers of attorney provisions or guardianship orders. The PCEHR system could leverage this existing framework and provide that a person who is authorised by the law of any jurisdiction to act on behalf of an individual for healthcare purposes could be recognised by the PCEHR system as an authorised representative. The PCEHR system would need to verify the legal authority, therefore a person would need to present to the PCEHR system operator appropriate documentary evidence of their authority. This process cannot be undertaken electronically.

An authorised representative would have the ability to decide whether to create a PCEHR for the individual they represent and to complete the registration process for that individual.

It is proposed that legislation would only provide a broad framework to support the participation of individuals through authorised representatives, and be supplemented by administrative arrangements and policy which would provide flexibility to accommodate changing circumstances.

Proposal 3: Legislation would provide a broad framework permitting an individual to participate in the PCEHR system through an authorised representative.

Proposal 4: Administrative and/or policy arrangements would provide the detail for how a person can be recognised by the PCEHR system as an authorised representative.

Proposal 5: Legislation would not prescribe eligibility criteria for authorised representatives, but would recognise authorised representatives established under existing Commonwealth, state and territory laws.

Q3. What possible barriers are there to the participation of individuals through their authorised representatives?

Nominated representatives

Section 3.2.7 of the draft Concept of Operations describes the difference between an authorised representative and a nominated representative. Essentially an authorised representative can act as the individual within the PCEHR system, including giving consent for healthcare providers to access the consumer's PCEHR, accessing records, adding information and changing control settings. In contrast, a nominated representative is nominated by the individual to have access to view the individual's PCEHR, but not to perform any other activity in relation to the PCEHR. The proposals in relation to nominated representatives are therefore in the section of this paper dealing with access (section 3.3.1).

Minors

Australian law recognises that individuals aged 18 years and above have full legal capacity to make decisions about their own health and health information. It is, however, important to recognise that parental authority is

not absolute and although Australian law recognises that children become increasingly competent as they progress toward adulthood, the *Privacy Act 1988* and other health information laws do not prescribe an age at which a child is determined to have capacity to make decisions about their health and health information.

The PCEHR system would ensure that children up to 18 years can have a PCEHR through the authorised representative arrangements.

Any parent or legal guardian who is listed on the same Medicare card as the child would be recognised as an authorised representative of the child for PCEHR system purposes up to 18 years of age. The authorised representative can then decide whether to create a PCEHR for that child and complete the registration process for that child. It is, however, important to recognise that due to many life challenges, some adolescents may find themselves in circumstances where parents are not available, are unable or unwilling to support them.

Across the health sector, the generally accepted age of competency and decision-making capacity in respect of medical treatment is 14 years.

Medicare Australia's claims information policy in relation to minors has, in general terms, set 14 years as the age of consent for release of information. It provides that Medicare or Pharmaceutical Benefits Scheme (PBS) information relating to a person under 14 years will generally be provided to the parent or legal guardian. If a person aged 14 to 15 years does not provide consent to disclose Medicare or PBS information, that information will only be provided to the young person's parent or legal guardian if a health practitioner determines that it is ethical and appropriate to do so. In the case of a person aged 16 years, information will only be disclosed with the consent of the young person.

Exceptions to these situations will occur where the adolescent does not have the capacity to consent to the disclosure of health information, or where a young person is deemed 'at risk' and has been determined as capable by a health practitioner.

In the operation of the PCEHR system, it is desirable to reflect current practice as far as possible, acknowledging the wide range of possible scenarios.

Exceptional circumstances may exist where a child younger than 14 years is deemed under existing arrangements to be a 'mature minor' or 'independent minor'. In these circumstances the PCEHR system would allow for that child to manage their own PCEHR.

The proposals below reflect existing settings regarding presumed competence of young people from the age of 14 years, and that parental authority discontinues from the age of 18 years. This position also recognises a desire to support young people seeking to register for and/or control their PCEHR.

As discussed at the section on authorised representatives, legislation will provide a broad framework to enable participation through authorised representatives. This will take into account individuals under 18 years of age.

To best accommodate the range of circumstances relating to the capacity of individuals under 18 years of age, administrative arrangements and policy will supplement the legislation.

Proposal 6: Legislation will not prescribe the age at which a person under 18 years of age is presumed to have capacity to manage their own PCEHR.

Proposal 7: Consistent with the approach taken by Medicare Australia, an administrative/policy framework will provide for participation in the PCEHR system by minors. The general participation arrangements will apply as follows:

- up to 14 years of age – a parent or legal guardian will be responsible for the child's PCEHR, including whether to register the child for a PCEHR and managing the access controls of the child's PCEHR;
- 14 to 18 years of age – a young person will be presumed to have capacity to make decisions in respect of their PCEHR. If the child elects to manage their own PCEHR they can decide whether or not to participate in the PCEHR system and manage the access controls of their PCEHR including choosing whether to allow their parent or legal guardian access. If a young person chooses not to manage their own PCEHR, the parent or legal guardian would continue to manage the young person's PCEHR;
- 18 years and over – an individual takes responsibility for their own PCEHR. The PCEHR system will no longer allow a parent or legal guardian to access the individual's PCEHR unless the individual grants access to the parent or guardian as a nominated representative. Alternatively, if the individual has limited or no capacity, the arrangements for authorised representatives will apply and the representative will need to provide evidence of their legal authority for verification by the PCEHR system operator.

Requests by minors under 14 years of age to manage their own PCEHR will be considered on a case by case basis by the PCEHR system operator.

Q4. What other circumstances might need to be accommodated in the administrative arrangements for minors?

Pseudonymity

If an individual regularly uses a pseudonym to obtain healthcare, they may wish to access the benefits from having their healthcare information contained in a PCEHR.

The main themes that emerge from research into pseudonymous healthcare are that an individual may:

- seek to quarantine certain types of treatment or choose not to have some items loaded onto the PCEHR. For example, an individual may seek particular treatment, such as that for sexually transmitted infections, using a pseudonym so that the resulting information is contained in a pseudonymous PCEHR not connected to their true identity;
- fear exposure due to the public nature of their work; and
- fear being traceable when escaping family violence. In this situation an individual may have fears due to their ex-partner being an employee of a healthcare provider organisation and therefore capable of gaining access to their demographic details.

A PCEHR would need to be established using the pseudonym in order to retrieve any health information recorded under their pseudonym from different sources.

The HI Service already provides for pseudonymous healthcare identifiers. An individual can obtain a pseudonymous healthcare identifier from the HI Service which would be used by the PCEHR system along with the associated pseudonymous identity details. Pseudonymous use of the PCEHR system would be subject to the provisions of the HI Service relating to pseudonymous healthcare identifiers.

A pseudonymous PCEHR would not identify the individual's true identity or be linked to the PCEHR created in their true name (if they have created one).

Proposal 8: The PCEHR system will support the creation and use of a PCEHR using a pseudonymous identity and healthcare identifier.

Q5. What are the possible risks related to the creation and use of a pseudonymous PCEHR?

3.2.2 Healthcare provider organisations

Healthcare provider organisations have a key role in the PCEHR system in authorising users within the organisation to access and download healthcare information to assist in their treatment of a patient, and to upload information relating to healthcare events and shared health summaries.

A healthcare provider organisation would be permitted to authorise individuals within its organisation as users of the PCEHR system, such as individual healthcare providers, contracted service providers and other staff.

A healthcare provider organisation can only authorise a user if that user is involved in the provision or support of care to the individual and meets the eligibility requirements, which are:

- in the case of individual healthcare providers, that they have an Healthcare Provider Identifier—Individual (HPI-I); or
- in the case of other individuals within a healthcare provider organisation, such as contracted service providers and administrative staff, that sufficient information be provided to the PCEHR system to enable the user to be identified by name to the PCEHR system operator.

