

Privacy Impact Assessment Report

Personally Controlled Electronic Health Record (PCEHR)

Prepared for the Commonwealth Department of
Health and Ageing

15 November 2011

MinterEllison

L A W Y E R S

Privacy Impact Assessment Report - PCEHR

Table of Contents

Chapter 1 - About this report	6
1.1 Privacy Impact Assessments	6
1.2 How should this PIA be used?	7
1.3 The process of assessing privacy impacts	8
1.4 Qualifications and Assumptions	10
Chapter 2 - Description of the PCEHR System	12
2.1 Overview of the PCEHR System	12
2.2 Key design features of the PCEHR System	12
2.3 The current state of play	14
2.4 An overview of privacy and security measures	16
2.5 Scope and reach	17
2.6 PCEHR System Participants	18
2.7 Individual participants	21
2.8 Healthcare participants	24
2.9 How personal information will flow through the PCEHR System	27
2.10 Features of the PCEHR System for the purposes of this assessment	28
Chapter 3 - Privacy principles used in this assessment	29
3.1 Overview	29
3.2 Collection of personal information	29
3.3 Data security	30
3.4 Access and correction	30

3.5	Data quality	30
3.6	Use and disclosure	31
Chapter 4	- Registration and creation of a PCEHR	32
4.1	Registration procedure	32
4.2	Limits to choice of channel	34
4.3	Activation: online channel	35
4.4	Activation: face to face channel	40
4.5	Activation: mail channel	41
4.6	Assisted Registration – verification of identity	42
4.7	Activation: authorised representatives must use assisted channels	43
4.8	Pre-population of data into PCEHR	45
4.9	Setting consumer controls	48
Chapter 5	- Access to and use of a PCEHR	55
5.1	Consumer access	55
5.2	Healthcare provider access	63
5.3	Healthcare provider access: download	65
5.4	Healthcare provider access: viewing a downloaded record	68
5.5	Healthcare provider access: restrictions on viewing	70
5.6	Healthcare provider access: upload	77
5.7	Third party access	84
Chapter 6	- PCEHR suspension, deactivation and reactivation	89
6.1	Overview of suspension, deactivation and reactivation	89
6.2	Suspension of a PCEHR	89
6.3	Deactivation of a PCEHR	91

6.4	Reactivation of a PCEHR	97
	Chapter 7 - System Operator	99
7.1	Governance structure	99
7.2	Reporting	99
7.3	Audit logging of access and use	100
7.4	External audit	102
7.5	Accountability of the System Operator	104
	Chapter 8 - Governance of the broader PCEHR System	107
8.1	Ensuring enforceable privacy responsibilities for participants	107
8.2	Ensuring enforceable privacy rights for consumers	110
8.3	Complaint handling	116
8.4	Obligations of participating organisations	118
8.5	Data storage	118
8.6	Protecting privacy into the future	120
	Chapter 9 - Conclusions & Recommendations	123
9.1	Phase One Conclusions	123
9.2	Phase Two Recommendations	137
	Schedule 1 List of Consultations and submissions reviewed	139
	Schedule 2 Privacy Legislation Considered (Phase One)	141
	Schedule 3 - Glossary and acronyms	143
	About the authors	152
1.	Minter Ellison	152
2.	Salinger Privacy	152

Introduction

The Australian Government through the Department of Health and Ageing (**Department**) proposes to introduce and implement a personally controlled electronic health record (**PCEHR**) system to enhance Australia's healthcare system. The PCEHR System is intended to enable the secure sharing of health information between an individual's healthcare providers, whilst enabling the individual to control who can access their PCEHR.

For the Australian Government to fulfil the objectives of improving the health system in this way it must demonstrate that every attempt has been made to achieve the appropriate balance between the competing objectives of multiple distributed access to health information and minimising any unnecessary and avoidable privacy intrusions. It will need to ensure that any unnecessary privacy intrusions have been avoided, and any remaining privacy impacts are proportionate to the risks, and justified by positive outcomes.

This Privacy Impact Assessment (**PIA**) has examined both the 'privacy positives' and the privacy risks arising from the design of the PCEHR System on the basis of the information provided to us. For each identified risk we have also recommended one or more ways in which to remove or mitigate that risk.

A summary of the privacy positives, risks and mitigation measures are set out in Chapter 9.

As the Australian Law Reform Commission (**ALRC**) has recognised, there are significant potential benefits to healthcare quality and safety that a shared electronic health record may deliver, but that 'such schemes will work effectively only if there is a sufficient degree of public trust and public confidence in the schemes and their administration.'

We trust that this PIA will contribute towards the Australian Government achieving the necessary balance of objectives.

Minter Ellison

15 November 2011

Chapter 1 - About this report

1.1 Privacy Impact Assessments

1.1.1 What is the scope of this PIA?

- (a) The primary purpose of this report is to analyse the possible impacts on the privacy of consumers' personal information in the PCEHR System by reference to Australian privacy laws (as at 31 August 2011) and to identify and recommend options for managing, minimising or eradicating these negative impacts.
- (b) This report is written in two phases.

Phase One

- (c) Phase One of this report identifies the potential privacy impacts of the proposed PCEHR System as at 16 September 2011, having regard to community values and expectations with respect to privacy by reference to:
 - (i) the submissions received by the Department and provided to us in response to:
 - (A) the Concept of Operations (version publicly released and dated 8 April 2011); and
 - (B) the Legislation Issues Paper; and
 - (ii) records of consultation conducted by the Department as provided to us.
- (d) Specifically, this phase of the PIA has been undertaken by reference to the following:

Intended design	the draft Concept of Operations (NeHTA, version 0.13.6, 8 April 2011), the revised Concept of Operations (NEHTA, version 0.14.12 August 2011) and as represented by representatives of the Department and NeHTA
Intended legislative underpinnings	as represented in the Legislation Issues Paper (the Department, July 2011)
Possible governance arrangements	as represented and instructed by representatives of the Department and NeHTA

- (e) Phase One was undertaken jointly by Minter Ellison and Anna Johnston of Salinger Privacy.

Phase Two

- (f) Chapters 4 to 9 of this report also contain annotations that address whether Legislation Submissions give rise to privacy impacts and risks concerning the PCEHR System that are not otherwise considered in this report together with comments and recommendations as to whether the Department should manage those privacy risk through the PCEHR Legislation.
- (g) Phase Two was undertaken by Minter Ellison. Salinger Privacy was unavailable at the time the Phase Two work was performed.

1.1.2 What is *not* in scope for this PIA?

- (a) This PIA report:
 - (i) does not address versions of the Proof of Concept document other than those versions specified in section 1.1 or documents not specified in Schedule 1;
 - (ii) is not an assessment of the adequacy of information security arrangements for the proposed PCEHR System. While ensuring appropriate data security is a critical privacy principle, expert assessment of the adequacy of information security arrangements will be required as the project moves towards a more detailed, operational level of design;
 - (iii) does not assess the proposed PCEHR System with respect to compliance with the proposed Australian Privacy Principles (**APPs**). This assessment has focused on the existing state of privacy regulation in Australia;
 - (iv) does not assess privacy risks by reference to the proposed APPs; and
 - (v) does not address risks or impacts relating to Australian secrecy laws.
- (b) Phase Two of this report does not address:
 - (i) whether the Exposure Draft Personally Controlled Electronic Health Records Bill 2011 (**Bill**) gives rise to any additional privacy risks other than those raised by the Legislation Submissions;
 - (ii) any privacy risks raised by the Legislation Submissions that respondents suggest should be managed through changes to governance and/or design of the PCEHR System;
 - (iii) any amendments to the Bill raised in the Legislation Submissions by respondents that only concern the technical drafting of the Bill; or
 - (iv) comments raised in the Legislation Submissions by respondents that merely go to the overall effectiveness of the PCEHR System, the need for adequate resourcing, adequacy of liability provisions or the desirability for harmonisation of privacy laws;
 - (v) any privacy impacts or risks that may arise from the changes to the design of the PCEHR System between the version of the Concept of Operations that we considered in Phase One and the final version of the Concept of Operations published by the Department.

1.2 How should this PIA be used?

1.2.1 Use of this PIA Report

- (a) Chapter 9 contains findings and recommendations with respect to the privacy impacts of the proposed PCEHR System, on its subjects and users: consumers, carers and authorised representatives of consumers, health service providers and related users.
- (b) This PIA report therefore provides:
 - (i) an assessment of the proposed controls and safeguards in the design and governance models for the proposed PCEHR System;
 - (ii) identification of risk areas in relation to compliance with privacy laws and community expectations; and

- (iii) suggested strategies to address those risks – by minimising privacy intrusions, and maximising privacy protections within the design, legislation and governance model for the proposed PCEHR System.
- (c) This report is intended as a valuable resource for the Department and NEHTA, as well as other stakeholders, to assist in finalising the design, legislation and governance of the proposed PCEHR System.
- (d) The PIA can also be used to further inform and educate those involved in, or affected by, the initiative as it is implemented – for example, in the design of guidelines, consumer communications, educational materials for users, staff training, system design and program evaluation.

1.2.2 Methodology

- (a) To produce this report we:
 - (i) have examined the documents specified in Schedule 1; and
 - (ii) held discussions with the persons specified in Schedule 1.
- (b) We have not undertaken consultations with stakeholders or interest groups, other than to consider the documents set out in Schedule 1.

1.3 The process of assessing privacy impacts

- (a) Identifying privacy impacts and risks involves an examination of how the PCEHR System will 'affect the choices consumers have regarding how information about them is handled, the potential degree of intrusiveness into the private lives of consumers, compliance with privacy law, and how the project fits into community expectations'.¹
- (b) The proposal is therefore assessed in Chapter 4 - Chapter 6 at each point in the life cycle of the 'personal information', as it is likely to be handled by participants in the PCEHR System. The assessment is made with respect to compliance with privacy laws, and whether the proposal can meet community expectations.
- (c) Chapter 7 outlines recommendations to minimise privacy risks relating to the System Operator.
- (d) Chapter 8 outlines further recommendations to minimise the privacy impacts and risks of the PCEHR System in a global sense.
- (e) A number of recommendations work together, and some deal with more than one privacy principle. The most significant recommendations are drawn together into coherent themes in Chapter 9. Chapter 9 also draws together our conclusions about the privacy impacts – both positive and negative - and risks of the PCEHR System.
- (f) As instructed by the Department, this PIA report does not provide an opinion on the severity or degree of significance of any particular privacy risk. In accordance with AS/NZS ISO 31000² such rating of risk should:
 - (i) be considered in the context of the specified objectives;
 - (ii) involve relevant informed project personnel (whether within the Department or otherwise);

¹ Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, August 2006, p.xxi

² Risk management – Principles and Guidelines

- (iii) assess the likelihood of the risk event arising and the consequences of the event arising by reference to the specified objectives; and
- (iv) apply criteria that is consistent with the Department's risk management methodology (assuming that is consistent with best risk management practice). In undertaking any such risk assessment it should be clear whether such risk rating is made on the basis that risk mitigation measures are adopted or not.

1.3.1 What are the privacy laws?

- (a) Privacy laws in Australia present a fractured and imperfect picture.³
- (b) This PIA Report considers the privacy impacts by reference to the legislation referred to in Schedule 2. For the purpose of conducting our assessment, we have developed a plain language summary and explanation of the National Privacy Principles (NPPs), which is set out in Chapter 3.

1.3.2 What does compliance with privacy laws mean?

- (a) PIAs respond to public concerns not only about strict compliance with privacy and related laws, but also about the wider implications of government and business initiatives that affect the level of surveillance and monitoring of consumers in society.
- (b) The need to examine issues beyond compliance with privacy laws is partly because in many respects, privacy principles in information privacy laws defer to other legislation. In some cases other legislation will create the conditions which ensure that an activity is treated as complying with the principle, while in other cases the activity will be considered to not comply with a privacy principle, but the non-compliance is authorised by the other law.
- (c) For example under NPP 2, there is a general presumption against using or disclosing personal information for purposes other than the purpose for which the information was collected. However that general presumption is waived where 'the use or disclosure is required or authorised by or under law'.
- (d) Therefore where the proposal undergoing assessment includes enabling legislation, for the most part compliance with the privacy laws will come automatically once that enabling legislation is in force.

1.3.3 Meeting community expectations

- (a) Authorising the collection, use or disclosure of personal information through the use of legislation may well ensure that a particular activity complies with the privacy law, and even with generally-accepted privacy principles. However that does not mean it will necessarily meet 'community expectations'.
- (b) The former Australian Privacy Commissioner Malcolm Crompton has noted that:

'consumers everywhere eventually reach a level of concern where they no longer accept a situation of low security and regular loss of privacy through inappropriate use and sharing of information, even if legal'.
- (c) Furthermore community expectations about what constitutes an invasion of privacy are not necessarily reflected in the law. For example a study of privacy complaints lodged

³ For a comprehensive overview of the various laws applying across the nation, see the Victorian Privacy Commissioner's interactive map titled 'Australian Privacy Regulation Map', available at www.privacy.vic.gov.au under Privacy Laws > Privacy Laws in Australia

against NSW government agencies found that while in 70% of cases the conduct complained of was found to have occurred, in only 28% of cases was the conduct found to have been in breach of the relevant privacy principles without lawful excuse. This suggests that many complainants' expectations about how the law is supposed to protect their privacy is not being met by the privacy laws in practice.

- (d) Reliable indicators of community expectations are notoriously difficult to produce. It is beyond the scope of this PIA to commission comprehensive research on expectations or attitudes with respect to this particular proposal.
- (e) For the purposes of this PIA Report our conclusions about the most likely community expectations concerning the PCEHR System are based upon:
 - (i) written submissions to the Department concerning the Concept of Operations dated 8 April 2011 and the Legislation Issues Paper listed in Schedule 1; and
 - (ii) comments made in consultation discussions listed in Schedule 1.
- (f) It should be noted that due to the many submissions made to the Department concerning the PCEHR System and the short time frame for the delivery of this PIA Report we have considered only those documents listed in Schedule 1.

1.3.4 Making recommendations

- (a) A PIA should 'identify avoidable risks and suggest measures to remove them or reduce them to an appropriate level'.⁴
- (b) Recommendations should however seek to achieve a balance between the interests of the agency making the proposal, and the people affected by the proposal. Those recommendations which are most strongly urged are therefore those which can significantly improve privacy protection for the people affected, without significantly impacting on the achievements of the proposal's objectives.

1.4 Qualifications and Assumptions

This PIA Report is subject to the following qualifications and assumptions:

- (a) The System Operator will be a body that fits within the definition of 'agency' in the *Privacy Act 1988 (Cth) (Privacy Act)*;
- (b) any submissions made to the Department that are not listed in Schedule 1 are not material to assessing the privacy impact of the PCEHR System;
- (c) Minter Ellison and Salinger Privacy have not undertaken any consultations or investigations other than those set out in Schedule 1;
- (d) the legislation considered for the purposes of this PIA Report is confined to that listed in Schedule 2;
- (e) we have not considered any existing privacy policies, guidelines or manuals, Chief Executive Instructions, or other internal documents of any Commonwealth agency that might perform the role of System Operator; and
- (f) we have not considered any existing State privacy policies, guidelines, manuals, directions, Cabinet instructions, Codes of Practice, ethical Codes of Practice, Chief

⁴ Office of the Privacy Commissioner, *Managing Privacy Risk*, November 2004, p.17

Executive Instructions, or other internal or administrative documents of any State agency that may perform the role of a registered repository operator.

Chapter 2 - Description of the PCEHR System

2.1 Overview of the PCEHR System

- (a) eHealth is an integral part of the Australian Government's objective 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.
- (b) A PCEHR is an electronic record of a consumer's medical history, stored and shared in a network of connected systems. The PCEHR will bring key health information from a number of different systems together and present it in a single view.
- (c) Information in a PCEHR can be accessed by the consumer and their authorised healthcare providers, nominated family members and carers whilst enabling the consumer to control who can access their PCEHR. With this information available to them, healthcare providers can make better decisions about a consumer's health and treatment advice. Consumers can contribute to their own PCEHR and add to the recorded information stored in their PCEHR.
- (d) The PCEHR will not hold all the information held in a consumer's records but will complement it by highlighting key information and indexing records held elsewhere. In the future, as the PCEHR becomes more widely available, consumers will be able to access their own health information anytime they need it from anywhere in Australia, provided that a consumer has internet access.⁵
- (e) The PCEHR System is being designed to use healthcare identifiers to support the accurate linkage of records to consumers and providers. The Department is currently reviewing the PCEHR System proposal to identify what amendments to the *Healthcare Identifiers Act 2010* (Cth) (**HI Act**) might be required to support the appropriate handling of healthcare identifiers, and will put the legislative proposal to all Australian Health Ministers for consideration, and to the public more generally for consultation. Under the National Partnership Agreement on eHealth⁶, the Commonwealth must obtain the prior agreement of all States and Territories to changes to the HI Act.

2.2 Key design features of the PCEHR System

- (a) The first release of the PCEHR System is expected to deliver the core functionality required to establish a PCEHR System that can grow over time. The first release will ensure that most consumers seeking care in the Australian healthcare system have the option to register for a PCEHR from July 2012.
- (b) The PCEHR System will build on the foundations laid by the introduction of the national Healthcare Identifiers (**HI**) Service for consumers, healthcare providers and healthcare organisations as well as the National Authentication Service for Health (**NASH**), clinical terminologies and methods for communicating health information between healthcare providers such as Discharge Summaries and electronic referrals.