Healthcare provider organisations would need to register with the PCEHR system operator in order to participate in the PCEHR system. The draft Concept of Operations proposes that it would be a requirement of participation that a healthcare provider organisation has a Healthcare Provider Identifier—Organisation (HPI-O), the requirements for which are set by the HI Act.

Proposal 9: Legislation would specify that in order to be eligible to register for the PCEHR system a healthcare provider organisation must:

- have a HPI-O;
- conform to specified technological requirements; and
- agree to prescribed terms and conditions.

Proposal 10: Legislation would provide a framework for standards with which healthcare provider organisations must comply.

Proposal 11: Legislation would provide authority for the making of terms and conditions which will apply to a healthcare provider organisation regarding the authorisation and identification of eligible users of the PCEHR system within the organisation. The legislation will describe that, to be eligible as an authorised user:

- healthcare providers must have an HPI-I and be identifiable in the healthcare provider organisation's local system; and
- other individuals within a healthcare provider organisation, such as contracted service providers and administrative staff, must be identifiable in the healthcare provider organisation's local system and have a legitimate need to access the PCEHR system.

Q6. Are there other terms and conditions that should apply to healthcare provider organisations in regulating the eligibility of authorised users?

Nominated healthcare providers

Section 4.2 of the draft Concept of Operations describes clinical documents that will provide information that can be indexed by the PCEHR system and accessed through the consolidated view¹⁰ of a patient's PCEHR.

Most of the clinical documents described are already part of the healthcare information created in the current healthcare system, such as discharge summaries, referrals, specialist letters, and pathology or imaging reports. However, healthcare providers are proposed to have a key role in creating documents specifically for the PCEHR such as shared health summaries and event summaries. The shared health summary would contain key pieces of information about an individual's health status, such as allergies and adverse reactions, medicines, medical history and immunisations. The event summary would contain similar information in relation to a healthcare episode and would be created when something significant happens that is important to the individual's ongoing care.

The draft Concept of Operations proposes at 3.2.5 that an individual will be able to nominate a healthcare provider organisation, or individual healthcare provider, to be responsible for establishing and maintaining the individual's shared health summary. An individual could only nominate one healthcare provider organisation at a time to manage their shared health summary, however it would not be essential to have a nominated healthcare provider in order to have a PCEHR.

The legislation would not describe criteria or specific functions for the role of the nominated provider, however it would provide a framework for rules and

¹⁰ See section 4.3.3 of the draft Concept of Operation for details about the consolidated view

standards to which a nominated provider must comply in managing a shared health summary. These rules and standards may also relate to the authorship of other documents on the PCEHR system, such as event summaries.

Proposal 12: Legislation would provide a framework for rules and standards with which a nominated healthcare provider must comply in authoring and managing a shared health summary.

Proposal 13: The legislation may set out a framework for the rules and standards that relate to the authorship of other PCEHR documents.

Q7. What are the essential rules and standards with which a nominated healthcare provider should comply in relation to authoring and managing a shared health summary?

3.2.3 PCEHR system operator

The role of the PCEHR system operator is outlined in section 7.3 of the draft Concept of Operations. The PCEHR system operator will be responsible for providing key services which integrate the PCEHR system. It will be the point in the system where the various components are drawn together to provide an integrated service to individuals and healthcare provider organisations.

Regardless of the identity of the PCEHR operator, there are key functions that need to be performed, including the provision of:

- an indexing service which allows information in different repositories to be linked to the right person and retrieved when required;
- an audit service which tracks the flows of information into and out of a PCEHR, enabling consumers and healthcare provider organisations to monitor how information is being accessed;
- a viewing service which assembles a series of 'views' of an individual's PCEHR;
- a reporting service which allows tracking of the performance of the PCEHR system against key performance indications;
- a participation and authorisation service which manages administrative information, settings and preferences about individuals, their representatives and healthcare provider organisations;
- assessment of the eligibility of individual consumers, their representatives and healthcare provider organisations to participate in the PCEHR;
- registration of eligible individuals and healthcare provider organisations; and
- management of changes to access and enquiries and initial complaints about access matters.

Legislation could establish the system operator and prescribe the operator's functions and responsibilities, thereby authorising the operator to undertake its necessary functions and ensure that it is accountable for its responsibilities.

In performing some of these roles, the PCEHR system operator will need to obtain and use healthcare identifiers from the HI Service. The HI Service was established prior to the detail of the PCEHR system being developed, so it is proposed that amendments to the HI Act be made to explicitly support its handling of healthcare identifiers.

Proposal 14: The legislation would establish the PCEHR system operator, prescribe the operator's functions and responsibilities and establish an administrative framework for setting the service levels and operational rules that the PCEHR system operator would need to meet.

Proposal 15: The HI Act would be amended to explicitly support the use of healthcare identifiers by the PCEHR system operator.

Q8. What are the essential obligations that should apply to the PCEHR system operator?

3.2.4 Repository operators

Section 6.6 of the draft Concept of Operations outlines the role of conformant repositories that will store health information that can be indexed for access by the PCEHR system. The draft Concept of Operations proposes that there will be a number of nationally operated repositories (including for shared health summaries, event summaries, discharge summaries and consumer entered information) and other conformant repositories such as those operated by Medicare Australia (e.g. PBS history, organ donor and immunisation registers), diagnostic service repositories and regional or state/territory operated repositories.

Repository operators are organisations that hold health information which is available for retrieval by the PCEHR system operator when the system operator receives a request for access from an authorised user.

Conformant repositories enable information (as agreed by an individual) to be indexed by the PCEHR system so that it can be found and viewed by authorised users. Conformant repositories capture and store information from existing e-health processes, such as those supporting pathology and diagnostic imaging.

National Repositories Services will be used to store key information, such as Shared Health Summaries, Discharge Summaries and Consumer Entered Information which is not captured in a suitable repository. Authorised users will use the PCEHR system to load the information (as agreed by the individual) to the appropriate National Repositories Service.

The PCEHR system will need a manner by which it can recognise repository operators, thereby differentiating actions by repository operators from other users of the system. Legislation could establish a framework for allocating identifiers to repository operators.

In order to participate in the PCEHR system repositories will need to conform to particular standards and requirements.

Given the nature of the information that will be held in PCEHR-conformant repositories and their critical role in the PCEHR system, it is proposed that repository operators be subject to regulation, whether by primary legislation alone or in conjunction with other mechanisms, such as contracts. Such regulation would provide for accountability, conformance, retention of records, penalties and address circumstances where a repository fails.

A key factor in determining what aspects of the framework for a repository operator are in principal legislation and what requirements are prescribed elsewhere (e.g. in regulations, other legislative instruments, contracts) is the need to ensure sufficient flexibility in the regulatory system to accommodate changes in technology over time.

It is proposed that legislation will provide that one of the requirements for participating in the PCEHR system is that a repository operator stores all health records in Australia. Storage of information outside Australia would

provide very limited avenues for individuals in the event that their health information is misused or mishandled. Therefore it is proposed that information used for PCEHR purposes must be held in Australia.

To ensure that requirements can be enforced and penalties imposed on repository operators, legislation would need to require that a repository operator must be a defined legal entity.

Legislation would specifically identify the role of National Repositories Service and identify its operator, to reflect the central and unique role of a National Repositories Service in the effective operation of the PCEHR system. There may be particular criteria that would be applicable to the National Repositories Service, which are not appropriate for other conformant repositories.

Proposal 16:The legislation would define repository operators to include registry operators and provide a framework for the regulation of PCEHR-conformant repositories, including:

- a framework for allocating identifiers to PCEHR-conformant repositories;
- requiring that all health information used for PCEHR system purposes must be held in Australia; and
- requiring that repository operators are a legal entity within Australia.