⁵ National E-Health Transition Authority, 'What is a PCEHR?' <<http://www.nehta.gov.au/ehealth-implementation/what-is-a-pcher>> (4 September 2011)

⁶ http://www.federalfinancialrelations.gov.au/content/national_partnership_agreements/health/e_health/e-health.pdf

(c) Key design features of the PCEHR System are explained the table below.⁷

The PCEHR System			
is	<i>opt in</i> – if a consumer or healthcare provider wants to participate, they need to register with the system.	and not	<i>compulsory</i> – both consumers and healthcare providers choose whether or not to participate.
is	<i>an enhancement to medical treatment</i> – the PCEHR System will allow a consumer’s health information to be shared as and when needed to support the best possible care.	and not	<i>a requirement for medical treatment</i> – if a person does not wish to participate in the PCEHR System, they will continue to be able to access treatment and Medicare benefits.
is	<i>a source of selected clinical data and records</i> – in addition to a shared health summary in each PCEHR (which contains basic health information about a consumer), records may be added to that consumer’s PCEHR.	and not	<i>a replacement for normal sharing of information between a consumer and their healthcare provider</i> – as currently occurs in medical practice, existing medical records are used as the starting point for the discussion about the consumer’s health, rather than as the complete and authoritative source of current information.
is	<i>an information system</i> – where participating healthcare providers can access additional selected records during a consultation with a consumer.	and not	<i>a communication system</i> – where participating healthcare providers are expected to review any new records loaded into a PCEHR in between consultations with the consumer.
is	<i>aligned with current privacy obligations</i> – healthcare providers will have the same responsibilities in relation to privacy of information in PCEHRs as they currently do in relation to clinical information from other sources.	and not	<i>immune to current sharing and reporting rights and obligations of providers</i> – 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 a range of disease and child welfare matters to government authorities.
is	<i>a distributed system of service providers working in concert</i> – government and private sector organisations will work together to deliver the PCEHR System to consumers and healthcare providers. The PCEHR System will be underpinned by a legislative framework intended to impose	and not	<i>a single government store of personal information</i> – 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 specifications and standards. ⁸

⁷ Con Ops, section 2.3 (Vision and concept)

⁸ Con Ops, section 2.3 (Vision and concept)

	appropriate controls and standards on all the delivery bodies.		
--	--	--	--

2.3 The current state of play

The implementation and adoption of a PCEHR System aims to address fragmented and patchy information spread across a vast number of different locations and systems. In many healthcare situations, quick access to key health information about a consumer is not always possible.

Limited access to health information at the point of care results in:

- (a) a greater risk to patient safety;
- (b) increased costs of care and time wasted in collecting or finding information;
- (c) unnecessary or duplicated treatment activities;
- (d) additional pressure on the health workforce; and
- (e) reduced participation by consumers in their own healthcare information management.

2.3.1 Health benefits from the PCEHR System

- (a) 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 accessible to different healthcare providers involved in their care. This may result in:
 - (i) improved continuity of care for consumers accessing multiple healthcare providers by enabling key health information to be available where and when it is needed to ensure safe ongoing care;
 - (ii) access to consolidated information about a consumer's medicines, leading to safer and more effective medication management and reductions in avoidable medication-related adverse events; and
 - (iii) enabling consumers to participate more actively in their healthcare through improved access to their health information.
- (b) The national PCEHR System is intended to place the consumer at the centre of their own healthcare by enabling access to important health information, when and where it is needed, by consumers and their healthcare providers. Consumers can choose whether or not to have a PCEHR. If they choose to participate, they will be able to set their own access controls. With the consumer's permission, key pieces of health information may be viewed by participating healthcare providers across different locations and healthcare settings.

- (i) Figure 1 below provides an overview of the different participants in the PCEHR System.

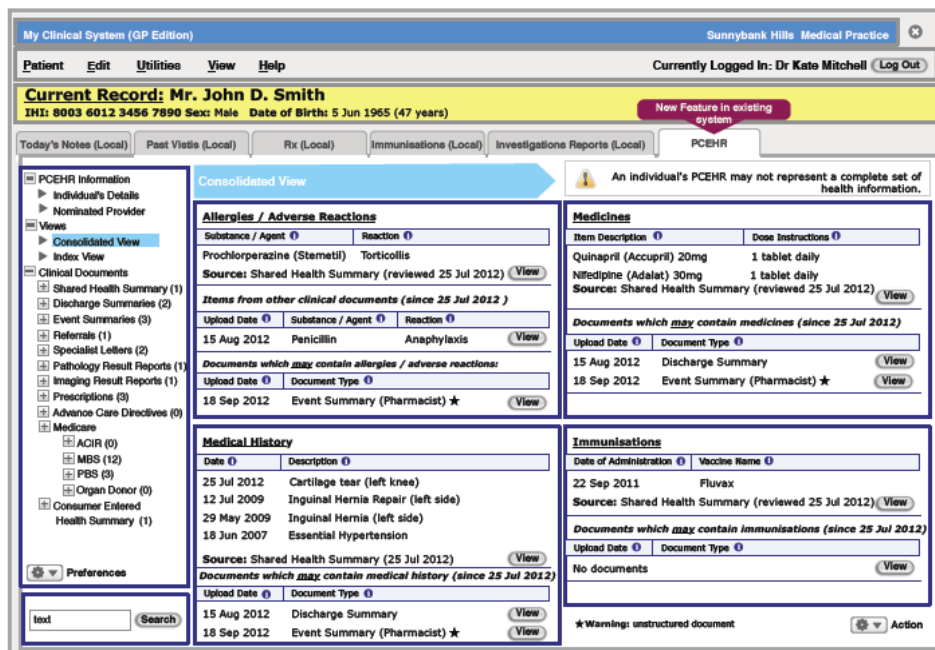


Figure 1: PCEHR System concept

- (c) In order to deliver this vision, the PCEHR System is designed to provide the necessary national infrastructure, standards and specifications to enable secure access to a consumer's health information drawn from multiple sources. Suppliers of eHealth systems will be able to enhance their products and services to become conformant with the relevant standards and specifications and support healthcare organisations in accessing the PCEHR System.
- (d) Records, such as shared health summaries, Discharge Summaries, Event Summaries, Pathology Result Reports and Specialist Letters will be collected from a range of participating organisations, and stored within a number of registered repository operators connected to the PCEHR System.
- (e) The PCEHR System may also share key health information entered by the consumer (such as over-the counter medications and allergies), and access information from the Department of Human Services (**DHS**). This includes Medicare information, such as a consumer's organ donor status, dispensed medications funded under the Pharmaceutical Benefits Scheme (**PBS**), information about healthcare events from a consumer's Medicare claiming history and a child's immunisation history. The PCEHR System will also be able to collect information about the location of a consumer's advance care directives (if they have one).
- (f) The PCEHR System will provide a number of core services that will allow Authorised Users to search for records, view records and access reports. A key feature of the PCEHR System is its ability to provide a series of views over different records in a consumer's PCEHR. These views will allow users of the system to easily see a consolidated overview of a consumer's allergies and adverse reactions, medicines, medical history, immunisations, directives and recent healthcare events from different information sources.⁹

⁹ Con Ops, sections 1.1 and 1.2 (Overview of the PCEHR System)

Figure 2 provides an example of a Consolidated View.



- (g) **Note** that this is a conceptual mock-up of what the Consolidated View may look like for an Authorised User and does not necessarily reflect how the view would appear when the PCEHR System is live.
- (h) One of the key records shared via the PCEHR System is a consumer's shared health summary. A shared health summary is a record sourced from the consumer's nominated healthcare provider (see description below), which provides a clinically reviewed summary of a consumer's healthcare status and provides information about a consumer's allergies and adverse reactions, medicines, medical history and immunisations.
- (i) As the shared health summary is a 'point in time' record, it is complemented by the 'Consolidated View'. The Consolidated View presents the shared health summary, together with information from other records received since it was created.
- (j) The shared health summary must be supplied as a level 2 record (level 1 records are not permitted). To enable easy extraction of shared health summaries from GP systems, the fields within a shared health summary will be congruent with the Royal Australian College of General Practitioners (**RACGP**) standards for health summaries.
- (k) In addition to the common fields, a shared health summary includes:
 - (i) allergies and adverse reactions (required);
 - (ii) medicines (required);
 - (iii) medical history (required); and
 - (iv) immunisations (required).¹⁰

2.4 An overview of privacy and security measures

A multi-layered approach is intended to surround the PCEHR System, and we understand that it will include the following:

¹⁰ Con Ops, section 4.3.1 (Shared Health Summaries)

Design

- accurate authentication of users accessing the PCEHR System;
- robust audit trails; and
- proactive monitoring of access to the PCEHR System to detect suspicious and inappropriate behaviour.

Security

- rigorous security testing, to be conducted both before and after the PCEHR System begins operation.

Communications

- education and training of users of the system.

Legislation

- requirements that healthcare providers and organisations comply with specific PCEHR Rules and other relevant legislation.

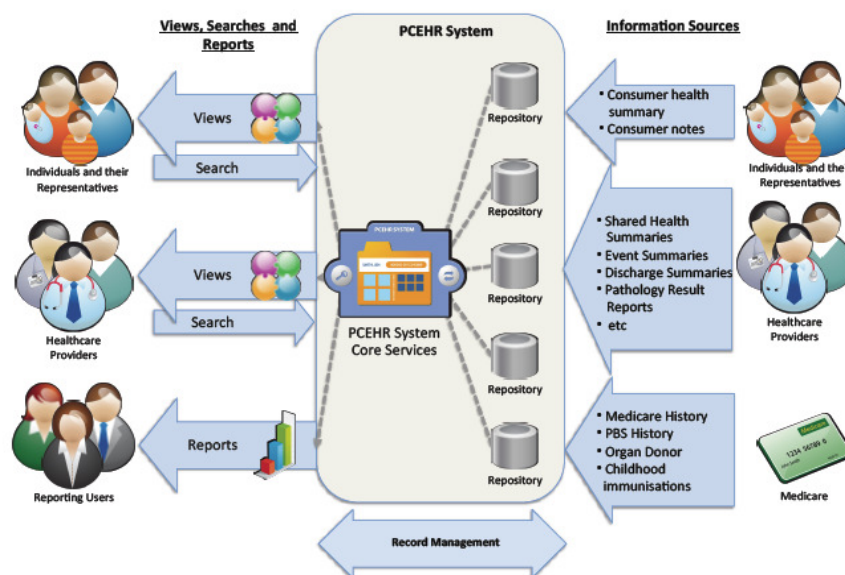
Project governance

- consumers will be able to make enquiries and lodge complaints regarding suspicious or unauthorised access to their PCEHR.

2.5 Scope and reach

2.5.1 Participants and users of the PCEHR System

- (a) The implementation, adoption, operation and use of the PCEHR System involves the participation of a variety of organisations and consumers. Set out below is a list of the participants, with further summaries below containing more information about their roles and functions.



- (b) We also include a diagram that illustrates some of the participants.¹¹

¹¹ Con Ops, section 1.2 (The PCEHR System)

2.6 PCEHR System Participants

PCEHR System Participant	Role and functions
System Operator (a Commonwealth agency)	<p>will operate the national infrastructure.</p> <p>will supply operational capabilities around:</p> <ul style="list-style-type: none"> • Channel Management of the consumer and provider portal, administration portal and the B2B gateway; • management of core services, such as the Participation and Authorisation Service, Index and View Service, Report Service, Audit Service and Contact Management Service; • management of the National Repositories Service; and • supply of operational capabilities around service support, service delivery, infrastructure management, security management, application management, asset management and corporate services (such as HR and finance).¹²
HI Service Operator	<p>The HI Service Operator will assign 3 types of healthcare identifiers:</p> <ul style="list-style-type: none"> • Individual Healthcare Identifier (IHI) (for consumers receiving healthcare services); • Healthcare Provider Identifier (Individual (HPI-I)) (for healthcare professionals and other health personnel involved in giving patient care; and • Healthcare Provider Identifier (Organisation (HPI-O)) (for organisations such as a the hospital or clinic where healthcare is given). <p>Chief Executive, Medicare is the initial operator of the Healthcare Identifiers Service as a trusted and provider of health related services. This new role is separate to Medicare's funding and claiming services.</p> <p>The HI Service will be reviewed 2 years after commencement and will take into account any further e-health developments.¹³</p>
National Repository Service Provider	<p>The National Repositories Service stores a minimum critical set of health information about participating consumers. The National Repositories Service does not consist of a single central data repository. It will consist of a number of nationally operated repositories.</p> <p>The minimum critical set of health information managed by this service includes:</p> <ul style="list-style-type: none"> • shared health summaries; • Event Summaries;

¹² Con Ops, section 7.3 (System Operator)

¹³ 'Questions and Answers: *Healthcare Identifiers Bill 2010*' (email received from the Department dated 30 August 2011)

PCEHR System Participant	Role and functions
	<ul style="list-style-type: none"> • Discharge Summaries; • Specialist Letters; • Consumer-Entered Health Summary; and • Consumer Notes.¹⁴ <p>The National Repositories Service will be managed by the System Operator.</p>
registered repository operators	<p>In addition to the National Repositories Service, the PCEHR System will have the capability to connect to other registered repository operators operated by a registered repository operator. Repository operators will have an obligation to ensure that information within a repository is available via other means (eg by placing it in escrow) if the repository is to be shut down.</p> <p>Examples of registered repository operators may include:</p> <ul style="list-style-type: none"> • DHS operated repositories holding Medicare history, PBS history, organ donor information and childhood immunisation information; • Pathology service repositories holding Pathology Result Reports; and • Regional or State/Territory operated repositories.¹⁵

¹⁴ Con Ops, section 6.6.1 (National Repositories Service)

¹⁵ Con Ops, section 6.6.2 (Conformant Repositories)

PCEHR System Participant	Role and functions
registered portal operators (for healthcare providers)	<p>Participating organisations may also access the PCEHR System via a Provider Portal. We note the Provider Portal is yet to be determined and would be selected in due course.</p> <p>The purpose of the Provider Portal is to complement existing local health record systems by providing an alternative form of access to the PCEHR.</p> <p>From within the Provider Portal, healthcare providers will be able to:</p> <ul style="list-style-type: none"> • access general information about the PCEHR System in a healthcare provider-oriented form; • login to the Provider Portal using their healthcare provider NASH token containing their digital credentials; • select which organisation they are accessing on behalf of (if the healthcare is linked to multiple healthcare organisations in the HI Provider Directory Service); and • access a PCEHR, including: <ul style="list-style-type: none"> • Find a PCEHR. • Add the healthcare organisation to the Access List (Provider Access Consent Code (PACC) may be required). • Access PCEHR views (see Con Ops, Section 4.4). • Search a PCEHR (see Con Ops, Section 4.5). • Download and/or print records. • Access support services: <ul style="list-style-type: none"> • Search the NHSPD. • Access online help. • Contact the System Operator and request support.¹⁶ <p>Note: this list is not exhaustive.</p>
Contracted Service Provider Portals	<p>The PCEHR System will be accessible from a range of third party contracted service providers who offer health software as a service (SaaS) and support access to the PCEHR System on behalf of a healthcare organisation. Examples could include companies who supply primary care and aged care software as a service.</p> <p>Contracted service providers will give healthcare providers access to a PCEHR, including:</p> <ul style="list-style-type: none"> • find a PCEHR; • add the organisation to the Access List (PACC may be required); • obtain emergency access;

¹⁶ Con Ops, section 6.3.2 (Provider Portals)

PCEHR System Participant	Role and functions
	<ul style="list-style-type: none"> • access PCEHR views (see Con Ops, Section 4.4); • search a PCEHR (see Con Ops, Section 4.5); • download and/or Print Records and Views; • upload records into the PCEHR System; • access support services: <ul style="list-style-type: none"> • access online help about the PCEHR System; and • contact the System Operator and request support.¹⁷ <p>Note: This list is not exhaustive.</p>
registered portal operators (for consumers)	<p>The purpose of a registered portal operator is to provide a nationally operated portal to allow consumers to access their own PCEHR. From within the Consumer Portal, consumers will be able to:</p> <ul style="list-style-type: none"> • manage their Consumer Portal account; • manage notification details; • register to have a PCEHR created; • request to deactivate a PCEHR; • request to reactivate a deactivated PCEHR; • associate/disassociate themselves with other individuals as their representative (note that this may require additional proof to be given to the System Operator); • link their PCEHR to their registered portal operator account to a PCEHR (if they already have one); • access PCEHR views; • search a PCEHR; • download/print records; • manage access controls; • view the audit trail; and • access support services.¹⁸

2.7 Individual participants

Individual participant	Role and functions
Consumers	Central to the PCEHR System is the concept of personal control. Participating consumers can exercise control over their PCEHR in the

¹⁷ Con Ops, section 6.2.3 (Contracted Service Providers)

¹⁸ Con Ops, section 6.3.1 (Consumer Portal)

Individual participant	Role and functions
	<p>following ways:</p> <ul style="list-style-type: none"> • decide whether or not to have an active PCEHR; • access information in their PCEHR; • set controls around healthcare provider 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.
authorised representatives (carers)	<ul style="list-style-type: none"> • Once the consumer is registered for a PCEHR, and the representative's legal authority to act on behalf of the consumer has been verified, the authorised representative will be given the same access and controls as the consumer. • There may be more than one authorised representative for a consumer. • We understand that once an authorised representative has control over a consumer's PCEHR, the consumer would be unable to take personal control over their PCEHR. However, the authorised representative could give the consumer 'read only' access by making the consumer a nominated representative.¹⁹ • The Con Ops notes that the definition for 'carer' is consistent with the <i>Carer Recognition Act 2010</i> (Cth) (Con Ops, s 3.2.8). We have included this term in the Glossary (Schedule 3) and assume the PCEHR legislation will also include this definition.
nominated representatives	<ul style="list-style-type: none"> • A consumer or authorised representative may nominate any other persons (such as carers and family members) to access their PCEHR. • A nominated representative may view the consumer's PCEHR, but will not be able to manage the consumer's access controls, contribute to information in a consumer's PCEHR or provide consent for a healthcare provider to obtain access to the consumer's PCEHR. • It is proposed that there are no age restrictions on nominated representatives and a minor can be a nominated representative.²⁰
Authorised Users	<ul style="list-style-type: none"> • The PCEHR System entrusts a participating organisation to grant access to healthcare providers and other local users who need to access the PCEHR System.