Proposal 17:The legislation would establish the role of the National Repositories Service, identify its operator and provide any unique criteria which will apply to the National Repositories Service.

Proposal 18:Relevant legislation would be amended to enable specific data sources held by Medicare Australia to be compliant repositories for the PCEHR system.

Q9. What are the essential obligations that should be met by repository operators?

Q10. What additional criteria might be applicable to the national repositories?

3.2.5 Trusted data source providers

During the registration process for both individuals, healthcare providers and healthcare provider organisations, it may be necessary to use trusted data sources in order to verify identity information. Trusted data sources, such as Medicare Australia, are sources of data on which one can rely with confidence on the accuracy and integrity of the data.

Legislation is required to authorise the use of demographic and other data held by trusted data sources to ensure that using the information for verification purposes is authorised for a new purpose and does not constitute a breach of privacy legislation.

It is proposed that Medicare Australia, DVA and the Department of Defence be specified in the legislation as trusted data sources, with the ability to add future data sources through the regulations if necessary. Consequential amendments to other Commonwealth legislation will need to be made to allow access to data sources such as MBS and PBS data.

Proposal 19:The legislation will authorise the use of data held by Medicare Australia, DVA and the Department of Defence as trusted data sources for identity verification purposes.

Proposal 20:The legislation will allow for future trusted data sources to be identified through regulations.

Q11. Are there any other trusted data sources that should be included in the legislation from the outset of the PCEHR system?

3.2.6 Portal providers

Section 3.4.3 of the draft Concept of Operations describes how individuals and healthcare providers will be able to access records in the PCEHR system via conformant portals complying with the functionality and specification requirements set out in section 6.2.1 of the draft Concept of Operations.

The PCEHR system will need a manner by which it can recognise portal providers, thereby differentiating actions by portal providers from other users of the system. Legislation should establish a framework for allocating identifiers to portal providers.

In line with the proposals for repositories, legislation would provide that one of the requirements for participating in the PCEHR system is that a portal provider stores its servers and any demographic information in Australia.

To ensure that requirements can be enforced and penalties imposed on portal providers, legislation will require that a portal provider must be a legal entity.

Proposal 21:The legislation will provide for the participation of portal providers.

Proposal 22:The legislation will provide a framework for the regulation of PCEHR-conformant portals, including:

- a framework for allocating identifiers to PCEHR-conformant portals;
- requiring that all servers used for PCEHR system purposes and all demographic information used for PCEHR system purposes must be held in Australia; and
- requiring that portal providers are a legal entity within Australia.

Q12. Are there any other essential requirements for portal providers?

3.2.7 Intellectual property

There may be property rights, mainly copyright, in some of the documents which are potentially uploaded by a healthcare provider organisation into the PCEHR system. There needs to be management of these rights within the PCEHR system, whether by legislation or by contractual arrangements.

Proposal 23: The assignment of intellectual property rights for the PCEHR system would be based in either legislation or contract. The changes required will be further developed as feedback is received as part of the consultation process.

Q13. Are you aware of specific examples of information for which intellectual property rights might present a significant barrier to the use of the information in the PCEHR system?

3.2.8 Health records management

Enabling the consolidation of clinically relevant health information held in disparate systems operating under different management regimes is at the centre of the PCEHR system. This highlights the need for a records management policy to deal with the period for which records are retained and this may need legislative backing.

The draft Concept of Operations proposes that a PCEHR is intended to be active throughout the lifetime of the individual, unless deactivated. However, this concept needs to be balanced with the goal of providing access to clinically relevant information in a form that is easy to access. Too much data on view past the time it is clinically relevant could run counter to this goal.

The PCEHR system is also not intended to replace the full medical records held by healthcare providers.

Existing legislation/guidelines

There are multiple Commonwealth, state and territory legislative requirements in relation to retention timeframes of health records. [Appendix 4](#) sets out a table dealing with general record retention timeframe requirements.

In addition to legislative requirements there are other standards and guidelines in relation to the retention of health records, with further examples and detail at the end of [Appendix 4](#).

In summary:

- For health record information held in the public sector, the retention period ranges from a minimum of seven years from the last provision of a health service to an individual, to a minimum for 15 years.
- Medical insurers recommend retaining health records for as long as possible for medico-legal reasons.
- Some health records of a more sensitive/complex nature have specific and more onerous retention schedules, e.g. genetic testing and radiation oncology.
- State/territory specific legislation for retention of prescription information in relation to 'dangerous drugs' differs slightly across jurisdictions.

In order to be consistent overall with existing general requirements, the PCEHR repositories and portals could adopt the longest minimum jurisdictional requirement of 15 years, and ensure that it is clear to healthcare providers that if they need to comply in their records management with legislation or guidelines for specific information, then it continues to be their responsibility to do so.

Proposal 24: The legislation would require retention of documents which have been indexed/accessed by the PCEHR system for 15 years since last action on record (or in the case of a minor, until they are 30 years of age).

Q14. Can you identify any other options for records retention and can you identify any other issues regarding records management that have not been considered in this paper?

3.3 Access

Section 5.5 of the draft Concept of Operations outlines how participating individuals will be able to set their own access controls. With the individual's permission, key pieces of health information contained in the individual's PCEHR may be viewed by participating healthcare providers across different locations and healthcare settings.

Healthcare providers who are given access by a consumer to the consumer's PCEHR will be able to download health information from the PCEHR system into the healthcare provider's local system, where the information will be subject to the existing protections and controls applying to that particular healthcare provider.

3.3.1 Individuals

Individuals will have access to the information held by the PCEHR system, will be able to provide access to a nominated representative(s) and be able to choose how to provide access to their PCEHR to healthcare providers involved in their care.

In particular, individuals will be able to:

- decide whether or not to have an active PCEHR;
- access information in their PCEHR;
- set controls around healthcare provider organisation access;
- authorise others to access their PCEHR;
- choose which information is published to and accessible through their PCEHR;
- view an activity history for their PCEHR; and
- make enquiries and complaints.

Appropriate information and support will be available to individuals to clearly describe the options available for managing their provider access controls and for accessing their own information. Establishment and maintenance of these controls will be available via a range of channels.

Individuals will have the option of authorising all healthcare providers involved in their healthcare access to their PCEHR.

Individuals will be able to access their PCEHR online via a consumer or other PCEHR-conformant portal and will be able to:

- access their PCEHR;
- link to online health literacy information;
- share information with healthcare providers, including information about their allergies and over-the-counter medications. They will also be able to keep notes online as an aide memoir for themselves and their carers;

- manage their access controls and view the activity history of their PCEHR; and
- improve the quality of their health information by highlighting potential errors in their records and requesting the potential error be reviewed.

Other access channels will be provided for people who do not speak English, do not have access to the internet, cannot use a computer or have specific accessibility requirements.

Proposal 25: Legislation would set out the individual's role in setting access controls, authorising others to access their PCEHR, choosing which information is published to and accessible through their PCEHR, viewing an activity history for their PCEHR and making enquiries and complaints.

Q15. Are there additional access functions for individuals that need to be included in legislation?

Authorised representatives

As discussed in section 3.2.1, an authorised representative is an individual who is recognised by the PCEHR system to manage another individual's PCEHR.

An authorised representative will be able to view and control the access settings of the PCEHR for the person they represent, and enter information into that PCEHR.

Proposal 26: The broad framework which permits an individual to participate in the PCEHR system through an authorised representative (see proposal 3) will provide the necessary legislative support for access by authorised representatives.

Q16. Should any specific restrictions apply to the extent to which an authorised representative can act on behalf of the individual within the PCEHR system?

Nominated representatives

Access to health information may be a critical contribution to an individual's ability to provide care to another. While a subset of carers may be authorised by law, support for an informal caring relationship within the context of the PCEHR system is proposed in section 5.4 of the draft Concept of Operations, whereby a nominated representative would be permitted to view information in a PCEHR.

Arrangements for nominated representatives differ from the arrangements for authorised representatives since a nominated representative is not recognised by the PCEHR system as having legal authority to act on behalf of the individual.

A nominated representative will be able to view the individual's PCEHR but will not be able to manage the individual's PCEHR access controls or contribute information to the individual's PCEHR.

An individual can elect to have more than one nominated representative.

Legislation is required to ensure that in accessing an individual's PCEHR a nominated representative would not breach any privacy protections.

Proposal 27:The legislation would allow an individual to nominate one or more persons to be their nominated representative for the purpose of viewing the individual's PCEHR.

Q17. Are there any other essential or additional requirements or obligations of a nominated representative that should be supported in the PCEHR legislative framework?

Minors as representatives

There are a range of circumstances where a minor is in a caring or assisting role for an adult.

Authorised representatives are authorised by other legislation and the PCEHR system would rely on the restrictions and criteria applied by that external authorising framework.

To cater to a broad range of different personal circumstances and noting that a nominated representative is only permitted to view the individual's health information through the PCEHR, it is proposed that no age restrictions would be imposed in being recognised by the PCEHR system as a nominated representative.

Proposal 28:Legislation would not prescribe eligibility criteria for nominated representatives, thereby allowing for representation by minors.

Q18. Are there any reasons why an individual should not be able to choose a minor as their nominated representative?

Q19. Would it be desirable to include any other eligibility criteria for a nominated representative?

3.3.2 Healthcare provider organisations

Section 5.4.1 of the draft Concept of Operations describes how healthcare providers and authorised users within a healthcare provider organisation will be able to access an individual's PCEHR subject to the access settings established by the individual.

In particular, healthcare providers and other authorised users will be able to:

- find an individual's PCEHR and access, view and search it;
- download and/or print clinical documents and views in an individual's PCEHR; and
- upload clinical documents.

The technical settings in the PCEHR system will ensure that a healthcare provider or other authorised user can only access an individual's PCEHR if the individual has granted access, except in emergency circumstances.

Healthcare providers and other authorised users within healthcare provider organisations will be able to access the PCEHR system using a range of options, including:

- Clinical systems – many healthcare provider organisations have already invested in a clinical system for healthcare delivery. In time, a range of new versions of many of these systems will become available with built-in capacity to access the PCEHR system. The PCEHR system will also support contracted service providers who operate healthcare software as a service on behalf of the contracting healthcare provider organisation.
- Provider portal – healthcare providers and authorised users will be able to access health information stored in the PCEHR system via the provider portal. This portal will be supplied as an alternative form of access to the PCEHR system. Access to the provider portal must be authorised by the participating healthcare provider organisation.

A call centre will be provided to assist healthcare providers and other authorised users in accessing the system.

Proposal 29: Legislation is required to define authorised users who may access a PCEHR when they have been granted permission to do so by the healthcare provider organisation they work for and in line with the access control settings established by the individual.

Q20. Are there additional issues in relation to authorised users that should be addressed in the legislation or regulations?

Emergency access

If an individual is in need of emergency care and is not capable of giving consent for a healthcare provider organisation to access the individual's PCEHR, the PCEHR system will provide for emergency access. In establishing their access control settings, individuals will not be able to prohibit emergency access to their PCEHR.

This is consistent with the existing Australian privacy frameworks which provide that health information be disclosed to healthcare providers to prevent or lessen a serious or imminent threat to life or health.

Proposal 30: Emergency PCEHR access is already provided under existing privacy and health legislation.

Q21. Should there be additional legislative provisions for emergency access to PCEHR information?

3.4 Privacy – coverage

Existing framework

The way in which personal information and health information is collected, used, disclosed and stored is currently regulated by privacy arrangements that have been put in place by Commonwealth, state and territory governments. Within this framework:

- private sector and Commonwealth healthcare providers are subject to the Commonwealth *Privacy Act 1988* ('the Privacy Act')¹¹;

¹¹ Private sector healthcare providers may also be subject to health privacy legislation in the Australian Capital Territory, New South Wales and Victoria

- public sector healthcare providers are covered by state or territory privacy legislation in all jurisdictions, except Western Australia (WA) and South Australia (SA) which rely on administrative schemes, common law duties of confidentiality associated with confidential health records and health-specific legislation restrictions on the disclosure of health information.

Health Ministers agreed in December 2009 that they would work towards nationally consistent health privacy laws.¹²

In 2008 the Australian Law Reform Commission (ALRC) released a report on Commonwealth privacy law¹³ which identified the desirability of national consistency in privacy law.

In its initial response to the ALRC report, the Commonwealth indicated that an initial program of changes would be completed and these would '*create a platform from which it can pursue national harmonisation through discussion with the states and territories*'.¹⁴ Legislation to implement the first stage of changes to Commonwealth privacy law is planned to be introduced into the Parliament in late 2011.

Privacy coverage of the system operator, repository operators and portal operators

There will need to be clear and compatible privacy obligations for those organisations delivering the PCEHR services to individuals and healthcare providers, i.e. the system operator, repository operators and portal operators. The obligations will need to reflect that these roles are likely to be undertaken by Commonwealth, state, territory and private sector bodies.

The Privacy Act covers a wide range of Commonwealth agencies and private sector organisations. To the extent that a body is not currently covered by the Privacy Act, there are a number of opt-in mechanisms within the Privacy Act which allow its coverage to be extended to other bodies, with their agreement.¹⁵

System and portal operators

It may arise that a body wishes to participate in the PCEHR system as the system operator or a portal operator, and is not covered by the Privacy Act. It is proposed that the legislation establish a framework which either:

- applies the Privacy Act to that body where it is participating in the PCEHR system in one of these capacities; or
- requires the body to opt-in to and maintain coverage by the Privacy Act in order to be eligible to participate in one of these capacities.

This would mean that the PCEHR system operator and all conformant portal operators would be subject to the same privacy rules and regulator.

Repository operators

The Commonwealth is examining whether the proposed arrangements for the system and portal operators should apply to all repository operators as well. If this were the case, then state and territory bodies which became repository operators would become subject to Commonwealth privacy rules.

States and territories have expressed the view that state or territory privacy legislation would be the appropriate privacy obligations to apply to a state or

¹² See National Partnership Agreement on E-Health, Schedule A

¹³ *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108) 12 August 2008 (see <<http://www.alrc.gov.au/publications/report-108>>)

¹⁴ *Enhancing National Privacy Protection. Australian Government First Stage Response*, October 2009, p13 (see <<http://www.dpvc.gov.au/privacy/reforms.cfm>>)

¹⁵ See, for example, sections 6EA and 6F of the Privacy Act

territory body which was participating in the PCEHR system as a repository operator. An alternative approach which accommodates this view could be that repository operators be required to be covered by the Privacy Act or equivalent state or territory privacy legislation. For bodies which are not currently covered by Commonwealth, state or territory privacy legislation, the PCEHR legislation could then establish a framework which either:

- applies the Privacy Act to that body where it is participating in the PCEHR system as a repository operator; or
- requires the body to opt-in to and maintain coverage by the Privacy Act in order to be eligible to participate as a repository operator.

This would mean that there would be binding privacy legislation governing all repositories within the PCEHR system, but that it may not be the same legislation or regulator for all bodies.