¹⁹ Con Ops, section 3.2.8 (Representatives)

²⁰ Con Ops, section 3.2.8 (Representatives)

Individual participant	Role and functions
	<ul style="list-style-type: none"> • These users are referred to as ‘authorised users’. An Authorised User may be any employee who has a legitimate need to access the PCEHR System as part of their role in healthcare delivery. As per the HI Act, an ‘employee’ is either a consumer who provides services for the entity under a contract for services or a consumer whose services are made available to the entity (including services made available free of charge). • When Authorised Users access the PCEHR System, they are only permitted to access the PCEHR of consumers they are involved in delivering healthcare services to. All access to the PCEHR System is audited.
Reporting Users	<p>We understand that the System Operator will offer a Reporting Service.</p> <p>The Report Service will be able to provide a range of reports, including:</p> <ul style="list-style-type: none"> • Operational reporting, such as, but not limited to: <ul style="list-style-type: none"> • Reporting against metrics in PCEHR System infrastructure Service Level Agreements and registered repository operator Service Level Agreements (eg uptime, incident reports, incident resolution times, call centre reporting, etc.); • Audit reports; and • Data quality ‘dashboard’ (see Con Ops, section 4.2.1). • PCEHR System uptake and usage reporting, including access to predefined reports showing: <ul style="list-style-type: none"> • Numbers of consumers registering, using the PCEHR System and withdrawing. • Numbers of Authorised Users and healthcare organisations using the PCEHR System; • Viewing of records, views and reports; • Uploading new records; <p>This data can be broken down by:</p> <ul style="list-style-type: none"> • Demographics (age, location, gender); • Time (time of day, day of week, month); • Healthcare provider role (eg General Practitioner, specialist, Emergency Department doctor); and • Kind of information accessed or uploaded (view name or clinical record types).

Individual participant	Role and functions
	<ul style="list-style-type: none"> • Reports related to outcomes realisation related key performance indicators (see Con Ops, section 9.2.1).

2.8 Healthcare participants

Healthcare participant	Role and functions
general practices	<ul style="list-style-type: none"> • The author of a shared health summary is referred to as the consumer's 'nominated healthcare provider.' • A nominated healthcare provider is an identified healthcare provider involved in the ongoing care of the consumer who has agreed with the consumer to create and manage their shared health summary. • It is anticipated that for many consumers, the nominated healthcare provider will be the consumer's regular GP, but a nominated healthcare provider may also be other providers involved in the ongoing care of the consumer, such as another medical practitioner, nurse practitioner or Aboriginal healthcare worker.²¹
hospitals	<ul style="list-style-type: none"> • The PCEHR System will be accessible from a range of clinical systems, including hospitals' systems. • Some hospitals may also become registered repository operators. • How a hospital's local system is integrated with the PCEHR System will vary from system to system. Some systems may have inbuilt features to access the PCEHR System and others may rely on a combination of backend gateways and provider portal integration to access the PCEHR System. • The PCEHR System will support collection of Discharge Summaries. When a healthcare provider creates a Discharge Summary, it will be sent directly to the intended recipient, as per current practices, and a copy of the Discharge Summary may also be sent to the PCEHR System.²² Over time, a consumer's existing Discharge Summaries may be able to be uploaded to the PCEHR System.²³
specialists	<ul style="list-style-type: none"> • The PCEHR System will support the collection of Specialist Letters. When a specialist creates a Specialist Letter, it will be sent directly to the intended recipient, as per current practices, and a copy of the Specialist Letter may also be uploaded to the PCEHR System.²⁴

²¹ Con Ops, section 4.3.1 (Shared Health Summaries)

²² Con Ops, section 4.3.3 (Discharge summaries)

²³ Con Ops, section 3.2.6 (Access to existing information)

²⁴ Con Ops, section 4.3.4 (Specialist letters)

Healthcare participant	Role and functions
pharmacies	<ul style="list-style-type: none"> • The PCEHR System will be accessible from a range of clinical systems, including pharmacies' systems. The PCEHR System will enable the collection of Prescribing and Dispensing information. • Participating prescribers and dispensers who have access to the PCEHR System will be able to upload a copy of Prescription and Dispensing information to the PCEHR System. This information is a copy of information that is also sent to the Prescription Exchange Service (PES). • The Fifth Community Pharmacy Agreement also includes an option to include loading information about dispensed prescription into the PCEHR System [DOHA2010e].²⁵
diagnostic imaging laboratories	<ul style="list-style-type: none"> • For the first release, we understand that allied health providers will not participate in the PCEHR System. The National E-Health Strategy proposed that the PCEHR System rollout be undertaken via an incremental approach, with the capabilities of the system being expanded over a four-year implementation period. • Candidates for later potential enhancements could include, support for collection of a broader range of health information from healthcare providers, such as diagnostic imaging reports, images and request.²⁶
pathology laboratories	<ul style="list-style-type: none"> • We understand that the PCEHR System will support collection of Pathology Result Reports.²⁷
allied health	<ul style="list-style-type: none"> • For the first release, we understand that allied health providers will not participate in the PCEHR System. The National E-Health Strategy proposed that the PCEHR System rollout be undertaken via an incremental approach, with the capabilities of the system being expanded over a four-year implementation period. • Candidates for later potential enhancements could include, views to support specific healthcare providers, such as nurses and allied health providers.²⁸

2.8.1 Overview of PCEHR System components

- (a) The PCEHR System is a 'system of systems', consisting of a number of core services and registered repository operators. The proposed approach will leverage existing foundations, such as the HI Service, NASH and Clinical Terminologies. The core national services include:
- (i) *A Participation and Authorisation Service*, which stores consumers' participation preferences and manages access controls to a consumer's PCEHR;

²⁵ Con Ops, section 4.3.6 (Prescribing and Dispensing information)

²⁶ Con Ops, section 2.8 (Potential enhancements)

²⁷ Con Ops, section 4.3.7 (Pathology result reports)

²⁸ Con Ops, section 2.8 (Potential enhancements)

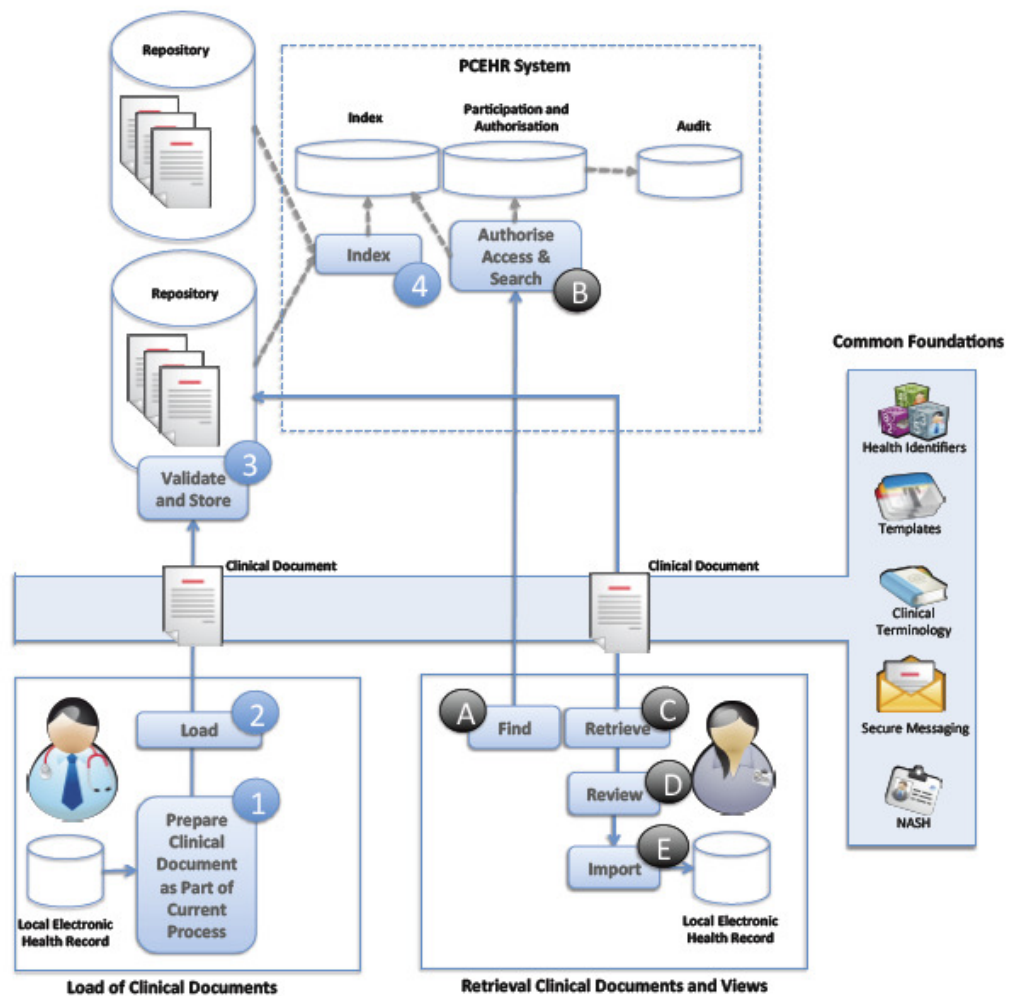
- (ii) *An index service*, which records the location(s) of a participating consumer's records in a range of PCEHR-registered repository operators;
 - (iii) *An Audit Service*, which audits all activity across the PCEHR System; and
 - (iv) *A View Service and a Report Service*, which are capable of extracting information from PCEHR-registered repository operators in order to support a range of different ways of viewing and reporting on information.
- (b) These services will be complemented by two new foundation services that operate alongside the other foundation services, such as the HI Service and NASH. These new foundation services include:
- (i) *A Proof of Record Ownership Service*, which can verify that a consumer has supplied sufficient information to correctly claim their records, which assists in verifying their relationship with another consumer (eg parent / child relationships), and also assists in verifying identity (but noting that verification of identity is a discrete process);
 - (ii) *A Template Service*, which provides definitions about the types of healthcare information that can be shared via the PCEHR System (and other systems); and
 - (iii) *A National Healthcare Provider Service Directory* to provide a 'Yellow Pages' style search of healthcare providers and organisations.
- (c) These infrastructure services will be used to facilitate access via a service coordination layer to a range of registered repository operators. This includes a National Repositories Service and the capability to link to other independent registered repository operators, such as repositories offered by the DHS Medicare master program, diagnostic service providers, regional operators, State/Territory public health system(s) and other parties.
- (d) The PCEHR core services and repositories will be accessible via a range of channels and user systems, including:
- (i) *Nationally provided Consumer and Provider-oriented portals*, as well as independently provided consumer-oriented Registered portal operators;
 - (ii) *A Call Centre* for consumers and healthcare provider support;
 - (iii) *A Business-to-Business (B2B) Gateway*, to allow a range of systems to access the PCEHR System, such as: clinical systems, systems integrated via a gateway and contracted service providers acting on behalf of healthcare organisations;
 - (iv) *A Report Portal* to support operational and evaluation based reporting; and
 - (v) *An Administration Portal and Contact Management Service* to aid a range of agents with supporting PCEHR users.
- (e) Access to the PCEHR System will be based on Australian and international standards for ensuring interoperability of eHealth systems as well as other relevant specifications.²⁹

²⁹ Con Ops, section 6.1 (Introduction: PCEHR System components)

2.9 How personal information will flow through the PCEHR System

2.9.1 Overview of the information flow

- (a) The PCEHR System will collect information from a wide range of sources within a number of registered repository operators and be able to present that information in a range of ways to meet the needs of consumers, healthcare providers and other parties.³⁰
- (b) The PCEHR System enables the collection of information from participating organisations, consumers and the DHS Medicare master program within a series of registered repository operators. Information will be collected in the form of a record. For the purposes of the PCEHR System, a record is an electronic record that contains personal health information about a consumer.³¹
- (c) We include a diagram below that summarises the upload and download of a record.³²



³⁰ Con Ops, section 4.1 (Introduction: Managing PCEHR information)

³¹ Con Ops, section 4.2 (Information model)

³² Con Ops, section 4.2 (Information model: Figure 8 Example information flow)

2.9.2 Download a record from a National Repository or registered repository operator

- (a) The PCEHR System permits authorised users to download and/or print any records and views they are authorised to access. Downloaded information can be supplied either in PDF format or a standards conformant electronic format for loading into the organisation's local electronic health record.
- (b) Users should only download and/or print information required to support the delivery of the consumer's care or to ensure that medico-legal integrity requirements are addressed. Once information has been downloaded and/or printed it becomes subject to the organisation's local health information management policies. All downloaded and printed records and views need to be clearly marked with the date and time of download/printing.³³

2.10 Features of the PCEHR System for the purposes of this assessment

- (a) For the purposes of conducting this PIA, we have conceived of the PCEHR System as containing a number of discrete features. Subsequent chapters of this report describe and analyse those features as follows:
 - (i) Chapter 4 reviews the processes by which a consumer registers for a PCEHR and sets their access controls;
 - (ii) Chapter 5 reviews the processes by which a PCEHR is accessed and used: by the consumer and their representatives, by healthcare providers, and by third parties;
 - (iii) Chapter 6 reviews the processes by which a PCEHR is suspended, deactivated and reactivated;
 - (iv) Chapter 7 reviews the governance and accountability of the System Operator; and
 - (v) Chapter 8 reviews the governance and accountability of the PCEHR System as a whole.

³³ Con Ops, section 4.2.3 (Downloading and printing clinical records and views)

Chapter 3 - Privacy principles used in this assessment

3.1 Overview

- (a) Privacy is often seen as short for secrecy or confidentiality – that is, as placing a bar on the disclosure of one’s personal information. However privacy is both a broader and more flexible concept than just a barrier to disclosure.
- (b) Personal information privacy generally refers to a person’s ability to control how their personal information is handled throughout the life cycle of that information – how it is collected, stored, accessed, checked, used and disclosed. By contrast, confidentiality only places restrictions on the disclosure of information – but it can relate to all types of information, such as business affairs, trade secrets or Cabinet-in-confidence material, not just ‘personal information’.
- (c) As the PCEHR System will involve a System Operator and many other participants, a number of different privacy laws and privacy principles will apply in practice. This PIA report refers primarily to the NPPs, and uses a plain language explanation of the scope or importance of each NPP (below) as the starting point for our analysis. Other privacy principles that may also have an impact on particular participants in the scheme will also be noted as relevant throughout Chapter 4 - Chapter 8.
- (d) Chapter 4 - Chapter 8 therefore reviews the PCEHR System described in Chapter 2 primarily as against a set of core privacy principles - the NPPs.

3.2 Collection of personal information

3.2.1 Anonymity and pseudonymity

- (a) NPP 8 provides that wherever it is lawful and practicable in the circumstances, organisations must give consumers the clear option of interacting anonymously or by using a pseudonym.

3.2.2 Collection necessity

- (a) Any collection of personal information by organisations must be 'necessary for one or more of its functions or activities', according to NPP 1.1.

3.2.3 Collection methods – lawful, fair and not intrusive

- (a) NPP 1.2 requires organisations to collect personal information only by lawful and fair means, and not in an unreasonably intrusive way.
- (b) The more a person perceives a request for information as intrusive, or the more concern they have about the secondary uses of the information, the more likely they are to give false answers to protect themselves.³⁴ This ultimately undermines a scheme's purposes in collecting the information in the first place. The quest for accurate data is a significant reason why effort should be made to only ask those questions which can be justified as necessary, proportionate, appropriate and not intrusive.

³⁴ See NSW Independent Commission Against Corruption, *Report on Unauthorised Release of Government Information*, August 1992, Vol I, Chapter 12.6; available at <http://www.icac.nsw.gov.au>

3.2.4 Collecting sensitive personal information

- (a) NPP 10.1 requires the collection of 'sensitive personal information' to generally be with the subject's consent, as required by or under law, or in emergency situations where the subject cannot communicate their consent.
- (b) What is defined by privacy law as 'sensitive' differs across jurisdictions within Australia,³⁵ but at its core is a recognition that health information, and information about people's ethnicity, race or religion, are deserving of additional protection.

3.2.5 Direct collection

- (a) NPP 1.4 provides that if it is reasonable and practicable to do so, an organisation must collect personal information about a consumer only from that consumer.
- (b) This principle of direct collection is not only about the transparency of the process, but also about ensuring the accuracy of the information collected, by giving the affected person the opportunity to correct any incorrect information, or challenge requested information as irrelevant.
- (c) Where direct collection is not possible, best practice is to ensure that the consumer has provided authorisation for their personal information to be collected via another party.

3.2.6 Collection transparency and choice (notification, options)

- (a) NPP 1.3 and 1.5 requires organisations, when collecting personal information about a consumer (whether from the consumer or from someone other than the consumer), to take such steps as are reasonable in the circumstances to ensure that the consumer is aware of various matters, including the purposes for which their personal information will be used or disclosed, whether the collection is voluntary, any consequences of not providing the information, and how the consumer might gain access to the information.

3.3 Data security

- (a) NPP 4 requires organisations to take reasonable steps to protect the personal information they hold from misuse, loss, and unauthorised access, modification or disclosure.
- (b) NPP 4.2 requires organisations to destroy or render non-identifiable personal information if it is no longer needed for any purpose for which it can be used or disclosed under NPP 2.

3.4 Access and correction

- (a) NPP 6.1 requires organisations to provide consumers with access to their own personal information within a reasonable time, unless an exception applies.
- (b) NPP 6.5 requires organisations to take reasonable steps to correct any personal information they hold to ensure it is accurate, complete, up-to-date, relevant and not misleading.

3.5 Data quality

- (a) NPP 3 requires organisations to take reasonable steps to ensure that the personal information they collect, use or disclose is accurate, complete and up-to-date.

³⁵ For example the federal Privacy Act protects criminal records as 'sensitive', but NSW privacy law does not

- (b) The principle of data quality, or accuracy, has been described as 'the most important' of all privacy principles, its status reflected in the fact that, unlike limitations on collection, use and disclosure, non-compliance cannot be authorised by another law.³⁶

3.6 Use and disclosure

3.6.1 Use and disclosure of personal information

- (a) NPP 2 places limitations around the use or disclosure of personal information for purposes other than the purpose for which the information was collected in the first place. Health information is classified as 'sensitive' personal information, and NPP 2.1 sets tougher standards for the disclosure of sensitive personal information than for other categories of personal information; for example, secondary purpose disclosures must be 'directly related to the primary purpose of collection'.

3.6.2 Use and disclosure of unique identifiers

- (a) NPP 7 limits the collection and use of government-issued identifiers by private sector organisations.
- (b) The Identifiers principle recognises the risk that the unique numbers found on government-issued identity documents, such as driver's licences and passports, could be used to track, link and match records about a person, and thus build up a profile of that person. The desire to prevent this situation occurring is not only for the protection of people's privacy, and in recognition of Australians' general opposition to the idea of national identity cards, but is also a sensible strategy in terms of tackling identity-based crime.³⁷

3.6.3 Disclosing health information in particular contexts

- (a) NPP 10.4 also creates particular requirements to de-identify health information collected for research or for the management, funding or monitoring of a health service, prior to any subsequent disclosure of that information.