To allow for differences between privacy legislation in each jurisdiction under this option, it may be necessary to include express reporting and information disclosure requirements to ensure that information flows smoothly between the service delivery bodies.

Proposal 31: In relation to the system operator and portal operators, the legislation should ensure that a body may not perform that role unless it is subject to the Privacy Act.

Proposal 32: In relation to repository operators, the legislation should ensure that a body may not perform that role unless it is subject to privacy obligations under Australian law.

Q22. Will this provide the necessary level of protection for personal information uploaded to the PCEHR system?

Q23. What privacy legislation should apply to repository operators?

Privacy coverage of healthcare providers

Covering the PCEHR system operator and PCEHR-conformant repositories and portals under the Privacy Act provides protection for information that is uploaded to the PCEHR system. However, section 4.2.1 of the draft Concept of Operations describes that healthcare providers will be able to download health information which they have permission to access, into their local systems. The downloaded information would then continue to be subject to the privacy coverage provided by existing law. This means that:

- all private sector and Commonwealth healthcare providers will be subject to the Privacy Act, and some will also be subject to privacy obligations under Australian Capital Territory (ACT), New South Wales (NSW) or Victorian legislation; and
- public sector healthcare providers will be subject to the privacy legislation or administrative arrangements in their jurisdiction.

WA and SA do not currently have specific privacy legislation and instead rely on health law and administrative arrangements for the protection of personal information. The Commonwealth continues to investigate and discuss with states and territories options for improving the consistency of privacy coverage around Australia.

This will mean that privacy coverage of health information downloaded from the PCEHR system and into healthcare providers' local systems will be subject to differing obligations around the country. Rather than result in additional complexity, this would reflect current privacy arrangements when clinical information is shared between sectors with different existing coverage.

Proposal 33:Healthcare providers will be subject to the privacy coverage provided by existing law.

Q24. Are there any reasons why clinical information downloaded from the PCEHR system should be required to be handled differently to other information held by a healthcare provider in their local records?

Q25. If so, how could the practical difficulties be overcome?

3.4.1 Privacy – use and disclosure of information

The PCEHR system is intended to facilitate the sharing of information to support healthcare services. Accordingly, the information flows in a PCEHR should follow the existing framework for the sharing of information between healthcare providers. If the information flows are different, a PCEHR system potentially adds to the complexity facing healthcare providers.

As a result, it is proposed secondary uses and disclosures of personal information permitted under the Privacy Act will continue to be allowed in the PCEHR system.

Those secondary uses and disclosures include:

- use or disclosure authorised or required by or under law (including a subpoena issued by a court, and public health and child welfare reporting obligations in state and territory legislation);
- use or disclosure to prevent or lessen a serious and imminent threat to life and health; and
- use or disclosure for law enforcement purposes.

An exception to this might be if state or territory health legislation imposes reporting or secrecy obligations which are inconsistent with the operation of the PCEHR system. In those cases, there may be some need for legislation to address the interaction of the state or territory law and the operation of the PCEHR system. There have been no circumstances where this would be required which have been identified to date, and the aim is to disturb existing state and territory obligations as little as possible.

Proposal 34:The legislation would not displace the exceptions to the prohibition on use and disclosure of health information in the Privacy Act. The Commonwealth will work with states and territories to identify any existing reporting or secrecy provisions that may impact on the operation of the PCEHR system.

Q26. Are you able to provide examples of existing reporting or secrecy provisions that might impact on the PCEHR system operations?

3.5 Security

Section 5.3 of the draft Concept of Operations outlines that authentication, authorisation and encryption are key aspects of the system's security and proposes a multi-layered approach within a Security and Access Framework. Security is about putting systems and processes in place which mitigate risk,

both when the PCEHR system is established and over time as technology and the needs of the community evolve.

Risks to the effectiveness and efficiency of the PCEHR system include:

- unauthorised access to information;
- unauthorised use or disclosure of information; and
- damage to the operability of the system.

There is not a single or immutable solution to any of these risks. As a result the PCEHR system security is addressed with a range of strategies. These include:

1. **design principles** – for example, the use of a distributed series of conformant repositories rather than a single consolidated store of personal data. This reduces the potential damage caused by unauthorised access to a single repository;
2. **technical design** – for example, drawing on national and international best practice in the development, maintenance and renewal of computer solutions to security risks;
3. **participation criteria** – for example, establishing registration processes and criteria which rigorously test the rights of individuals and healthcare providers to participate in the system (see 3.2.1);
4. **complaints and accountability** – for example, the ability to make a complaint to a privacy regulator (see 3.6.2);
5. **offences and penalties** – for example, criminal consequences for serious misconduct relating to the unauthorised access to and use of personal information held in the PCEHR system (see 3.5.1).

It may not be appropriate to address technical design issues specifically in legislation because of the rapid pace of technological change. Retaining control of technical specifications at a policy level provides greater flexibility to both adopt new and more efficient technologies, and also to respond quickly to new and emerging risks.

The importance of the technical design will still come through indirectly in other legislated areas. For example, participation requirements include obligations on healthcare providers connecting to the system to meet and maintain system conformance standards (see 3.2.2).

Proposal 35: The legislation will provide a framework to support ongoing security of the PCEHR system, but will not set technical requirements, to allow for quick and flexible responses to technological change.

Q27. Are there technical aspects of the PCEHR system design that are so critical to security and sufficiently stable over time as to warrant inclusion in the legislation or regulations?

3.5.1 Offences and penalties

It is proposed that a combination of existing and new criminal provisions should provide appropriate penalties for serious misconduct in relation to the PCEHR system. These provisions are similar to the provisions that currently apply to the HI Service.

The PCEHR system will use healthcare identifiers as part of the information used to index health information for access through a PCEHR, during registration of individuals, healthcare providers and healthcare provider organisations. Because healthcare providers who are accessing records in the

PCEHR system are using healthcare identifiers to do so, they are subject to the provisions in the HI Act covering the inappropriate use or disclosure of healthcare identifiers. This would mean, for example, that the use and disclosure of a healthcare identifier to obtain access to a PCEHR for a purpose other than one recognised by the HI Act would be the commission of an offence under section 26 of the HI Act punishable by two years' imprisonment or 120 penalty units.

In addition, it is proposed that specific offences be imposed on healthcare providers participating in the PCEHR system. The content of those offences will be shaped by the final design of the PCEHR system but are likely to address:

- failure of a registered healthcare provider to notify the PCEHR system operator within a specified period when it ceases to meet the requirements for registration to participate in the PCEHR system;
- requests for and receipt of a record from the PCEHR system by a healthcare provider when the provider or her/his requesting employer or contractor is not authorised to do so; and
- failure of a registered healthcare provider to meet audit trail or other record-keeping obligations imposed by the legislation.

The offences in the regulations each attract a penalty of 50 penalty units (currently equivalent to \$5,500).

These offences would be directed to officeholders or other legal entities involved in the management or control of the healthcare provider. This reflects that the obligations relate to matters of management control and responsibility.

In addition, employees of the service operator will be covered and subject to penalties such as misuse and inappropriate access to information.

Proposal 36: Criminal offences would be included in PCEHR legislation covering officeholders or other legal entities involved in the management or control of the healthcare provider, to address:

- failure of a registered healthcare provider to notify the PCEHR system operator within a specified period when it ceases to meet the requirements for registration to participate in the PCEHR system;
- requests for and receipt of a record from the PCEHR system by a healthcare provider, when the provider or her/his requesting employer or contractor is not authorised to do so; and
- failure of a registered healthcare provider to meet audit trail or other record-keeping obligations imposed by the legislation.

Q28. Is the size of the penalty (50 penalty units or \$5,500) used in the HI Service appropriate for the PCEHR system?