3.6.4 Transborder disclosures

- (a) NPP 9 applies in addition to the normal limitations on disclosures.

³⁶ *Director General, Department of Education and Training v MT (GD)* [2005] NSWADTAP 77 at [37]

³⁷ The National Identity Security Strategy for example recognises that a multiplicity of identifiers, rather than a single national identifier, presents a more robust system of protection against identity theft and fraud

Chapter 4 - Registration and creation of a PCEHR

4.1 Registration procedure

4.1.1 An overview of the registration channels

- (a) A consumer can register for a PCEHR in 3 ways:
 - (i) Online registration via a Consumer Portal (**online channel**);
 - (ii) Over the counter/in person registration (**face to face channel**); and
 - (iii) Registration by post (**mail channel**).
- (b) A PCEHR is only active after registration is complete and the consumer or their authorised representative has agreed to the terms and conditions. We understand that the Change and Adoption Partner is exploring various methods for presenting the terms and conditions to consumers.
- (c) We have described each channel separately, in detail, to highlight the differences in information flows with respect to each channel and method of registration.

4.1.2 Registration Process - Privacy positives

- (a) Lessons learned from previous trials of shared Electronic Health Records (**EHRs**) include the need to ensure that participation is voluntary, but with workable consent models. As reported in the draft Con Ops, the Department identified a number of key points:
 - (i) consumers preferred voluntary participation based on an 'opt-in' model for participation; and
 - (ii) consumers prefer to provide some form of 'standing' consent to nominated healthcare providers to have ongoing access to their record (rather than consent at every episode of care).³⁸
- (b) A central 'privacy promise' made to Australians is that having a PCEHR is entirely voluntary. It has been described as an 'opt in' system.
- (c) This is a clear 'privacy positive' of the proposal.

4.1.3 Registration Process - Privacy risks

Pressure to change the voluntary nature of the PCEHR

- (a) There is a risk that the central 'privacy promise' of the PCEHR System - that having a PCEHR is 'opt in' - is not met or changed due to pressure from some stakeholders, including system designers, as occurred in the NSW Healthlink trial. According to an Orion report, a controversial switch by NSW Health to the opt-out patient consent model was based on the consortium's recommendation.³⁹
- (b) Appropriate PCEHR legislation should instead embed the 'opt in' nature of the proposal.

³⁸ Con Ops, April 2011, p.109

³⁹ Karen Dearne, *The Australian*, 'State looks to NZ for e-health tips', 28 March 2006; see also Ruth Pollard, 'Privacy alert: every patient on database', *Sydney Morning Herald*, 1 June 2005

Practical limitations to the voluntary nature of the PCEHR

- (c) The voluntary 'opt-in' nature is a central promise of the PCEHR System.
- (d) The voluntary nature of any consent based proposal can be undermined if people feel social or financial pressure to participate.
- (e) Consent must be freely given, which means that there are no repercussions for the consumer if they withhold their consent. For example, the NSW Privacy Commissioner has advised that consent will only be valid if it is 'voluntary, informed, specific and current'. In particular, 'if a person has no practical alternative but to provide certain information in order to receive a service, an agency should not suggest they are seeking the person's consent'⁴⁰.
- (f) Case law also supports this construction of 'consent':

'Under the general law such consents must be both freely given and informed. ... Whether any given consent will operate to satisfy the consent requirements will depend on the construction of the consent itself, the circumstances in which was given, and the understanding of the person giving consent, taking into account their particular vulnerabilities'.⁴¹
- (g) The validity of the consumer's 'consent' could therefore be brought into question if their agreement to register for a PCEHR was treated as a condition of obtaining a benefit (other than the inherent benefit of having a PCEHR), or avoiding a disadvantage. The benefits to the consumer of having a PCEHR should be a stand-alone proposition. Any extraneous inducements to consumers to register for a PCEHR would undermine the voluntary nature of the proposal, the central 'privacy promise', and the proposal's credibility as a result. In effect this creates a risk that the PCEHR System will not meet community expectations that the PCEHR System will not unreasonably invade their privacy.
- (h) We understand the policy intention is that no health consumer should suffer a disadvantage, in terms of their access to healthcare, should they choose *not* to have a PCEHR.⁴²
- (i) We suggest that a 'no disadvantage' rule should be included in the PCEHR legislation.
- (j) On the basis that this community expectation objective prevails over any other objectives relating to the PCEHR System, the PCEHR legislation should extend to other likely points of pressure, such as the employment context or in relation to the provision of insurance (healthcare or other insurance). Such an approach has been taken in s 24 of the HI Act.
- (k) The absence of a benefit, such as a discounted insurance premium or the offer of employment, is effectively a disadvantage to the consumer who chooses not to register for a PCEHR. Likewise a request from an insurer to provide a copy of the consumer's PCEHR Consolidated View in order to be assessed for eligibility of an insurance product could be viewed as an inducement to 'consent' to register for a PCEHR and/or 'consent' to provide a copy.
- (l) Communications from registered portal operators to their customers should ensure that consumers are not misled into registering for a PCEHR, simply in order to obtain other services from the portal provider. For example, registered portal operators should not

⁴⁰ Privacy NSW, *Best Practice Guide: Privacy and people with decision-making disabilities*, 2004, pp.5, 7

⁴¹ *JK v Department of Transport Infrastructure Development* [2009] NSWADT 307 at [78]-[79]

⁴² Con Ops, section 3.2 (Individuals)

suggest that the treatment of claims, medical conditions or other services requires the consumer to have a PCEHR.

- (m) We suggest that the legislation should prohibit:
- inducing a consumer to register for a PCEHR (other than by reference to the benefits of the PCEHR itself);
 - inducing a consumer to provide a copy of their PCEHR to a third party;
 - consumers being placed at a disadvantage (financially or in relation to access to healthcare) if they do not have a PCEHR; and
 - consumers being placed at a disadvantage (financially or in relation to access to healthcare) for declining to provide permission for a healthcare provider to access their PCEHR.
- (n) Possible models for drafting a 'no inducement' provision may be found at ss 20 and 22 of the *Health Records (Privacy and Access) Act 1997* (ACT), and s 80 of the *Health Records Act 2001* (VIC).

4.1.4 Registration Process - Recommendations

Pressure to change the voluntary nature of the PCEHR

- 4.1 That the PCEHR Bill include the requirement for a consumer (or their authorised representative)'s express consent to register for a PCEHR.
- 4.2 That the PCEHR Bill not allow regulations or other subordinate legislation to create an exemption from the express consent requirement.
- 4.3 That any plans for transition of data from existing shared EHR systems incorporate a 'fresh' express consent process.

Practical limitations to the voluntary nature of the PCEHR

- 4.4 That the PCEHR Bill prohibit:
- (a) inducing a consumer to register for a PCEHR (other than by reference to the benefits of the PCEHR itself);
 - (b) inducing a consumer to provide a copy of their PCEHR to a third party;
 - (c) consumers being placed at a disadvantage (financially or in relation to access to healthcare) if they do not have a PCEHR; and
 - (d) consumers being placed at a disadvantage (financially or in relation to access to healthcare) for declining to provide permission for a healthcare provider to access their PCEHR.
- 4.5 That advice be provided to registered portal operators, to ensure that their marketing, privacy notices and terms and conditions clearly reflect the distinction between the PCEHR System and any services offered by the registered portal operator.

4.2 Limits to choice of channel

4.2.1 Authorised representatives

- (a) Where a consumer lacks capacity or has diminished capacity, registration may be undertaken by the consumer's authorised representative. However, registration must be undertaken in an assisted channel (face to face or hard copy channels only). The

limitation in channel for consumers lacking capacity is due to the special verification procedures needed for authorised representatives.

4.2.2 Consumers using a pseudonym

- (a) If a consumer has a pseudonymous IHI, the online channel is unlikely to be available, and registration through an assisted channel would be required.

4.3 Activation: online channel

4.3.1 Portal Provider

- (a) To register and activate a PCEHR online, a consumer can:
 - (i) create an online account with a registered portal operator; and
 - (ii) then register for a PCEHR and activate the PCEHR via that online account.
- (b) If a consumer already has an online account with a registered portal operator, it would not be necessary for the consumer to create the online account.
- (c) We understand that for the first release, several registered portal operators are under consideration:
 - (i) A possible registered portal operator would be the Australian Government Online Service Portal (**AGOSP**). AGOSP is a gateway to information and services for around 900 Australian Government websites as well as selected State and Territory resources: www.australia.gov.au. Most material indexed by this site is created and stored externally to the site and is, therefore, the responsibility of the authoring department or agency. Finance is responsible for the development and ongoing operation of this site.
 - (ii) Private health insurers might wish to apply to become registered portal operators and provide access to the PCEHR System as a value added service to their members.
- (d) Alternatively, if a consumer does not have an online account with a registered portal operator and does not want to establish one, it is proposed that a generic URL⁴³ would be established by the System Operator to allow consumers to register online through a PCEHR specific registered portal operator.
- (e) registered portal operators will be required to pass a Conformance, Compliance and Accreditation (**CCA**) process and obtain a Notice of Connection (**NOC**) from the System Operator before being approved to connect to the PCEHR System.
- (f) The registered portal operator will use the information provided by the consumer to establish an online portal account for the consumer. The types of personal information a consumer may be required to provide to the registered portal operator are yet to be clarified.
- (g) The consumer will then log in to their registered portal operator account with a unique username and password. Once the consumer is logged in to their registered portal operator account they will be able to click on a link within the portal to register for a PCEHR.
- (h) The terms and conditions for participation in the PCEHR System will be displayed to the consumer.

⁴³ Discussions with the Department held on 29 August 2011

- (i) If the consumer chooses to participate in the PCEHR System they will then be asked to review and accept or decline the terms and conditions. We note that the Change and Adoption Partner is working on how the terms and conditions will be presented to consumers.
- (j) We also understand that there would be a minimum set of data that a consumer must provide to the registered portal operator (to mitigate the risk of a PCEHR being unlawfully created by a third party). This would likely include the consumer's name, date of birth, sex and Medicare card number.

4.3.2 HI Service

- (a) To establish a consumer's PCEHR, the System Operator will first need to request the IHI from the HI Service Operator. To make this request the consumer must disclose to the System Operator their:
 - (i) name;
 - (ii) date of birth;
 - (iii) sex; and
 - (iv) Medicare or DVA file number (**HI Information Set**).
- (b) The HI Information Set is the minimum amount of personal information required by the HI Service Operator to locate the unique IHI for that Consumer.
- (c) The System Operator discloses the HI Information Set to the HI Service Operator for the purpose of requesting the IHI for the Consumer.
- (d) Assuming the HI Information Set matches a record held by the HI Service Operator, the corresponding IHI will be disclosed to the System Operator and applied to the consumer's PCEHR.
 - (i) The PCEHR System will include a maximum number of times a consumer can attempt to create a PCEHR through a single portal account without providing the correct HI Information Set. Once that threshold is reached, that registered portal operator is locked out of the PCEHR System.⁴⁴
 - (ii) If the request for an IHI does not result in a match, then the consumer would be directed to Medicare to address any problems with the data. The consumer must fix any error in data held by Medicare before attempting to register again.⁴⁵

4.3.3 Proof of Record of Ownership (PORO)

- (a) After the consumer's IHI has been disclosed from the HI Service Operator to the System Operator, the consumer would be offered a range of organisations to complete the registration process; eg a Commonwealth agency or private health insurer.
- (b) The consumer must then successfully complete a PORO process which can be done online using a Trusted Data Source (**TDS**). An approved TDS is likely to be a government agency such as DHS or a private sector body with whom the consumer has an established relationship, such as a private health insurer.

⁴⁴ Notes on data flows (registration of the individual), diagram and narrative received from the Department, 8 August 2011

⁴⁵ Notes on data flows (registration of the individual), diagram and narrative received from the Department, 8 August 2011

- (c) The System Operator will disclose part or all of the HI Information Set to the TDS selected by the consumer for the purpose of identity verification.⁴⁶
- (d) DHS, for example, might ask a series of questions presented to consumers using information held in the consumer's agency records. Each question has an allocated point value and a consumer must achieve a sufficient number of points to prove they own the record they claim to.
 - (i) It is expected that these questions will be about recent interactions that the consumer had with the TDS, such as when the consumer last accessed a service from the TDS and details about the type of service.
 - (ii) If a consumer has not had any recent interactions with a TDS eg DHS, it is possible that sufficient questions may not be able to be generated from the TDS's records. This could be commonplace for healthy consumers who make few Medicare claims and do not have Centrelink payments.
- (e) When a consumer answers a question, the answer will be marked as correct, incorrect or 'did not answer' by comparing the answer provided by the consumer with the answer held on the consumer's record. At the conclusion of the questions, the consumer's responses will be calculated using a calculator tool.

4.3.4 Consumer passes the PORO process

- (a) If the consumer meets the minimum threshold, the consumer could proceed to finalise the registration and activation process.
- (b) If a sufficient number of points are achieved by the consumer, the System Operator will create a PCEHR for the consumer.
 - (i) This can be automatically linked to the consumer's registered portal operator account, if that was how they entered the registration process.
 - (ii) If the consumer entered the registration via the generic URL, the PCEHR could be linked to the generic URL instead.⁴⁷
- (c) The consumer will then be able to access their PCEHR by logging into their registered portal operator account using their username and password. For future access, the consumer only requires their user ID and password to open their portal account, and access to their PCEHR would be immediately available.

4.3.5 Consumer does not pass the PORO process

- (a) If the consumer does not meet the minimum threshold to 'claim' their records, the consumer will be advised that an insufficient number of points was achieved. The consumer may be asked to answer further questions to attempt to meet the minimum threshold. If the consumer is still unable to complete the PORO process satisfactorily, then we assume the consumer would be advised to complete registration via an assisted channel (face to face or mail).
- (b) If the consumer does not achieve a sufficient number of points, their identity will be verified through the use of an Identity Verification Code (IVC). The IVC is a one-time use number generated by the System Operator and given to a TDS. The TDS will then send the IVC by post, email or possibly text message to the consumer using the contact

⁴⁶ We have not reviewed whether this disclosure is consistent with the relevant provisions of the HI Act

⁴⁷ Email from the Department dated 12 September 2011

details listed with the TDS. We understand the current practice at Medicare and Centrelink is for all activation codes to be sent by post.

- (c) In our view, if a consumer cannot pass the PORO process, there is a risk that the individual is not the consumer who they claim to be. In these circumstances, rather than proceeding to authenticate the claimant by giving them an IVC, we suggest that the individual be directed to assisted registration channels (to mitigate the risk of a false PCEHR being activated) rather than proceeding to issue the individual with an IVC.
- (d) Consumers who are unable to complete this process online (for example, the consumer does not yet have an IHI, Medicare has a returned mail flag set for the consumer, etc.), the consumer will be provided with other options for completing the process (eg via assisted registration).
- (e) When the consumer receives the IVC they will enter the code into their registered portal operator account. This notifies the System Operator that:
 - (i) the consumer's PCEHR has been activated; and
 - (ii) the consumer's PCEHR has been linked to the consumer's registered portal operator account.⁴⁸
- (f) For future access, the consumer only requires their user ID and password to open their portal account, and access to their PCEHR would be immediately available.

4.3.6 Overview of the process for registering a minor (online channel)

- (a) The process for registering a minor is very similar to the process described above. To the extent that there are any differences, these are summarised below. A minor can also be registered by a parent or guardian using an assisted channel. We understand that if the minor is not on the Medicare card of the parent or guardian, then use of the assisted channel would be required in the same way as other authorised representatives – see paragraph 4.7 (Activation: authorised representatives must use assisted channels).⁴⁹
- (b) When the terms and conditions for participation in the PCEHR System are displayed to the guardian, the guardian will be asked to review and accept or decline the terms and conditions.
- (c) If the guardian agrees to the terms and conditions, the guardian would be asked to submit the guardian and minor's HI Information Set (name, date of birth, sex and Medicare card number), and an assertion that the person claiming to be the minor's guardian, is the guardian. We understand that this assertion is stored in a database associated to the Participation and Authorisation Service.⁵⁰
 - (i) Once this information is disclosed to the System Operator, the System Operator will check that the guardian and minor have the same Medicare card number.
 - (ii) We understand that checking the Medicare card numbers involves collection of a Medicare card number from both parent/guardian and minor. The System Operator will then be able to establish from this that the card numbers are the same, and IHI search will verify that Medicare numbers match the parent/guardian and minor.⁵¹

⁴⁸ Email from the Department dated 12 September 2011

⁴⁹ Email from the Department dated 16 September 2011

⁵⁰ Email from the Department dated 13 September 2011

⁵¹ Email from the Department dated 13 September 2011

- (iii) A guardian may not provide a DVA file number or an IHI in lieu of a Medicare card number. This is because the guardian must be able to demonstrate that the minor has the same Medicare card number as the minor to support the assertion that the guardian is, in fact, the guardian of the minor.
- (iv) The requirement to provide a Medicare card number reduces the risk of a minor being associated to the wrong parent, or the wrong individual altogether. This is a 'privacy positive' of the registration process.
- (v) When the operational details are clearer, we suggest reviewing the arrangements or policies relating to separated parents. For example, where a Court order is in place against a guardian, the design of the system should prevent that guardian from registering a minor for a PCEHR. If this is not included in the design, it creates a risk that:
 - (A) a minor fleeing from harm is associated to the harmful guardian; or
 - (B) a guardian could view the contact details for the other guardian and cause harm that way.
- (d) The HI Information Set is the minimum amount of personal information required by the HI Service Operator to locate the unique IHI for that consumer. The System Operator discloses the HI Information Set (of both the guardian and minor) to the HI Service Operator for the purpose of requesting the IHI for the minor.
- (e) Assuming the HI Information Set matches both of the records held by the HI Service Operator, the corresponding IHI will be disclosed to the System Operator and applied to the minor's PCEHR.

4.3.7 Privacy Risks - Online registration - verification of identity

- (a) The detailed processes for online registration were not fully developed during Phase One and Phase Two.
- (b) One option being developed is the use of 'Trusted Data Sources', such as DHS or private health funds also operating Conformant Provider Portals, which could help to verify a consumer's identity through a 'challenge and response' mechanism.
- (c) There is a risk that the online channel introduces new 'collections' of personal information by registered portal operators.

4.3.8 Recommendation - Online registration - verification of identity

- 4.6 That there be a further review of the detailed plans for online registration, to ensure the online channel offers a similar level of privacy protection as the assisted registration channels, particularly in terms of collection necessity and data security.
- 4.7 That the PCEHR Bill clearly describe the type of information to be used and disclosed to verify consumer identity, by whom it will be used or disclosed, and for what purposes.
- 4.8 That there be a further review of the detailed plans for face to face registration of a minor, to ensure the face to face channel offers a similar level of privacy protection as the online channel, particularly in terms of data security and association to the correct guardian.
- 4.9 That there be a further review of the purpose of asking 'challenge and response' questions, noting that verification can alternatively occur by entering an IVC number, irrespective of whether the questions are answered correctly.

4.3.9 Annotations to recommendations 4.6 and 4.8 (Registration of newborns)

- (a) In its submission concerning the Bill, SA Health noted that the draft Bill excluded newborns from being registered for a PCEHR.⁵²
- (b) The exclusion of newborns may relate to the effectiveness of the PCEHR System rather than raising any new privacy risk. However, once the arrangements for the registration process for newborns are clearer the privacy implications should be considered.

4.4 Activation: face to face channel

4.4.1 An overview of the face to face channel

- (a) We note this is also known as the 'fast track process'.
- (b) A consumer can register for a PCEHR in person by attending an Authorised Registration Agent (ARA). An ARA is likely to be employed by a Commonwealth agency eg DHS (Medicare program) or private sector bodies eg aged care facility operators.
- (c) The consumer would enquire about registering for a PCEHR. Before providing assistance with registration, an ARA will require the approval of the consumer to act on their behalf. The ARA will then use an Administration Portal to help the consumer complete the registration process.⁵³

4.4.2 Attending a shop front to register for a PCEHR

- (a) The ARA provides the consumer with a hard copy of the terms and conditions of participation in the PCEHR System. The consumer must accept the terms and conditions for participation before continuing with registration. Acceptance will be indicated by signing a copy of the terms and conditions. We understand that the consumer's decision to consent would be stored in a database associated to the Participation and Authorisation Service.⁵⁴
- (b) The Participation and Authorisation Service has three major functions:
 - (i) managing the participation process for registration of consumers and their representatives;
 - (ii) capturing administrative information, settings and preferences about consumers and their representatives; and
 - (iii) controlling access to a consumer's PCEHR based on their access control settings.⁵⁵
- (c) The consumer will then be asked to disclose to the ARA the HI Information Set which will be disclosed to the System Operator in order to request the consumer's IHI from the HI Service Operator.
- (d) The consumer will also be asked to show 100 points of identification in order for the ARA to verify the identity of the consumer. The ARA will assess the identity claim using the 100 points provided. It is not proposed for an ARA to keep a copy of the identity records on file but will make a notation of what documentation was sighted.
- (e) The ARA will notify the System Operator that the consumer's identity has been verified and will disclose the HI Information Set to the System Operator.

⁵² Submission to the Bill from SA Health dated 26 October 2011, page 4 re clause 34 of the Bill.

⁵³ Con Ops, section 6.3.6 (Administration Portal)

⁵⁴ Email from the Department dated 12 September 2011

⁵⁵ Con Ops, section 6.4.2 (Participation and Authorisation Service)

- (f) The System Operator then discloses the HI Information Set to the HI Service Operator for the purpose of requesting the IHI for the Consumer.
- (g) Assuming the HI Information Set matches a record held by the HI Service Operator, the corresponding IHI will be disclosed to the System Operator to be applied to the consumer's PCEHR.

4.4.3 Face to face channel: use of an 'activation code'

- (a) The System Operator will create a PCEHR for the consumer and will generate a one-time activation code which will enable the consumer to link their PCEHR to a registered portal operator account at a later date, if the consumer chooses to associate their registered portal operator account.
- (b) The System Operator provides the activation code to the ARA. The ARA would then print a copy of the activation code for the consumer and advises the Consumer that registration is complete.
- (c) Noting that all that is required to activate and link the accounts is the activation code, it will be important for consumers to be advised to keep the code secure and to activate their PCEHR as soon as practicable (to mitigate the risk of the activation code being misplaced, stolen or otherwise compromised).
- (d) With the PCEHR created, the consumer may proceed to set up their access controls, elect any nominated representatives that they wish to have access to their PCEHR and also enter details of emergency contacts such as next of kin and custodians of advanced care directives. This will involve the disclosure of third party personal information to the System Operator.
- (e) After the consumer receives the activation code they would enter the code into their registered portal operator account. This notifies the System Operator and their PCEHR will be linked to the consumer's registered portal operator account. For future access, the consumer only requires their user ID and password to open their portal account, access to their PCEHR would be immediately available.

4.5 Activation: mail channel

- (a) A consumer will also be able to register for a PCEHR by mail. The consumer obtains a registration form by downloading a copy from the internet, contacting the PCEHR call centre or ARA and requesting that a copy be mailed to them.
- (b) The consumer completes the form and discloses the HI Information Set together with a surface mail address.
- (c) The consumer then submits the completed registration form to the System Operator by mail. We understand that the following details will be required (where applicable):
 - (i) certified copies of 100 points of identification of the consumer;
 - (ii) details about the consumer's preferred access controls;
 - (iii) any nominated representatives that they wish to have access to their PCEHR;
 - (iv) details of emergency contacts such as next of kin; and
 - (v) details of custodians of advanced care directives.
- (d) As such, this will involve the disclosure of third party personal information to the System Operator.

- (e) The System Operator will disclose the HI Information Set to the HI Service Operator for the purpose of requesting the IHI for the Consumer.
- (f) Assuming the HI Information Set matches a record held by the HI Service Operator, the corresponding IHI will be disclosed to the System Operator to be applied to the consumer's PCEHR.
- (g) The System Operator will create a PCEHR for the consumer and will generate a one-time use passcode for the consumer to use if they wish to link their PCEHR to a registered portal operator account at a later date.
- (h) The System Operator notifies the consumer that the registration process is complete and provides the consumer with the activation code (presumably via mail⁵⁶).
- (i) After the consumer receives the activation code, they will enter the code into their registered portal operator account. This notifies the System Operator and their PCEHR will be linked to the consumer's registered portal operator account.
- (j) With the PCEHR created, the consumer may proceed to set up their access controls, elect any nominated representatives that they wish to have access to their PCEHR and also enter details of emergency contacts such as next of kin and custodians of advanced care directives. This will involve the disclosure of third party personal information to the System Operator.

4.6 Assisted Registration – verification of identity

4.6.1 Privacy Risks

- (a) Whether by mail or through a shopfront, assisted registration requires the consumer (or their authorised representative) to provide 100 points worth of records (or certified copies of those records) as evidence of their identity (EOI).
- (b) We understand that ARAs are expected to sight, but not copy, the EOI records. It is not clear whether or not the ARA will be expected to keep a record of the EOI record number, such as passport number or driver's licence number.
- (c) There is a risk that ARAs will not realise if fake or forged EOI records are presented to them. Further, any collection of information about EOI creates a new 'identity store', which raises the risk profile of the ARA, in terms of managing their own information security. (For some ARAs this may simply increase an existing risk they have, rather than create a new risk.)
- (d) We suggest that ARAs for the PCEHR instead be encouraged to utilise the national Document Verification Service (DVS), which is currently being implemented across Australian, State and Territory government agencies. Use of the DVS would enable ARAs to check the validity of typical presented EOI records (birth certificates, passports and driver's licences) in real time, and generate an audit log of the transaction in case it is needed in a future investigation, without actually storing any of the EOI information itself.
- (e) Legislation should also ensure the secure disposal of any copies of EOI records sent to an ARA by mail, and confirm our understanding that the design of the process has changed since version 0.13.6 of the Con Ops, such that it will not be possible for consumers to simply send a letter or form from a Justice of the Peace (JP) to state that their EOI records have been sighted by the JP.

⁵⁶ Email from the Department dated 12 September 2011

4.6.2 Recommendations

- 4.10 That ARAs for the PCEHR be encouraged to utilise the national Document Verification Service, instead of recording details of the EOI records presented.
- 4.11 That the PCEHR Bill provide that ARAs for the PCEHR may not keep copies of EOI records, and that any such copies must be securely destroyed as soon as the registration process is complete.
- 4.12 That the PCEHR Bill clarify whether ARAs for the PCEHR may or must keep a record of a record of the EOI record number.
- 4.13 That the PCEHR Bill require consumers seeking to register via mail to post certified copies of the EOI records (not just a statement from a JP about sighting the records).
- 4.14 That the arrangements with ARAs ensure that there are physical privacy protections for consumers using their shop fronts, such as timed logouts and privacy screens on public-facing computers.
- 4.15 That the arrangements with ARAs ensure that there are administrative and technical privacy protections, such as appropriate staff screening, staff training in privacy obligations, and audit logging of staff registration transactions.

4.7 Activation: authorised representatives must use assisted channels⁵⁷

4.7.1 An overview of the registration process for consumers lacking capacity

- (a) Consumers with diminished capacity will be unable to register for a PCEHR online. A consumer's authorised representative must use the face to face or mail channels.

4.7.2 Authorised representatives: face to face channel

- (a) The process for registering a consumer with diminished capacity is similar to the regular face to face process described above. To the extent that there any differences, these are summarised below.
- (b) Firstly, an authorised representative would enquire about registering for a PCEHR by attending an ARA.
- (c) If the authorised representative agrees to the terms and conditions, the authorised representative would be asked to submit:
 - (i) the authorised representative and consumer's HI Information set (name, date of birth, sex and Medicare card number); and
 - (ii) documentary evidence of legal authority to act on the consumer's behalf (for example, a guardianship order or power of attorney) must also be provided to the ARA.
- (d) It is then proposed for the ARA to assess:
 - (i) the identity claim of the authorised representative; and
 - (ii) the authenticity of documentary evidence of legal authority provided.
- (e) We understand that it is not proposed to require 100 points of suitable identification from the consumer.

⁵⁷ Other than for minor children, where online registration can be used in some circumstances – see paragraph 4.3.6 (Overview of the process for registering a minor (online channel))

- (f) The HI Information Set is the minimum amount of personal information required by the HI Service Operator to locate the unique IHI for that Consumer. The System Operator discloses the HI Information Set (of both the authorised representative and consumer) to the HI Service Operator for the purpose of requesting the IHI for the consumer.
- (g) Assuming the HI Information Set matches both of the records held by the HI Service Operator, the corresponding IHI will be disclosed to the System Operator and applied to the consumer's PCEHR.

4.7.3 Authorised representatives: mail channel

- (a) The process for registering a consumer with diminished capacity is similar to the regular mail process described above. To the extent that there any differences, these are summarised below.
- (b) When an authorised representative completes a registration form, the authorised representative must disclose the HI Information Set for both the consumer and themself. In the HI Information Set, a Medicare card number may be replaced with a DVA file number or IHI.
- (c) It is then proposed for an authorised representative to present to a JP for sighting:
 - (i) 100 points of suitable identification; and
 - (ii) documentary evidence of legal authority to act on behalf of the consumer.
- (d) We understand that certified copies of 100 points of identification belonging to the authorised representative will be required to be sent to the System Operator. We understand that it is not proposed to require 100 points of suitable identification from the consumer.⁵⁸
- (e) The HI Information Set is the minimum amount of personal information required by the HI Service Operator to locate the unique IHI for that Consumer. The System Operator discloses the HI Information Set (of both the authorised representative and consumer) to the HI Service Operator for the purpose of requesting the IHI for the consumer.
- (f) Assuming the HI Information Set matches both of the records held by the HI Service Operator, the corresponding IHI will be disclosed to the System Operator and applied to the consumer's PCEHR.

4.7.4 Privacy Risks - Registration via authorised representative

- (a) We understand that authorised representatives of child consumers (typically the child's parent/s) will need to produce their own EOI, and a Medicare card to demonstrate their link to the child consumer.
- (b) Authorised representatives of adult consumers will need to produce their own EOI, and separate evidence of their position as a representative of the adult consumer, such as a guardianship order. However we understand that no EOI for the adult consumer will be required.
- (c) If sufficient EOI is not presented for both the consumer and the authorised representative, there is a risk that the authorised representative will be associated to the wrong consumer. We suggest that the authorised representative of an adult consumer also be required to produce at least the Medicare card or similar of the adult consumer.

⁵⁸ Email from the Department dated 12 September 2011

- (d) In the case of an enduring guardianship, we further suggest that the authorised representative be required to also produce some evidence (such as a letter from the consumer's GP) that the consumer now lacks capacity, such that that guardianship responsibility has been triggered.

4.7.5 Recommendations - Registration via authorised representative

- 4.16 That the PCEHR Bill provide that in order to register an adult consumer, an authorised representative must provide:
- certified copies of 100 points worth of evidence of their own identity;
 - certified copy of documentary evidence of legal authority to act on behalf of the consumer eg certified copy of guardianship order;
 - the Medicare card of the consumer; and
 - where the evidence of their position as a representative of the adult consumer is unclear as to the consumer's current state of capacity, further evidence that the consumer currently lacks the capacity to make a decision about registration, or manage their PCEHR, themselves.
- 4.17 That communications to consumers explain the registration rules in relation to authorised representatives, including those appointed under enduring guardianship arrangements.

4.7.6 Phase Two Annotation - Registration via authorised representative

- (a) In its submission to the Bill SA Health stated that it was unclear from the Bill whether the authorised representative had to have a verified healthcare identifier in order to be registered.⁵⁹ It is our understanding (see section 4.7.2(f)) that this is the case. If this is correct then, unless there are countervailing policy reasons, the Bill or the PCEHR Rules should say so.
- (b) In its submissions to the Bill, Medibank Private raised a concern that the Bill does not allow for concurrent authorisation of the consumer and his/her authorised representative.⁶⁰ The Companion document to the Bill notes that *'The consumer will not be able to access [his/her] PCEHR unless the authorised representative has granted her or him access as a nominated representative (see section 3.3.1 of the ConOps)'*. Whether this outcome is desirable from a privacy perspective will largely depend on the basis for the authorised representative being appointed in the first place. We suggest that if possible, the design of the PCEHR System accommodate some flexibility for this concurrent access to occur and at the very least the PCEHR Rules not prohibit such an outcome.

4.8 Pre-population of data into PCEHR

4.8.1 Data from Medicare

- (a) DHS, through the Medicare program, is able to provide a longitudinal source of information amount about a consumer's healthcare events, including:
- (i) information about healthcare events funded under the Medicare Benefits Schedule (MBS), such as:
- (A) date of service;
 - (B) provider;

⁵⁹ dated 26 October 2011, page 3

⁶⁰ Submission dated 25 October 2011, page 2

- (C) service in hospital indicator;
- (D) item number; and
- (E) brief Item description;
- (ii) information about packets of medicines dispensed under the Pharmaceutical Benefits Scheme (**PBS**), such as:
 - (A) date of supply;
 - (B) date of prescribing;
 - (C) item Code;
 - (D) brand;
 - (E) brief item description;
 - (F) quantity; and
 - (G) number of repeats;
- (iii) information about vaccinations given to children under the age of 7 via the Australian Childhood Immunisation Register (**ACIR**), such as:
 - (A) date vaccination received;
 - (B) vaccine type and provider;
 - (C) vaccine dose number;
 - (D) natural Immunity;
 - (E) information provider; and
 - (F) medical contraindications; and
- (iv) donation decisions recorded with the Australian Organ Donor Register (**AODR**), such as:
 - (A) date of initial registration;
 - (B) donor end date;
 - (C) donor nominations;
 - (D) for each nomination that exists:
 - (I) donor's consent;
 - (II) donor's intent; and
 - (III) donor nomination.
- (b) Financial information associated within Medicare supplied information is not accessible by the PCEHR System.
- (c) Two of the four proposed data 'streams' (organ donor status and childhood immunisation history) pose fewer privacy concerns than the other two: a list of claimed events (MBS) and/or medications dispensed (PBS), running up to two years into the past.
- (d) We understand that each Item Number and Item Code in the MBS and PBS data streams is associated to a brief item description. In some instances, the description could disclose medical information about a consumer. For example, some blood tests are only performed

if a consumer has diabetes. A health literate consumer could identify that the consumer has diabetes and had a blood test. This discloses health information.

- (e) We also note that while the MBS and PBS data may be considered of limited clinical value, it will be of some value in the early days of a PCEHR, until Event Summaries and other records begin to 'enrich' the clinical history of each consumer.⁶¹

4.8.2 Privacy Risks – Medicare Data

- (a) The risk is that MBS and/or PBS data may disclose health information that the consumer wishes not to be exposed in their PCEHR, thus undermining their intention when setting other access controls in relation to uploading clinical information about a particular illness or episode of care. This risks unlawful / unauthorised collection by other users of the PCEHR.
- (b) The consumer may mitigate this risk by:
 - (i) not consenting to the disclosure of MBS or PBS data into their PCEHR; or
 - (ii) after the fact, managing individual data items by way of access controls, such as 'Limited View' or 'Remove From View'.
- (c) The latter option assumes a fairly high degree of 'health literacy' from the consumer, such that they can identify which MBS / PBS data items relate to a particular illness or episode of care. This may expose consumers to privacy risks which they thought they had controlled through other means.
- (d) We also suggest clarifying which data streams can be populated with historical data. We understand that Medicare data fields are the only fields which have the ability to be populated with historical data. This is distinct from other data fields of a PCEHR, which can only be populated with data created after the date of registration. Clarification on these points will assist a consumer to better understand how their PCEHR will operate in practice.
- (e) To illustrate by example, consider a consumer who had a sensitive episode of care prior to registering for a PCEHR, such as a pregnancy termination. If this consumer consented to the pre-population of all Medicare streams, both current and historical, the consumer may not fully understand or appreciate that the episode of care will appear in their PCEHR. Unless the 'streaming controls' are clearly communicated to the consumer, the consumer may give consent on a misinformed basis, namely that only data relating to episodes of care after the date of registration would be uploaded from Medicare.