Q29. Is it appropriate to impose a penalty on the individual who requests a record from the PCEHR system when not entitled to do so?

It is proposed that penalties also apply to a repository operator or portal operator where it fails to notify the HI Service within a specified period when it ceases to meet its requirements for participation in the PCEHR system. As

the roles and responsibilities of repositories and portals are further developed, there may be additional penalties which will be considered.

Again, as the offence relates to matters of management control and responsibility, these penalties would apply to officeholders or other legal entities involved in the management or control of the operator.

In addition, employees of the repositories will also be covered and subject to penalties such as misuse and inappropriate access to information.

Proposal 37: Criminal offences would be included in PCEHR legislation which relates to the participation in the PCEHR system by a repository or portal operator, where that body has failed to meet or maintain the requirements for participation in the system.

Q30. What specific breaches of requirements should result in an offence and penalty for repository or portal operators?

The PCEHR system is designed to build on the existing flows of information between healthcare providers allowable under the Privacy Act, so that better care is delivered to patients. To support this aim, it is proposed that the Privacy Act would provide the appropriate confidentiality obligations for the PCEHR system operator.

The Privacy Act is based on broad principles so that decisions about whether information can be shared can be made on the facts of the particular case.

In the absence of specific confidentiality obligations on the PCEHR system operator and its staff, inappropriate handling of personal information will be subject to investigation and determination by the Australian Information Commissioner. Where that handling constitutes a criminal offence under another statute, then the relevant police force is responsible for investigation and prosecution.

If the operator is an 'agency' subject to the Commonwealth *Public Service Act 1999* then employees are subject to the obligations of the Australian Public Service Code of Conduct ('the Code'). Serious breaches of privacy, such as browsing of records, can be dealt with by agencies as a breach of the Code which are subject to disciplinary sanctions. These sanctions range from counselling to termination of employment.

Privacy breaches by contractors are dealt with in accordance with the contract with the agency.

Proposal 38: The legislation may not include an obligation of confidentiality on the PCEHR system operator or its employees or contractors. Instead, inappropriate handling of personal information would be dealt with under existing privacy, disciplinary or criminal law.

Q31. If the system operator is an agency and its employees are subject to the Code, would these disciplinary measures be sufficient?

Q32. If the PCEHR system operator is a private sector organisation would additional mechanisms be required?

Existing identity crime provisions

The Commonwealth has recently introduced identity crime offences in Part 9.5 of the Commonwealth Criminal Code. These offences are:

- An offence of making, supplying or using identification information with the intention that a person will pass themselves off as another person, for the purpose of committing, or facilitating the commission of, a Commonwealth indictable offence (an offence punishable by more than 12 months' imprisonment). This offence is the main identity crime offence, known as the 'dealing offence'.
- An offence of possessing identification information with the intention of using that information to engage in the dealing offence.
- An offence to possess equipment where the person intends to use, or allows another person to use, that equipment to make identification documentation for the purpose of the dealing offence.

The PCEHR system is an initiative which has been developed in collaboration with the states and territories, and they continue to play a significant role in the governance of the e-health system. It is proposed to be established under Commonwealth law however, and as such it is considered appropriate that the Commonwealth should be responsible for prosecution of crimes intimately connected with the operation of the system.

As a result, it is proposed that the Commonwealth consider the coverage of the identity crime and other related Commonwealth offences to assess whether they would capture PCEHR-related identity crime matters, or whether there is a need to include offences within the PCEHR legislation to specifically capture identity crime-related conduct involving a PCEHR.

Proposal 39: The Commonwealth will assess the coverage of existing Commonwealth offences to determine whether specific PCEHR offences are needed to better enable the Commonwealth to have jurisdiction in PCEHR-related identity crime matters.

Maintaining system integrity

The Commonwealth has cyber crime offences which are based on model provisions developed in collaboration with all states and territories. As a result, the Commonwealth offences are substantially the same as those in other jurisdictions which have also enacted the model provisions, which are NSW, Victoria, SA, the Northern Territory (NT) and the ACT. Computer offences in Queensland, Tasmania and WA are not as aligned with the model provisions.¹⁶ The Commonwealth's computer offences are directed to the problems of hacking, denial of service attacks and malware intrusions. Because of constitutional limitation on the Commonwealth's ability to legislate against criminal activity, the Commonwealth offences currently apply only to the:

- protection of Commonwealth computers and computer systems, and data held on behalf of the Commonwealth; and
- commission of crimes by means of a carriage service (such as the internet).¹⁷

There may be some circumstances where PCEHR-related misconduct would not be covered by the current Commonwealth offences, for instance where:

¹⁶ *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*, House of Representatives Standing Committee on Communications, June 2010 (see <<http://www.aph.gov.au/house/committee/coms/cybercrime/report.htm>>)

¹⁷ *Ibid*, p104

- the access to the data is **not** made using a carriage service; and
- the data is **not** stored in a Commonwealth computer or on behalf of the Commonwealth.

On 22 June 2011 the Government introduced the Cybercrime Legislation Amendment Bill 2011 into the Parliament. The Bill will amend the current Commonwealth offences in the *Criminal Code Act 1995* to bring Australian law into line with its obligations under the Council of Europe by removing the constitutional limitations in the Commonwealth provisions. The amendments will retain the existing savings provisions in the Criminal Code so that it is clear that it is not the Commonwealth's intention to displace any state or territory offences.

Proposal 40: The Commonwealth will seek to amend its existing computer offence provisions to remove existing constitutional limitations. This will enable the offences to apply to all PCEHR-related cyber crime matters.

3.6 Governance

3.6.1 Principles for long-term governance

The issue of governance concerns the management and operation of the PCEHR system in particular, and e-health more generally. The principles for long-term governance have been canvassed in the National E-Health Strategy and the report *A National Health and Hospitals Network for Australia's Future: Delivering the Reforms*.

The National E-Health Strategy notes that the current governance arrangements for e-health reflect the degree of ultimate accountability that Australian governments have for national healthcare funding and the delivery of outcomes.

The Strategy identifies a set of seven governance principles that should underpin the design of the national e-health governance structure¹⁸: accountability, transparency, appropriate stakeholder representation, sustainability, support for activity at multiple levels, effective leadership and coordination, and balancing local innovation and national outcomes.

The key functions which need to be provided for through the governance arrangements include:

- **Strategic:** The strategic oversight function would include high level decision-making and planning such as developing and implementing national policies and determining directions, at the direction of Health Ministers or in consultation with Health Ministers.
- **Operational:** The operational management function would include responsibilities such as managing assets, maintaining and upgrading equipment, and engaging and managing service providers for the information communication technology infrastructure. This would also extend to benefits realisation and change and adoption activities and work programs.
- **Regulatory:** The regulatory oversight function would concern issues such as the development, accreditation and enforcement of operational and system standards, compliance and possibly the imposition of penalties following complaint investigations for breaches.

¹⁸ *National E-Health Strategy*, 30 September 2008, Commonwealth of Australia, p 63 Fig 5-7

The issues identified as potentially requiring some form of day-to-day management and requiring a primary and secondary legislative response will most likely include, but are not limited to:

- Commonwealth requirements for participation and access settings;
- national infrastructure and asset management, including repositories;
- contractor and contract management;
- determination of operational and system standards;
- compliance framework for standards;
- training and system education;
- establishment and operation of a call centre and a consumer enquiry capacity;
- establishment and monitoring of audit activities;
- investigation and penalties framework for misuse of the system;
- liability and responsibility of repository providers;
- development of privacy and consent arrangements;
- clinical governance;
- development of national components such the National Authentication System for Health;
- definition of compliance schedules; and
- establishment of repository compliance standards.