4.8.3 Recommendations – Pre-population of Medicare Data

- 4.18 That the PCEHR Bill authorise the disclosure of each 'stream' of Medicare held data (MBS, PBS, organ donor status and/or childhood immunisation records) to a consumer's PCEHR, upon confirmation that the consumer has provided a positive consent to that 'stream'.
- 4.19 That the final design allow a consumer who consents to the MBS and/or PBS data stream to choose whether they wish the data stream to include data already collected up to two years prior to the date of their consent, with the default position being 'no back dated data'.
- 4.20 That the PCEHR Bill clarify which data 'streams' can be populated with data that pre-

⁶¹ Con Ops, section 4.3.8 (Medicare information)

dates the commencement of the consent decision.

- 4.21 That consumer communications advise consumers who are concerned about the privacy of specific illnesses or episodes of care (such as a pregnancy termination), that unless they are very health literate and prepared to 'remove from view' specific data items, their best option may be to not consent to the disclosure of the MBS / PBS data streams into their PCEHR.

4.9 Setting consumer controls

4.9.1 An overview of personal control settings

- (a) Central to the PCEHR System is the concept of personal control. Participating consumers can exercise control over their PCEHR in the following ways:
- (i) *Decide whether or not to have an active PCEHR:* The PCEHR System operates on an opt-in model, where consumers elect to register and create a PCEHR. Consumers may deactivate their PCEHR at any time and subsequently reactivate their PCEHR at any time.
 - (ii) *Access information in their PCEHR:* Consumers will be able to view any health information contained in their PCEHR.
 - (iii) *Set controls around healthcare provider access:* Consumers may determine and change settings around access to their PCEHR by participating healthcare organisations involved in their healthcare.
- (b) Consumers may choose from a range of approaches to setting and managing these controls that will give general or limited access. Some access controls may be overridden in situations where the consumer requires emergency care.
- (i) *Authorise others to access their PCEHR:* Consumers may nominate other people (such as carers and family members) to view their PCEHR as a nominated representative. (By contrast authorised representatives will have full access to a consumer's PCEHR.)
 - (ii) *Choose which information is published to and accessible through their PCEHR:* Consumers may request healthcare providers to withhold certain information from their PCEHR.
 - (iii) *View an activity history for their PCEHR:* The PCEHR System will provide an audit trail so that consumers can view a history of actions on their PCEHR.
 - (iv) *Make enquiries and complaints:* Consumers may make enquiries and complaints in relation to the management of information in their PCEHR and the PCEHR System.
- (c) We understand that appropriate information and support will be made available to consumers to exercise proper decision-making and determine consent with regard to the controls described here. Establishment and maintenance of these controls will be available via a range of channels.⁶²

⁶² Con Ops, section 3.2.1 (Personal control)

4.9.2 The Access List

- (a) Access to information within the PCEHR System will be moderated by a series of access controls managed by the consumer. For each consumer's PCEHR, the PCEHR System will maintain:
 - (i) an 'Access List'; and
 - (ii) a series of either basic or advanced access control settings.
- (b) Each of these items are discussed below. To help consumers understand the access controls, registered portal operators will provide an online interactive tutorial. We understand that consumers must view the online interactive tutorial before a consumer adjusts advanced access settings.
- (c) Consumers will also be able to call the Call Centre to seek support in understanding the access controls.
- (d) Some access controls may also be overridden in situations where the consumer requires emergency care (see Con Ops, section 5.5.4).
- (e) At the core of access control to a consumer's PCEHR is the 'Access List'. The Access List provides a set of organisations that are permitted to access a consumer's PCEHR. The Access List contains a list of healthcare organisation's HPI-Os and by inference includes all network HPIOs beneath the participating organisation HPI-O.
- (f) Through the exercise of access controls, the consumer can control how an organisation is added (or removed) from the list.
- (g) Consumers will be able to see the Access List and update it at any time via a number of channels (including the registered portal operators, shop front services, etc). In general, organisations will remain on the Access List for a period of 3 years from the last time they accessed a consumer's PCEHR. After 3 years of inactivity the PCEHR System will automatically remove the organisation from the Access List and the organisation will need to re-obtain access based on the consumer's access control settings.

4.9.3 Basic access controls

- (a) If a consumer opts for their PCEHR to be operated using basic access controls, the PCEHR will operate on a 'care based access' mode, and any organisation involved in the care of the consumer will be able to add themselves to a consumer's Access List. We understand that where a consumer does not exercise a choice at the time of registration, the default access controls will be 'basic access'.

4.9.4 Phase Two Annotation to subparagraph 4.9.3 (Basic access controls)

- (a) In its submission to the Bill, the Australian Medical Association submitted that 'to ensure ongoing review of the system and the effectiveness of the privacy control settings for the PCEHR, the mechanism by which the System Operator specifies default access controls under section 11(b) should be a disallowable instrument.'⁶³

⁶³ Submission to the Bill from the Australian Medical Association, page 3

- (b) Section 11 (b) (Functions of the System Operator) is extracted below:

The System Operator has the following functions:

...

(b) to establish and maintain mechanisms (access control mechanisms):

(i) that enable each registered consumer to set controls on who may obtain access to health information included in the consumer's PCEHR; and

(ii) that specify default access controls that apply if a registered consumer has not set such controls;

- (c) The Bill has an existing mechanism for specifying the default access controls. The Minister may, by legislative instrument (and which are disallowable), make PCEHR Rules on a range of matters that apply to participants in the PCEHR System, including but not limited to, the administration and day-to-day operations of the PCEHR System: s 97 (3).
- (d) We agree that the access rules are significant in determining the privacy protections for consumers. To support the management of privacy risks it would be appropriate for the Bill to recognise that access controls would be within the ambit of the PCEHR Rules.

4.9.5 Advanced access controls

- (a) Consumers will be given the option of creating a series of advanced access control settings. The advanced access control settings will include all basic access control settings as well as some additional access controls.
- (b) Advanced access control settings are only accessible via a registered portal operator. Due to the nature of these controls consumers will need to complete the online interactive tutorial before using the settings.
- (c) Additional options available under advanced settings include:
- (i) setting up a PACC;
 - (ii) setting up a Provider Access Consent Code (**PACCCX**) for access to a record within a PCEHR;
 - (iii) restricting organisations from being on the Access List;
 - (iv) an ability to prevent a PCEHR from being found; and
 - (v) managing record level access.

4.9.6 Advanced consumer control: Provider Access Consent Code (PACC)

- (a) If the consumer chooses to set up a PACC (effectively a PIN or passphrase), then organisations will not be able to add themselves to the Access List unless they have the PACC. We understand that consumers cannot set up a PACC at the time of registration but may do so immediately after.⁶⁴
- (b) If the consumer opts to set up a PACC, then they will also be requested to answer the following question:

'If you forget your PACC, do you wish participating organisations to be able to access your PCEHR by obtaining your consent?'

⁶⁴ Email from the Department dated 12 September 2011

- (c) If the consumer responds 'no', then access will not be granted to the organisation without the valid PACC. If this setting is set to 'yes', then participating organisations will be able to access the consumer's PCEHR without the valid PACC when the consumer forgets their PACC. The reason for accessing their PCEHR without a PACC will be recorded in the audit trail. The organisation will only be granted access to 'general access' information.
- (d) If this setting is set to 'yes', the consumer will also be asked:

'Do you want to be notified if your PCEHR is accessed without your PACC?'
- (e) If the consumer opts to be notified, they will be notified via their preferred method whenever access without their PACC occurs.

4.9.7 Privacy positives

- (a) The flexible, 'sliding scale' set of additional access controls available to the consumer is a privacy positive aspect of the system design. Consumers can choose how much they want to be involved in on-going access control management, such as:
 - (i) whether they want to set a password-based PACC;
 - (ii) whether they want supply of the PACC to be mandatory for access by a provider (except in emergencies);
 - (iii) (if 'no' to the above) whether they want to be notified if their PCEHR is accessed without their PACC; and
 - (iv) whether they want to be notified when a new healthcare organisation is added to their Access List.
- (b) Other privacy setting choices include:
 - (i) whether they want their PCEHR to be automatically 'findable' by a local clinical system;
 - (ii) the ability to set 'General', 'Limited' or 'Revoked' access rights for organisations in their Access List;
 - (iii) the ability to ask a healthcare provider to not upload a record to the PCEHR;
 - (iv) the ability to set 'General' or 'Limited' access PCEHR Rules over consumer records indexed in the PCEHR; and
 - (v) the ability to 'Remove From View' consumer records indexed in the PCEHR.
- (c) As the Con Ops states:

*Many individuals who choose to have a PCEHR will probably not exercise all these options. However, when building a national system we must allow for those people with specific sensitivities to participate in a way that is respectful and responsive to their concerns.*⁶⁵
- (d) This statement provides an important recognition that consumers should not be expected to choose between realising the benefits of a PCEHR and protecting their privacy; a well-designed shared EHR system should aim to deliver both.

⁶⁵ Con Ops, April 2011, part 5.1

- (e) There are a number of types of 'specific sensitivities' that a consumer might have, depending on their circumstances, and the proposed design is to provide a number of access controls and other privacy settings to mitigate the risks they face. For example:
 - (i) a public figure (such as a celebrity) may be concerned about the 'curious onlooker'; they could choose to set a PACC to restrict access to their record;
 - (ii) a person with a one-off episode of care which they consider particularly private (such as a pregnancy termination) could request that their healthcare provider to not upload information from that episode to their PCEHR, and/or may choose to 'Remove From View' records which disclose that episode;
 - (iii) a person with an on-going illness which they consider particularly private (such as treatment for depression) could either set a PACC to restrict access to their record, or request their healthcare provider to not upload information about that illness to their PCEHR, and/or 'Remove From View' records which disclose that illness; and
 - (iv) a person concerned about their personal safety through exposure of their home address (such as a person who has fled a violent relationship, or who may face threats due to their position eg as a police officer or judge or a public figure) may choose to prevent display of their home address (subject to a design change we have recommended), set a PACC and/or 'revoke' access rights by certain organisations.
- (f) Generally speaking, the intended design reflects a balance between protection and flexibility/efficiency, offering a sliding scale of access controls and other privacy-related choices, to suit a range of consumer preferences and circumstances.

4.9.8 Privacy risks – 'Not Findable' Feature

- (a) One of the proposed privacy settings is allowing a consumer to decide whether they want their PCEHR to be automatically 'findable' by a local clinical system. If 'yes' (the default position), the design intention is that there would be something like a green 'dot' or 'flag' appearing on a healthcare provider's screen when they looked at their local records for that consumer, to prompt them to 'click through' to the PCEHR.
- (b) However if the consumer chooses the 'not findable' option, the current design intention is that while the existence of the consumer's PCEHR would not be 'flagged' in the local clinical system, the healthcare provider or other user could still search for the PCEHR using a more manual process (ie entering the consumer's IHI). The intention is that the healthcare provider should only do this with the consent of the consumer, but the proposed design will not ensure this.
- (c) However, we understand that the 'not findable' setting is designed to allow the consumer to give access to the PCEHR if he or she chooses, without having to remember a PACC. This access control setting may have particular benefit for those with a mental illness or other condition affecting their ability to remember a PACC. It can also be used in conjunction with a PACC to prohibit access except in emergency scenarios. We therefore suggest that the 'no findable' setting be re-named to provide clearer picture for the consumer.

4.9.9 Recommendations - 'Not Findable' Feature

4.22 That the default position for consumers be that the existence of their PCEHR will be 'flagged' within local clinical systems unless the consumer chooses otherwise.

4.23 That there be a name change to the 'not findable' access control, to instead be called 'not

flagged'.

4.9.10 Privacy Risks - The Access List

- (a) A consumer's primary privacy concern might be about a specific individual, such as their ex-partner or a neighbour, accessing their PCEHR, either to find their home address or to find out health information about the consumer.
- (b) The current design does not allow consumers to 'block' specific users from accessing their PCEHR. Their only option is to set access controls for the organisation for which the specific user works.
- (c) The intended design would allow a consumer to move an organisation on their Access List into a 'Revoked' status. However this may not be done in advance of the organisation obtaining access in the first place, and it would not affect access to any personal information or health information already 'downloaded' from the PCEHR into that organisation's local systems. There may also be a risk that an organisation with 'Revoked' status has stored a record of the consumer's PACC in their local systems, and thus gains access afresh.
- (d) The 'Revoked' access control is set on the HPI-O level, which may be fairly small, such as a single GP surgery or a unit within a hospital, or it may be extremely wide, such as if one HPI-O is set for an entire State network of public hospitals. The consumer will not necessarily know if the specific individual they are concerned about has moved positions (or works for multiple HPI-Os), or if the changing structure of an HPI-O has the effect of undermining the intention of their access control settings.
- (e) We also understand that an organisation's HPI-O may change frequently. The fluctuating nature of an HPI-O may make it harder for a consumer to accurately identify the organisation they wish to 'revoke'.⁶⁶
- (f) There are therefore a number of practical limits to the extent to which the 'Revoked' privacy control can mitigate the specific risk faced by the consumer.
- (g) To a certain extent, this situation exists now; a consumer may choose to avoid a particular hospital or GP surgery so that a specific, known individual will have no opportunity to peruse their records. However the situation will be exacerbated with the PCEHR, if the size of the 'organisation' covered by an 'Access List' is larger than a single hospital or practice - the consumer may not have a practical choice about where to obtain their healthcare other than through that organisation.

4.9.11 Recommendations – The Access List

- 4.24 That consumer communications carefully explain the practical limits of the 'Revoke' access control option.
- 4.25 That the PCEHR Bill prohibit healthcare organisations from recording a consumer's PACC or PACC-X for future use (ie in the event that the organisation is moved to 'Revoked' status).
- 4.26 That one option for the range of optional consumer notifications (SMS messages or emails) should be to receive a notification if an organisation on their 'Revoke' list changes their HPI-O in some way.
- 4.27 That the Department develop some incentive for organisations to set their HPI-Os (for the

⁶⁶ Minutes of meeting from the National Health and Information Regulatory Framework Working Group dated 2 September 2011

purposes of the Access List) at a level which reflects the management of records within the organisation itself.

4.9.12 Privacy Risks - Complexity for consumers

- (a) While the number of different privacy settings available to consumers offers a privacy positive, there is also a risk inherent in the design complexity, such that consumers may not understand their own settings. The particular risk is that consumers may expose themselves to risks they thought they had mitigated.
- (b) For example, consumer communications will need to warn consumers that exercising the 'Remove From View' option does not mean 'delete entirely', so the record will still be legally discoverable. As noted above, the limited 'reach' of access controls expressed in the PCEHR System should also be clearly explained, so that consumers understand that local clinical systems may be treated differently. These messages should be available to consumers before they decide to register for a PCEHR.
- (c) We also recommend including a 'preview' tool which allows consumers to see how a record or 'view' will look like to the user in question - such as what their nominated representative will 'see', or what a healthcare provider on 'General' access will 'see'. Implementing a preview tool may be a simpler way of communicating to consumers how their access settings will work (before those settings 'go live'), than requiring consumers to take an online tutorial. Communications should regardless be provided to consumers on the consequences of adjusting their setting in the manner selected.

4.9.13 Recommendations - Complexity for consumers

- 4.28 That consumer communications about the various privacy control settings and the limits to those settings be available to consumers before they decide to register for a PCEHR.
- 4.29 That consumers have available to them a 'preview' function which allows the consumer to see how their record will appear to other types of users depending on the access controls they set.

4.9.14 Privacy Risks - Creating nominated representatives

- (a) The current design allows a consumer to have one or more 'nominated representatives', with no set time period for their nomination. There is a risk that consumers will 'set and forget' who else can see their PCEHR. Although this is a risk created by consumers, the design of the system could potentially assist consumers to protect their own privacy, with a reminder every few years.

4.9.15 Recommendations - Creating nominated representatives

- 4.30 That the design of the system include some prompt every few years (such as a screen prompt on next log in) to consumers with nominated representatives to review their choices and check the accuracy of their information.

Chapter 5 - Access to and use of a PCEHR

5.1 Consumer access

5.1.1 Overview of consumer access entry points

- (a) The PCEHR System needs to be accessible in a range of situations, including situations where a consumer may not have access to a computer or the Internet, may not be computer literate, may not speak English or may have an impairment or disability that may affect their ability to access the PCEHR System.
- (b) While achieving full equity of access may not be possible in a number of situations, the PCEHR System will put in place a number of options that will help facilitate access in a range of different situations. As the PCEHR System progresses, the range of options available will be enhanced.⁶⁷
- (c) Consumers can gain access to the PCEHR System through a variety of channels:
 - (i) registered portal operators (**online channel**);
 - (ii) Call Centre (**telephone channel**);
 - (iii) shop front (**face to face channel**); and
 - (iv) postal system (**mail channel**).
- (d) The Call Centre, shop front and mail handling staff would interact with the PCEHR System through either the Registration Portal or Service Portal (depending on the nature of the activities being undertaken). The Administration Portal is intended to support internal System Operator functions such as system configuration management.⁶⁸

5.1.2 Consumer access: online channel

- (a) Once a consumer has registered for a PCEHR, they may access their PCEHR with a choice of two entry points:
 - (i) an existing registered portal operator eg DHS website or the Australian Government's AGOSP hub (www.australia.gov.au); or
 - (ii) a PCEHR specific URL to be established for the PCEHR.
- (b) Consumers must correctly enter their unique username and password to access their PCEHR.
- (c) We also understand that consumers may have the option of including additional 'challenge response' questions or 'secret questions and answers'.
 - (i) These questions and answers are distinct from the questions presented to a consumer at the time of registration and deactivation (PORO questions generated from a Consumer Portal eg DHS).
 - (ii) The additional 'secret questions and answers' would be drafted by the consumer themselves.⁶⁹

⁶⁷ Con Ops, section 3.2.5 (Ensuring access in a range of different situations)

⁶⁸ Response from NEHTA dated 30 August 2011

⁶⁹ Response from NEHTA dated 15 August 2011

- (iii) When the operational details are clearer, we suggest reviewing this process for privacy impacts.⁷⁰

5.1.3 Overview of consumer access: assisted channels

- (a) While the use of computers and broadband is becoming increasingly pervasive across Australia, the PCEHR System will still need to support a number of avenues for consumers who either do not have access to the Internet or may not be able to use a computer. Consumers in this situation will be able to:
 - (i) register (and withdraw) using an assisted registration process or a mail based process;
 - (ii) access a 24-hour Call Centre to help them manage their PCEHR and answer general questions about the PCEHR System; and
 - (iii) identify representatives to help them access and manage their PCEHR.
- (b) Assistance will also be provided to consumers via Medicare shop fronts, Call Centre and remote area support services.
- (c) Some healthcare providers may help consumers to access their PCEHR information, by, for example, providing printed copies of relevant information to take home.⁷¹

5.1.4 Consumer access: telephone channel

- (a) The System Operator will provide a Call Centre to allow consumers to obtain general information about the PCEHR System, register/withdraw from the PCEHR System and manage their access controls.
- (b) The Call Centre is available to both consumers and healthcare providers and in the first release, will be able to support:
 - (i) general enquires about the PCEHR System;
 - (ii) assistance around the registration process;
 - (iii) assistance in managing basic access controls;
 - (iv) assistance in resolving issues around the PCEHR System;
 - (v) resolution of complaints; and
 - (vi) feedback around the PCEHR System.⁷²
- (c) We understand that further functions may be added in time.
- (d) When contacting the Call Centre, consumers and their representatives will be required to authenticate themselves by providing sufficient identifying information to help the operator locate the consumer's PCEHR, and by answering a series of questions they have set at registration.⁷³
- (e) As nominated representatives have 'read only' access to the consumer's PCEHR, it could be possible for the nominated representative to contact the Call Centre and pretend to be the consumer. In doing so, a nominated representative could then make changes to the consumer's PCEHR when they otherwise would not have that access.

⁷⁰ Con Ops, section 5.4.2 (Authentication to the Consumer Portal and Conformant Portals)

⁷¹ Con Ops, section 3.2.5 (Non-computer access)

⁷² Con Ops section 6.3.5 (Call Centre)

⁷³ Con Ops, section 5.4.2 (Authentication via Call Centre)

- (f) We understand that the Call Centre will primarily address enquiries of an administrative nature. If a consumer's enquiry is clinical in nature or the consumer wants to amend a record, it would be more appropriate for the consumer to contact the relevant clinician.⁷⁴
- (g) Consumers accessing the PCEHR System will be able to make use of the Australian Government Translating and Interpreting Service (**TIS**) when accessing the Call Centre about registering for a PCEHR and managing their PCEHR. The PCEHR System will have the ability to record whether a consumer requires an interpreter and whether languages other than English are spoken at home.⁷⁵
- (h) The System Operator will provide information packs in a range of languages other than English. We understand that the Change and Adoption Partner is currently exploring ways to present the terms and conditions for registration to consumers.
- (i) We also understand that the operational details for the Call Centre are under development.

5.1.5 Consumer access: face to face channel

- (a) DHS in collaboration with the Department will support services through Medicare shop fronts including enquiries, assisted registration and a point of contact around requests and complaints.
- (b) We assume that existing authentication procedures would be used to ensure that the consumer presenting before the DHS employee at the counter, is the consumer who they claim to be - ie presentation of some evidence of identity. We understand that where existing authentication procedures are not in place, PCEHR specific measures are under development.
- (c) Consumers may be able to access their PCEHR via computers at a number of Medicare shopfronts. If computers are placed in a Medicare shop front, consumers may be subject to additional privacy exposures that are not present in other channels. Shop fronts are public open spaces and other members of the community could view a consumer's PCEHR if they were in close vicinity to the computer.

5.1.6 Consumer access: mail channel

- (a) We also understand that consumers will be able to access their PCEHR via a mail request,. At the time of Phase One and Phase Two, detailed information about this process was not available.⁷⁶
- (b) We note that issues of data quality and data security should be further reviewed when the operational details are clearer. For example, if a person wants access by mail, the consumer would have to supply an address and not leave this data field blank. Further consideration of data quality issues may also be needed if the address supplied does not match the consumer's recorded address held by Medicare.

5.1.7 Privacy positives

- (a) The development and uptake of the PCEHR will dramatically improve the ability of consumers to access their own health information in a timely and accessible way. The increased transparency to consumers of both their health information, and information about who has been accessing their health information, is a major privacy positive for the PCEHR proposal.

⁷⁴ Minutes from meeting with Department dated 29 August 2011

⁷⁵ Con Ops, section 3.2.5 (Support for languages other than English)

⁷⁶ Email from the Department dated 12 September 2011

5.1.8 Privacy risks – Consumer-Entered information

- (a) Consumers will be able to enter some information about themselves into their PCEHR, including their home address, emergency contacts, private 'notes', and a structured Consumer-Entered Health Summary.
- (b) As noted above, for some consumers the display of their home address may be cause for concern. It should not be necessary for the PCEHR System to display this information for all consumers. We suggest that consumers have the option of leaving this field blank, or entering alternative contact details, such as a postal address.
- (c) Allowing consumers to enter personal information of other people, such as their emergency contacts, poses the risk that the PCEHR System, and users of the system, will be collecting personal information indirectly, in breach of NPP 1.4 and equivalent provisions.
- (d) In the situation where a consumer and a clinician disagree about the accuracy of information stored in or indexed through the PCEHR, NPP 6.6 requires the holder of that information to allow the consumer 'to associate with the information a statement claiming that the information is not accurate, complete or up-to-date'. In the event that the consumer has been unable to have the authoring clinician or body to attach their statement to a revised version of the record in question, the Consumer-Entered Health Summary may provide an alternative mechanism for a consumer to exercise their privacy right of correction.
- (e) We understand that the current design proposes that the consumer remove disputed records from the PCEHR System, rather than have a statement attached. However, the consumer may wish to keep a record as part of their PCEHR because they recognise its clinical importance, but seek to dispute or clarify one aspect of it for future readers.
- (f) As with any web based system, incorrect entry of password details may occur and there is latent risk of hacking. The design of the system should require usual 'anti-hacking' measures. We note that websites including Australia.gov.au and www.staysmartonline.gov.au already have helpful guidance and tips to consumers.

5.1.9 Recommendations – Consumer-Entered information

- | |
|---|
| <ul style="list-style-type: none">5.1 That the design of the PCEHR System allow the consumer's 'home address' field to be left blank, or accept postal box addresses.5.2 That consumer communications advise consumers of their choices regarding the address entered in their PCEHR, but also warn them that their home address might be contained in records indexed through the PCEHR.5.3 That the design of the PCEHR System remind a consumer, at the point of data entry about their emergency contacts, that all other users including authorised representatives and nominated representatives will see that data; that the PCEHR System provide a notice to consumers, recommending that consumers take reasonable and practical steps to obtain consent from those other people, where appropriate.5.4 That a privacy notice be visible when a consumer seeks to enter data in their private 'Notes' area, explaining the circumstances (if any) in which third parties could gain access to that information.5.5 That the design of the PCEHR System include a mechanism by which a consumer can exercise their privacy right of correction, by associating a statement with an indexed record, such as through the Consumer-Entered Health Summary. |
|---|

- 5.6 That the design provide for appropriate anti-hacking measures such as a maximum number of attempts before the PCEHR System 'locks out' the consumer and that mechanisms are in place for consumers to then reset their password or be re-directed to an assisted channel (eg face to face or telephone).
- 5.7 That consumers are given advice on the suitability of questions and answers, eg the answer should only be known by the consumer and the answer remains true over time.
- 5.8 That special authentication mechanisms are put in place for consumers with a nominated representative (to allow Call Centre employees to distinguish between the consumer and a nominated representative). To mitigate this, the importance of 'secret questions and answers' set at registration by the consumer must be clearly communicated to consumers ie do not record the answers in your PCEHR.

5.1.10 Phase Two Annotations to Recommendations – Consumer-Entered information

- (a) The Victorian Health Services Commissioner in her submission regarding the Bill recommended that a consumer's right to correct health information in the PCEHR should be reflected in the Bill itself rather than the PCEHR Rules and that a process be articulated concerning the rectification of errors.⁷⁷ We would envisage that this right of correction would sit within the PCEHR Rules as proposed in Chapter 8.
- (b) In its submissions to the Bill, the Australian Privacy Foundation noted that the Bill excludes any discussion of access to the PCEHR System from new and emerging technologies, such as cloud computing, smart phones and tablets. The Australian Privacy Foundation says that these new and emerging technologies pose privacy and security risks to a consumer's personal information. To mitigate the risk to privacy, the Australian Privacy Foundation recommended that:

*'the legislation must specify guidelines or standards to enable the application of new and emerging technology to the PCEHR System.'*⁷⁸

- (c) We note that the scope of the proposed PCEHR Rules are broad enough to deal with emerging technologies: s 97 (2) and s 97 (3).
- (d) The privacy risks that may arise with emerging technologies may vary between technologies and the manner in which they may be used to access the PCEHR System. It is appropriate for a privacy impact analysis to be undertaken as the details of those technologies and applications become known.

5.1.11 Privacy Risks - Collection of personal information by registered portal operators

- (a) It is intended that consumers will have a choice of 'portal' through which they access their PCEHR online. Portal providers may offer other 'value add' services.
- (b) There is a risk that consumers do not understand the difference between the PCEHR and other services offered through their portal provider. There is also a risk that registered portal operators could collect health information beyond what is necessary for their functions, in contravention of NPP 1.1.

⁷⁷ Submission by Health Services Commissioner of Victoria 28 October 2011

⁷⁸ Submission to the exposure draft PCEHR Bill 2011 from the Australian Privacy Foundation, submitted 27 October 2011, page 2

- (c) We understand that registered portal operators may have legitimate reasons to have access to the information passing through the portal, particularly where they provide services for disabled consumers. An example might be a consumer portal for people with visual impairments, which provides a read aloud service for consumers. While technical requirements for protecting the security of information in transit and in storage will be addressed in conformance requirements, appropriate access to data may not be able to be meaningfully managed in this way. Instead, this may be more usefully managed through clear boundaries around appropriate uses and disclosures, and enforcement of these.
- (d) In any event, consumers should be notified of the purposes of collection, access and storage of their personal information by registered portal operators, if the design proposes that this occur. To mitigate this risk we note that consumers could instead choose to access the PCEHR System via the PCEHR specific URL rather than a registered portal operator.

5.1.12 Recommendations - Collection of personal information by registered portal operators

- 5.9 That the PCEHR Bill prohibit registered portal operators from recording a consumer's IHI.
- 5.10 That the design of the PCEHR System include a 'PCEHR-specific' portal, such that consumers need not expose their personal information to any other organisation in order to gain access to their PCEHR online.

5.1.13 Privacy Risks - Access to personal information by call centre

- (a) It has not yet been determined the extent to which staff of the System Operator's Call Centre will be able to 'view' data held in a consumer's PCEHR.

5.1.14 Recommendation - Access to personal information by Call Centre staff

- 5.11 That regulations under the PCEHR Bill set controls over the System Operator's Call Centre including requirements for staff security screening the monitoring of calls and how much of a consumer's data can be 'viewed' in what circumstances.

5.1.15 Privacy Risks - Access to personal information by authorised representatives

- (a) There is a risk that authorised representative/s of adult consumers will, through their access to the PCEHR, gain information they normally would not be able to, such as health information about the consumer unrelated to a current decision about their healthcare. For example, the Australian Privacy Commissioner has warned that 'it is particularly important to ensure that only the information necessary for treatment, care or compassionate reasons is disclosed to the 'responsible' person'.⁷⁹
- (b) Allowing an authorised representative to access all the consumer's health information creates a risk of unauthorised disclosure of the consumer's health information, contrary to NPP 2.1.
- (c) There may also be disagreement between authorised representatives as to who should be the nominated healthcare provider for the consumer, or disagreements about the contents of a shared health summary. These problems will be exacerbated in situations where family members are estranged. We suggest that the System Operator will need a protocol

⁷⁹ See OAIC Information Sheet 24 - 2008: 'Disclosure of health information and impaired capacity', at www.privacy.gov.au

for dealing with complaints by or about 'competing' authorised representatives, and that legislation provide a framework for the System Operator to manage such complaints.

5.1.16 Recommendations - Access to personal information by authorised representatives

- 5.12 That the design of the 'authorised representative' component of the PCEHR System be reconsidered, with a view to limiting the access of authorised representatives of adult consumers (and authorised representatives of children in some circumstances) to only viewing the shared health summary and Consumer-Entered Health Summary, rather than all records.
- 5.13 That the PCEHR Bill establish the eligibility rules for authorised representatives of both child and adult consumers, as well as providing the System Operator with the ability to limit, suspend or revoke access rights of authorised representatives in accordance with an established protocol.
- 5.14 That the System Operator develop a protocol for dealing with complaints by or about 'competing' authorised representatives, including the circumstances in which the System Operator may limit, suspend or revoke access rights of authorised representatives, such as on presentation of evidence such as an apprehended violence order.
- 5.15 That the design of the 'authorised representative' component of the PCEHR System include technological design and procedural protocols to ensure regular reviews (such as every three years) of the continued validity of instruments asserting the eligibility of authorised representatives of adult consumers with intermittent or fluctuating capacity.

5.1.17 Privacy Risks - Consumers with intermittent capacity

- (a) The PCEHR System will leverage existing Commonwealth, State and Territory legislative frameworks 'so that a person who is authorised by the law of any jurisdiction to act on behalf of a consumer for healthcare purposes will be recognised by the PCEHR System as an authorised representative'⁸⁰. There are a number of potential issues arising from the proposed manner of involving authorised representatives. We raise these as issues for further consideration by the Department and NEHTA in developing the PCEHR System.
- (b) Firstly, the law in relation to substitute decision making for healthcare decisions in Australia is complex and there are inconsistencies between the laws of the various jurisdictions which relate to terminology, requirements for the appointment of authorised representatives, and the obligations and powers of authorised representatives.
- (c) Secondly, in the case of healthcare decisions, the legislation in Queensland, New South Wales, Tasmania, Victoria, Western Australia and South Australia makes provision for the identification of a person to make decisions on a consumer's behalf where that person lacks capacity and there is no formal enduring instrument in place. In most of those jurisdictions, the authorised representative is determined in accordance with a hierarchy set out in the legislation, which commences with the consumer's spouse. Consequently, in a significant number of cases the proper decision maker for healthcare decisions will not have documentary evidence of their appointment. Further, it is possible that there will be multiple authorised representatives identified by operation of the relevant hierarchy.
- (d) Finally, the authority of an authorised representative to act on behalf of a consumer operates only when the consumer lacks capacity. In the healthcare setting, capacity of a

⁸⁰ Con Ops, section 3.2.8 (Representatives)

consumer may alter over time and therefore so too will the authority of the authorised representative.

- (e) Therefore, there is a risk that the provision of access to an authorised representative of an adult consumer, during periods when the consumer actually has capacity, will be in breach of the disclosure principles.
- (f) Even when a consumer has limited capacity, best privacy practice is to enable as much participation as possible by people with decision-making disabilities.⁸¹ However, we note by contrast the approach in the ACT is to deny consumers the right to exercise their privacy rights themselves if they are exercisable by their guardian (see s 26 of the *Health Records (Privacy and Access) Act 1997 (ACT)*).

5.1.18 Phase Two Annotation to recommendation 5.14 (Disputes between 'competing' authorised representatives)

- (a) In its submissions to the Bill dated 26 October 2011, SA Health submitted that the complaints process needs to address:
 - (i) disputes between authorised representatives and the individual concerned over the capacity of the individual to manage their own PCEHR;
 - (ii) disputes between two authorised representatives over the registration and management of a consumer for whom they are responsible in the PCEHR System; and
 - (iii) disputes between the parents or guardians of a minor over the registration and management of the minor in the PCEHR System.⁸²
- (b) Recommendation 5.14 relates to the System Operator developing protocols for dealing with complaints from competing authorised representatives, including when the System Operator may limit, suspend or revoke access rights of authorised representatives. Such protocols should cover all of the situations referred to by SA Health above.

5.1.19 Recommendation - Consumers with intermittent capacity

5.16 That the design of the 'authorised representative' component of the PCEHR System be reconsidered to allow some mechanism for adult consumers who have one or more authorised representatives to exercise their privacy rights (such as setting access controls or removing records) while in a state of capacity. This mechanism would need to be time critical for example when in the presence of a healthcare provider who can make a judgment about their capacity at that immediate time.

5.1.20 Phase Two Annotation – Recommendation 5.16

- (a) The Victorian Health Services Commissioner in his submission regarding the Bill recommended that administrators fall within the definition of 'authorised representatives' in the Bill.⁸³ We note that section 6 of the Bill defines 'authorised representative' to include a person whom the System Operator is satisfied is authorised to act on behalf of the consumer under the law of the Commonwealth, a State or Territory...⁸⁴ An

⁸¹ See Privacy NSW, Best Practice Guide: *Privacy and People with Decision-Making Disabilities*, 2004, at www.ipc.nsw.gov.au, and OAIC, *Information Sheet 24 - 2008: Disclosure of health information and impaired capacity*, at www.privacy.gov.au

⁸² Submission to the Bill from SA Health dated 26 October 2011, page 7

⁸³ Submission by Health services Commissioner of Victoria 28 October 2011

⁸⁴ Sub sections 6((2)(a), (4)(a)

administrator appointed by the Administrative Tribunal in accordance with applicable State law would seem to fall within that definition.

5.1.21 Annotation to recommendation 5.16 (Consumers with intermittent capacity)

- (a) In its submission to the Bill dated 26 October 2011, SA Health submitted that subsections 6 (6) and (7) (Definition of authorised representative of a consumer) of the Bill do not provide sufficient guidance for the System Operator to determine the authority of an authorised representative of a consumer with intermittent capacity. SA Health also noted similar types of privacy risks arising.⁸⁵ The scope of the PCEHR Rules appear to be broad enough to cover this issue.