It is anticipated that the PCEHR system operator will be prescribed in the PCEHR legislation. The Government is considering this issue as part of the governance discussion.

Q33. What are your views about the preferred governance structures for the PCEHR system and national e-health elements more broadly?

3.6.2 Complaints handling scheme

Individuals who are unhappy with the way their personal information is handled by the PCEHR system operator, a repository operator or a portal operator will have the ability to escalate their complaint to the Australian Information Commissioner if they are not satisfied with the response they receive from the operator.

Similarly, individuals will be able to escalate complaints about privacy matters relating to private sector healthcare providers who access health information through the PCEHR system to the Commonwealth Privacy Commissioner. In many jurisdictions they will also have rights to complain to a state or territory privacy or health service regulator.

Where an individual is unhappy with the conduct of a public sector healthcare provider then the individual may make a complaint to an appropriate regulator in the state or territory.

This means that there are multiple regulators around the country who could potentially have jurisdiction over a complaint relating to personal information which goes into, or comes out of, the PCEHR system. As a result, identifying rights and obligations can be confusing.

The Commonwealth, in collaboration with the states and territories, is developing proposals for a single entry point for PCEHR privacy complaints which are then referred to the appropriate regulator(s). It is likely that this will be an administrative arrangement rather than a legislative one.

Proposal 41: The Commonwealth, in collaboration with the states and territories, will develop proposals for a single entry point for PCEHR privacy complaints which are then referred to the appropriate regulator(s).

Q34. What would be your preferred single entry point for PCEHR privacy complaints?

4 Next steps

When the opportunity to provide comment on the legislation issues related to the PCEHR closes on 3 August 2011, the content of submissions and the feedback received during the public consultation process will be collated and consolidated. It is expected that this may take up to one month.

The input received as part of this process will inform the drafting of the legislation. Further public comment on legislative proposals will be sought during the August to September 2011 period.

It is planned that legislation be introduced into the Parliament in the 2011 Spring sittings.

Appendix 1: Acronyms and key definitions

ALRC	Australian Law Reform Commission
COAG	Council of Australian Governments
Code	Australian Public Service Code of Conduct, made under the <i>Public Service Act 1999</i>
Draft Concept of Operations	<i>Draft Concept of Operations—Relating to the introduction of a PCEHR system</i> , released on 12 April 2011 and available at < www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/pcehr >.
DVA	Department of Veterans' Affairs
NEHTA	National E-Health Transition Authority Established by the Council of Australian Government in 2005 to develop standards and manage the development of systems to support connectivity and interoperability of electronic health information systems across Australia
FOI	Freedom of Information The <i>Freedom of Information Act 1982</i> provides for individuals to see documents held by federal government ministers, their departments and most statutory authorities; ask for information concerning them to be changed if it is incomplete, out of date, incorrect or misleading; and appeal against a decision not to grant access to a document or amend or annotate a personal record
HI	Healthcare identifier Established under the <i>Healthcare Identifiers Act 2010</i>
HI Act	<i>Healthcare Identifiers Act 2010</i>
HI Service	Healthcare Identifiers Service The service that allocates, maintains and manages healthcare identifiers, established under the <i>Healthcare Identifiers Act 2010</i>
IHI	Individual Healthcare Identifier The identifier allocated to an individual (i.e. someone that has received, is receiving or will receive healthcare in Australia)
HPI-I	Healthcare Provider Identifier—Individual The identifier allocated to an individual healthcare provider
HPI-O	Healthcare Provider Identifier—Organisation The identifier allocated to a healthcare provider organisation
NASH	National Authentication Service for Health A secure and authenticated service for healthcare organisations and personnel to exchange e-health information
PBS	Pharmaceutical Benefits Scheme
PCEHR	Personally controlled electronic health record
Privacy Act	Commonwealth <i>Privacy Act 1988</i>

Appendix 2: E-health and national healthcare identifiers

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.

At present, there is limited ability to effectively share patient health information in the course of delivering healthcare services, particularly when patients move between healthcare sectors and providers.

Poor availability of health information across healthcare settings can be frustrating for patients and their healthcare providers. Also, it is a barrier to individuals managing their own health. It can also result in adverse drug events, medication errors and poor transitions as patients move from one healthcare setting to another.

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.

E-health is an integral part of the Australian Government's agenda for health reform which aims to create a continuously improving healthcare system for the 21st century; a system that is accountable, affordable and sustainable, with safety and quality at its centre.

Key elements that are central to the successful implementation of a national e-health system are the establishment and implementation of national healthcare identifiers for consumers and healthcare providers, widespread use of secure standards-based health communications, electronic authentication mechanisms for healthcare providers and the establishment of robust regulatory arrangements to ensure appropriate safeguards for patient health information and encourage participation in e-health initiatives.

Significant work has been undertaken by all governments in relation to the development of national healthcare identifiers and to address health information regulatory issues nationally. The National E-Health Transition Authority (NEHTA), a company established by all governments in 2005 to develop better ways of electronically collecting and securely exchanging health information has been working to develop the standards and infrastructure needed for e-health and which underpin the personally controlled electronic health record (PCEHR) system.

In 2006 the Council of Australian Governments (COAG) agreed to a national approach to healthcare identifiers as part of accelerating work on electronic health records to improve the safety of patients and improve efficiency for healthcare providers.¹⁹

The design and development of national infrastructure for national healthcare identifiers was undertaken by NEHTA. The implementation of healthcare identifiers is supported by a strong and effective legislative framework that includes governance arrangements, permitted uses and privacy safeguards. The Healthcare Identifiers Service ('HI Service') was established by the

¹⁹ Council of Australian Governments Communiqué, 10 February 2006

Healthcare Identifiers Act 2010 and commenced operation on 1 July 2010. Medicare Australia is the HI Service operator.

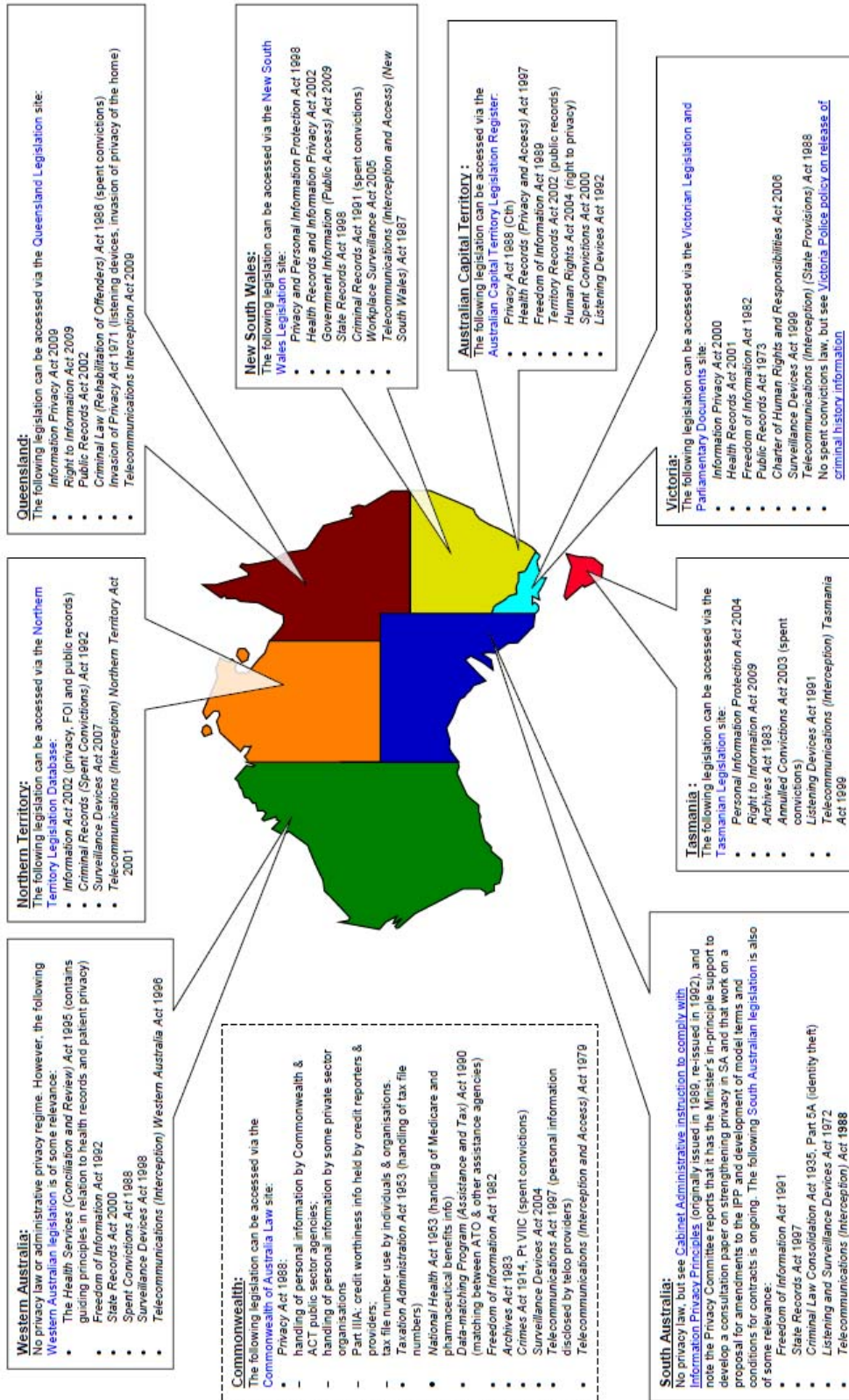
Three unique identifiers are assigned and issued by the HI Service. An Individual Healthcare Identifier is assigned to all individuals receiving health services in Australia. Individual healthcare providers are assigned a Healthcare Provider Identifier—Individual, and healthcare provider organisations are assigned a Healthcare Provider Identifier—Organisation.

Healthcare identifiers issued by the HI Service are designed to be used by individuals and organisations as part of reliably managing and communicating health information in the delivery of healthcare services. Identifiers are added to a healthcare provider organisation's patient administration and medical records. 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 HI Service is a fundamental starting point for secure, reliable electronic exchange of information for healthcare purposes.

Appendix 3: Privacy laws in Australia

PRIVACY & RELATED LEGISLATION IN AUSTRALIA



Note: For Queensland, refer also to the *Health Services Act 1991*.

Last updated 24 December 2010

Office of the Victorian Privacy Commissioner

Appendix 4: State/territory general medical record retention requirements

State/territory	Legislation	Requirement(s)	Timeframe
New South Wales	<i>Health Records and Information Privacy Act 2002</i> (HRIPA)	Section 25 of the Health Records and Information Privacy Act requires private sector persons who are health providers to retain health information relating to an individual as follows: (a) in the case of health information collected while the individual was an adult, for seven years from the last occasion on which a health service was provided to the individual by the health service provider; (b) in the case of health information collected while the individual was under the age of 18 years, until the individual has attained the age of 25 years.	Seven years in general across public and private sector
	<i>Health Practitioner Regulation (New South Wales) Regulation 2010</i>	Under regulation 10 of the Health Practitioner Regulation (New South Wales) Regulation medical practitioners and medical corporations must keep medical records for a certain period. 'A record must be kept for at least seven years from the date of last entry in the record, unless the patient was less than 18 years old at the date of last entry in the record. If the patient was less than 18 years old at the date of last entry in the record, the record must be kept until the patient attains or would have attained the age of 25 years' (this is consistent with the HRIPA above).	
	<i>State Records Act 1998</i>	Like the Commonwealth <i>Archives Act 1983</i> , the State Records Act requires state and local government agencies to maintain public records, and grants the public a right of access to some records, including some personal information, after 30 years. However personal health records held by NSW health agencies are closed to public access for 110 years (as per Attorney-General's Guidelines, Making Access Directions under the <i>State Records Act 1998</i>).	

Victoria	<i>Health Records Act 2001</i>	<p>The Health Records Act's Health Privacy Principle 4.2 imposes specific requirements for the retention of personal health information:</p> <ul style="list-style-type: none"> • for adults, seven years from the last entry; • for records created when a patient was less than 18 years, until they reach 25 years. <p>The retention requirements specified above do not apply where the <i>Public Records Act 1973</i>, the regulations or any other Act specifies a minimum retention period that is of a longer or shorter duration.</p> <p>The General Retention and Disposal Authority for Public Health Services Patient Information Records ('the Authority') was established under section 12 of the Victorian <i>Public Records Act 1973</i>. The effect of the Authority is that the medical records of individuals who receive treatment as admitted patients in Victorian public hospitals must not be destroyed until 15 years after the last attendance, or access on behalf of the patient, provided the patient has reached 25 years of age.</p>	Seven years in general; 15 years in public hospitals
Australian Capital Territory	<i>Health Records (Privacy and Access) Act 1997</i>	<p>Under the Health Records (Privacy and Access) Act, health records are required to be retained by the record keeper until:</p> <ul style="list-style-type: none"> • if the consumer is under 18 years old when the information is collected, the day the consumer turns 25 years old; or • if the consumer is an adult when the information is collected, seven years after the day a service was last provided to the consumer by the record keeper. 	Seven years in general across public and private sector
Queensland	<i>Public Records Act 2002</i>	<p>As required by section 13 of the Public Records Act, disposal of public records can only be undertaken with the authorisation of the State Archivist. In line with these requirements, Queensland Health has an approved retention and disposal schedule which allows for the disposal of adult health records 10 years after the last patient/client service provision or medico-legal action. In the case of minors, disposal is allowed 10 years after the patient/client has turned 18 AND 10 years after last patient/client service provision or medico-legal action.</p>	10 years in general, specified for public sector only

Western Australia	<i>State Records Act 2000</i>	The State Records Act places obligations on state and local government agencies to keep and retain public records for a certain period by developing record-keeping plans which outline these retention periods, e.g. WA Health Patient Information Retention and Disposal Schedule, which must be approved by the State Records Commission. According to the schedule, health records of discharged patients and outpatients from acute hospitals are generally allowed to be disposed 15 years after the date of last attendance or last access (provided the patient has reached the age of 25 years). Under section 49 of this Act access to personal medical and disability information held in the State Archive is not normally allowed unless the person concerned has consented or the information is at least 100 years old.	15 years in general, specified for public sector only
Tasmania	<i>Archives Act 1983</i>	The Archives Act provides that disposal of public records can only be undertaken with the authorisation of the State Archivist. Accordingly, the Archives Office has given approval through Retention Schedule DS20 to the relevant authorities to manage the disposal of health records. Disposal of individual patient records in acute hospitals is generally allowed 15 years after the last attendance or last access on behalf of patient (provided the patient has attained the age of 30 years). Note: requirement for emergency departments is seven years after attendance, regardless of age.	15 years in general, specified for public sector only
South Australia	<i>State Records Act 1997</i>	The State Records Act imposes obligations on state and local government agencies to keep and retain public records.	Public sector only (retention schedule not publicly available)
Northern Territory	<i>Information Act 2002</i>	Section 134 of the Information Act requires public sector organisations to keep records and make arrangements 'for the records service and archives service to monitor the management of its records'.	Public sector only (retention schedule not publicly available)