5.2 Healthcare provider access

5.2.1 Healthcare provider entry point: Provider Portal

- (a) Healthcare providers wishing to use the Provider Portal to access the PCEHR System will need to be linked to the healthcare organisation within the HI Provider Directory Service (HI-PDS) and will need to use a NASH token (eg smart card or USB token) asserting their identity to log in.
- (b) If the healthcare provider is linked to multiple healthcare organisations, they will be required as part of the login process to select which organisation they are accessing the PCEHR System on behalf of.
- (c) The Organisation Maintenance Officer (**OMO**) will be responsible for maintaining the links between the organisation and the healthcare provider and for removing the links when the healthcare provider leaves the organisation.⁸⁶
- (d) From within the Provider Portal, healthcare providers will be able to (subject to a consumer's access settings):
 - (i) access general information about the PCEHR System in a healthcare provider-oriented form;
 - (ii) login to the Provider Portal using their healthcare provider NASH token containing their digital credentials;
 - (iii) select which organisation they are accessing on behalf of (if the healthcare is linked to multiple healthcare organisations in the HI Provider Directory Service); and
 - (iv) access a PCEHR, including:
 - (A) find a PCEHR;
 - (B) add the healthcare organisation to the Access List (PACC may be required);
 - (C) access PCEHR views;
 - (D) search a PCEHR;
 - (E) download and/or print records;
 - (F) search the NHSPD;

⁸⁵ Submission to the Bill from SA Health dated 26 October 2011, page 4

⁸⁶ Con Ops, section 5.4.1 (Authorised users)

- (G) access online help; and
 - (H) contact the System Operator and request support.
- (e) This list is not exhaustive and consultation will be required to refine it.⁸⁷

5.2.2 Healthcare provider entry point: clinical systems

- (a) The PCEHR System will be accessible from a range of clinical systems, including GP systems, pharmacy systems, hospital systems, aged care systems, specialist systems, etc. How the clinical system is integrated with the PCEHR System will vary from system to system.
- (b) It is intended that these systems will leverage a range of e-health foundation measures, including:
 - (i) HI Service;
 - (ii) NASH;
 - (iii) Secure Messaging; and
 - (iv) Clinical Terminology.
- (c) These systems will be able to access a PCEHR (subject to a consumer's access settings):
 - (i) find a PCEHR;
 - (ii) add the organisation to the Access List (PACC may be required);
 - (iii) obtain emergency access;
 - (iv) access PCEHR views;
 - (v) search a PCEHR;
 - (vi) download and/or print records and views;
 - (vii) upload records into the PCEHR System;
 - (viii) access online help about the PCEHR System; and
 - (ix) contact the System Operator and request support.
- (d) This list is not exhaustive and consultation will be required to refine it.⁸⁸

5.2.3 Healthcare provider entry point: Contracted Service Providers

- (a) The PCEHR System will be accessible from a range of third party contracted service providers who offer health software as a service (**SaaS**) and support access to the PCEHR System on behalf of a healthcare organisation.
- (b) It is intended that these systems will leverage a range of e-health foundation measures, including:
 - (i) HI Service;
 - (ii) NASH;
 - (iii) Secure Messaging; and
 - (iv) Clinical Terminology.

⁸⁷ Con Ops, section 6.3.2 (Provider Portal)

⁸⁸ Con Ops, section 6.2.2 (Clinical systems)

- (c) It is intended that these systems will be able to access a PCEHR (subject to a consumer's access settings):
 - (i) find a PCEHR;
 - (ii) add the organisation to the Access List (PACC may be required);
 - (iii) obtain emergency access;
 - (iv) access PCEHR views;
 - (v) search a PCEHR;
 - (vi) download and/or print records and views;
 - (vii) upload records into the PCEHR System;.
 - (viii) access online help about the PCEHR System; and
 - (ix) contact the System Operator and request support.
- (d) This list is not exhaustive and consultation will be required to refine it.⁸⁹

5.3 Healthcare provider access: download

5.3.1 Access required to find a PCEHR

- (a) The 'key' to finding a consumer's PCEHR is their IHI. We understand that a healthcare provider (including 'other authorised users' who work in a registered healthcare provider organisation) can search for an IHI from the HI Service using the following minimum set of data about a consumer:
 - (i) family name;
 - (ii) given name;
 - (iii) gender;
 - (iv) date of birth; and
 - (v) Medicare card number, DVA file number or full address.
- (b) We understand that a decision was taken in relation to the design of the HI Service, that a consumer's Medicare card or DVA file number would not be a mandatory field for entering the parameters of a search for an IHI, if a full address was provided instead. That design decision was taken to ensure that consumers who presented for healthcare without their Medicare or DVA details were able to obtain the benefits of an IHI and, by extension, their PCEHR.
- (c) This caters for emergency scenarios, such as if the consumer is unconscious but a person accompanying them knows their details, or they have other information on them, such as a driver's licence, which provides that information. It also caters for consumers who do not carry their Medicare card with them at all times.

5.3.2 Access required to download

- (a) A healthcare provider can download a record anytime, provided they have access to the consumer's PCEHR and the relevant record.⁹⁰

⁸⁹ Con Ops, section 6.2.3 (Contracted Service Providers)

- (b) We understand that if a healthcare provider is connected to the PCEHR System, the creation of a new record causes a message to be sent to the System Operator, asking if the consumer has a PCEHR. The message would include:
 - (i) the consumer's IHI;
 - (ii) the healthcare provider's HPI-O; and
 - (iii) the healthcare practitioner's HPI-I.⁹¹
- (c) Once the System Operator receives this message, the System Operator would proceed to verify the right of the healthcare provider to access the PCEHR System, and determine whether the consumer has a PCEHR. The System Operator then advises the healthcare provider whether the consumer has a PCEHR.
- (d) If the consumer has a PCEHR, it may be set to allow automatic access, or to restrict access using a PACC. A consumer uses a PACC by adjusting the advanced control settings. Where a PCEHR has a PACC, a healthcare provider may only access the consumer's PCEHR if the consumer discloses the PACC to the healthcare provider.⁹²
- (e) If the consumer has a PACC, the healthcare provider would either:
 - (i) request the PACC from the consumer; or
 - (ii) the consumer gives the PACC to the healthcare provider.
- (f) After the healthcare provider has the PACC, the healthcare provider requests access to the PCEHR System, entering the PACC where required. If the consumer does not have a PACC, the healthcare provider can enter the PCEHR System without the need to enter a PACC.⁹³
- (g) The System Operator would then identify the consumer's relevant records by using the index service.

5.3.3 Indexing services

- (a) The index associates a consumer with a range of his/her records already stored within the PCEHR registered repository operators.
- (b) The index stores metadata (ie data that serves to provide contextual information about other data) about each record; the actual content of the records are stored within the registered repository operator.
- (c) Key functions of the index service include the ability to:
 - (i) register a new record;
 - (ii) update an existing record index entry;
 - (iii) deregister a record;
 - (iv) search the index; and

⁹⁰ Information flow diagram received from the Department, 8 August 2011 (Download of documents from the PCEHR System – documents held by the NRS and other Conformant Repository Operators, Steps 1 and 2)

⁹¹ Information flow diagram received from the Department, 8 August 2011 (Download of documents from the PCEHR System – documents held by the NRS and other Conformant Repository Operators, Step 3)

⁹² Information flow diagram received from the Department, 8 August 2011 (Download of documents from the PCEHR System – documents held by the NRS and other Conformant Repository Operators, Step 6)

⁹³ Information flow diagram received from the Department, 8 August 2011 (Download of documents from the PCEHR System – documents held by the NRS and other Conformant Repository Operators, Step 7)

- (v) execute quality functions to assess the integrity of the data.
- (d) In order to support this functionality, for each registered record, the index service stores:
 - (i) the consumer's IHI;
 - (ii) the record ID (a unique identifier for the information);
 - (iii) the template ID;
 - (iv) the type of record (eg Discharge Summary, Event Summary);
 - (v) a keyword list for search function;
 - (vi) the location where the record can be retrieved;
 - (vii) the date and time at which when the record was created;
 - (viii) the name, speciality / sub speciality and HPI-I of the healthcare provider that created the record;
 - (ix) the name and HPI-O of the healthcare organisation where the record was created;
 - (x) the name and HPI-O of the participating healthcare organisation that created the record;
 - (xi) versioning information about the record;
 - (xii) management information about the integrity of the link (eg last time the link was checked, flag to indicate potential duplicate, etc.);
 - (xiii) a label indicating if the information is 'general access' or 'limited access';
 - (xiv) a flag indicating the record had to be 'effectively removed' and a reason why it was removed (eg request by consumer, posted in wrong PCEHR) and the date/time of removal; and
 - (xv) an annotation indicating if the record has been archived or disposed of in the registered repository operator.⁹⁴

5.3.4 Indexing service: to locate and search record

- (a) In order to help users find records within a PCEHR more readily, the PCEHR System provides two search functions: basic search and advanced search.
 - (i) Basic search
 - (A) The basic search function allows users to find records within a consumer's PCEHR based on matching keywords. Users will, for example, be able to find all records that contain the term 'kidney' within the body of the record.
 - (B) The basic search is limited and will only support simple matching methods. In time, as the number of records within each PCEHR increases and demand for this function increases, more sophisticated matching techniques will be investigated.
 - (ii) Advanced search
 - (A) The advanced search function allows the user to search a consumer's PCEHR for records via a number of parameters, including:

⁹⁴ Con Ops, section 6.4.3 (Index Service)

- (I) keywords;
 - (II) date uploaded;
 - (III) type(s) of record;
 - (IV) provider organisation; and
 - (V) healthcare provider speciality/sub-speciality.⁹⁵
- (b) The advanced search function is limited in its search capabilities. In time, as the number of records within each PCEHR increases and demand for this function increases, more search parameters will become available.⁹⁶
- (c) It will be important for the design to ensure that, where a consumer has 'hidden' a record, those records do not appear in a search result. Where a record is hidden, the search result should return a result of 'no records found'. The disclosure that a record relating to a particular keyword eg 'pregnant' may in itself disclose health information and be of interest to the reader viewing the search result. We understand from our discussions with NEHTA that the design would not allow hidden records to be revealed in any search result.⁹⁷

5.3.5 Downloading a record from a National Repository or registered repository operator

- (a) After the index service is used, the System Operator requests the relevant record from either a National Repository or registered repository operator. The record is identified by the unique number allocated to each record.
- (b) Once the unique number is provided to either the National Repository or registered repository operator, the repository would disclose the record to the System Operator. The System Operator then sends the record to the healthcare provider, consistent with the level of access available to that healthcare provider (as chosen by the consumer).⁹⁸

5.4 Healthcare provider access: viewing a downloaded record

5.4.1 Index and viewing services

- (a) After the index service is used, the System Operator requests the relevant record from either a National Repository or registered repository operator. The record is identified by the unique number allocated to each record.
- (b) By default, the Index View will be sorted in reverse chronological order, with the most recent records first. The user will be able to sort the view by some of the fields (eg date, type, clinical setting, role of the author, name of the author, etc.).
- (c) The user will be able to filter the view by some of the fields (eg by date range and record type / subtype). By default, the Index View will have no filters set. Additional settings in the index view will allow the user to search for recently amended and/or changed records.⁹⁹

⁹⁵ Information around specialities/sub-specialities to be provided in accordance with HI Service Provider classifications

⁹⁶ Con Ops, section 4.5 (Search)

⁹⁷ Notes from meeting with NEHTA and the Department dated 15 August 2011

⁹⁸ Information flow diagram received from the Department, 8 August 2011 (Download of documents from the PCEHR System – documents held by the NRS and other Conformant Repository Operators, Steps 9 to 11)

⁹⁹ Con Ops, section 4.4.1 (Index View)

- (d) The View Service allows authorised users, consumers and their representatives to access a series of ‘views’ of a consumer’s PCEHR. These views are intended to allow the underlying information within a PCEHR to be reassembled in different ways for different categories of users with different needs:
 - (i) Request View;
 - (ii) Update View Content; and
 - (iii) Execute quality functions to assess the integrity of the data.
- (e) In some cases the View Service will assemble views using information from the index or other services. For some kinds of views, such as the Index View, this approach is appropriate as such information can be readily requested from the index service. However, for other kinds of views, such as the Consolidated View, which have greater performance demands, it may be necessary to update the view as new information is added to the PCEHR System. It is likely that the View Service will need to maintain an atomic data store specifically for this purpose.¹⁰⁰

5.4.2 Viewing the Consolidated View

- (a) The Consolidated View is intended to provide an up-to-date picture of the consumer’s health status with information drawn from their shared health summary and additional information drawn from other more recent records.
- (b) Information in the Consolidated View is grouped into categories such as Allergies and Adverse Reactions, Medicines, Medical History and Immunisations and it also provides a means of navigation into the full suite of records available in the consumer’s PCEHR.
- (c) Users of the Consolidated View will be able to select a piece of information, identify where it came from and open the record from which it was sourced. The Consolidated View may be incomplete, as information may not be extracted from unstructured records, and will include a notice to this effect. The view will include a list of unstructured records that may contain additional information since the shared health summary was last updated.
- (d) For users of a registered portal operator, the Consolidated View will also include a series of links to related health literacy material. Users of the Consolidated View will be able to follow links from allergies and adverse events, medicines, medical history and immunisations named in the Consolidated View to a search on healthinsite.gov.au. This in turn will allow consumers to access related health literacy resources and consumer medication information sheets (where available).¹⁰¹
- (e) Within views such as the Consolidated View and Index View, healthcare organisations with general access will not be able to see that ‘Limited Access’ records exist. For healthcare organisations with access to ‘limited access’ records, these views will show the presence of these records as well as any extracted information in the case of the Consolidated View.
- (f) Authorised users with access to ‘limited access’ records will be required to exercise increased caution regarding sharing of this information, if not clinically relevant. They may also prompt a conversation with the consumer regarding any clinical risks associated with the status of the record.¹⁰²

¹⁰⁰ Con Ops, section 6.4.5 (View Service)

¹⁰¹ Con Ops, section 4.4.2 (Consolidated View)

¹⁰² Con Ops, section 5.5.3 (Advanced access controls)

- (g) We understand that illustrative examples of how the Consolidated View would appear to a healthcare provider are under development by NEHTA. We suggest further review of the Consolidated View when operational and design details are clearer.
- (h) We also assume that illustrative examples of how the Consolidated View would appear to a consumer are under development by NEHTA. We suggest further review of the Consolidated View when operational and design details are clearer.

5.5 Healthcare provider access: restrictions on viewing

5.5.1 Advanced access controls for consumers

- (a) In Chapter 4, we discussed how consumers can adjust a series of advanced access control settings. The advanced access control settings will include all basic access control settings as well as some additional access controls. Some advanced access controls are only available after registration, or at the time of uploading or downloading.
- (b) Additional options available under advanced settings include:
 - (i) setting up a PACC;
 - (ii) setting up a PACCX for access to a record within a PCEHR;
 - (iii) restricting organisations from being on the Access List;
 - (iv) an ability to prevent a PCEHR from being found; and
 - (v) managing record level access.¹⁰³

5.5.2 Advanced consumer control: restricting organisations

- (a) Consumers will be able to mark organisations on their Access List as being 'revoked'. If an organisation is marked as being 'revoked', then they will not be able to access the consumer's PCEHR, unless the consumer either provides them with a PACC or they use emergency access.
- (b) We understand that a consumer would be unable to mark an organisation as being 'revoked' unless the organisation is already on the consumer's Access List. Where a consumer has specific privacy concerns relating to a particular organisation, the consumer would not be able to revoke access until the organisation appeared on the consumer's Access List.
- (c) The other option is for the consumer to change the organisations access level via the registered portal operator. A consumer does not need to set up a PACC to use this feature.¹⁰⁴

5.5.3 Advanced consumer control: hiding PCEHR visibility

- (a) Consumers will be able to select if they want their PCEHR to be 'findable' or not. A consumer is unable to set this option at the time of registration but may do so afterwards.¹⁰⁵ If the consumer chooses this option, then when a consumer arrives at a new healthcare organisation not currently on their Access List, any search for their PCEHR will return 'not found'. Similarly, if the organisation is marked as 'revoked' on the Access List then it will not be able to find the consumer's PCEHR.
- (b) By default, a PCEHR will be findable, unless the consumer changes this advanced setting.

¹⁰³ Con Ops, section 5.5.3 (Advanced access controls)

¹⁰⁴ Con Ops, section 5.5.3 (Advanced access controls)

¹⁰⁵ Email from the Department dated 12 September 2011

- (c) A PCEHR can still be found with emergency access if the consumer has selected this option.
- (d) A consumer does not need to set up a PACC to use this feature.¹⁰⁶

5.5.4 Advanced consumer control: adjusting access at time of upload

- (a) If the consumer chooses to set up a PACC, they will also be given the option of controlling access to records. Under this option, the consumer will be able to set an access control level on each record in their PCEHR and be able to select what level of access each organisation on their Access List is afforded (either 'general access' or 'limited access').
- (b) The levels available are summarised below.¹⁰⁷

Option	Description	Possible consequences
'general access'	The record will be accessible by any healthcare organisation that has access to the consumer's PCEHR.	The record will be available when needed for a consumer's care by any healthcare organisation that currently has permission to access the consumer's PCEHR.
'limited access'	<p>The record will be accessible via the consumer's PCEHR to a more limited group of healthcare organisations selected by the consumer.</p> <p>The record is still accessible to the healthcare organisation that supplied it and in an emergency situation.</p> <p>shared health summaries and Consumer-Entered Health Summaries cannot have 'limited access' option applied to them.</p> <p>nominated representatives may be granted access 'limited access' information by the consumer or authorised representative.</p>	<p>The consumer has opted for more control over the healthcare organisations that can access these records, allowing them to decide the level of access based on the kind of care they are seeking.</p> <p>The consumer will take the responsibility that this information may be important to ensuring that consumer receives the right care. Where the healthcare provider does not know this information, it may mean that the consumer is given inadequate or inappropriate care.</p>

- (c) The application of access levels to records is managed by the consumer within the registered portal operator. Healthcare providers do not need to select the level of access to be applied to a record when it is uploaded.
- (d) The default access level for a record when posted to a PCEHR will be same as the level of access granted to the healthcare organisation by the consumer. For example, if a healthcare organisation with General Access has uploaded a record, then it will be marked as 'General Access'.

¹⁰⁶ Con Ops, section 5.5.3 (Advanced access controls)

¹⁰⁷ Con Ops, section 5.5.3 (Advanced access controls)

- (e) If a healthcare organisation with Limited Access has uploaded a record, then it will be marked as 'Limited Access'. For the avoidance of doubt, if a healthcare organisation does not presently have access, and they upload a record to the PCEHR (eg after using emergency access), the record will be marked as 'general access'.
- (f) In some cases a consumer may be seeing a healthcare provider for two different healthcare issues, one that needs to be managed at a 'general access' level and one that is managed at a 'limited access' level. In this case, the onus is on the consumer to use the registered portal operator to adjust the access level of the record accordingly.¹⁰⁸

5.5.5 Healthcare provider access: emergencies

- (a) The PCEHR System provides the option of emergency access for use in situations where the consumer is in need of emergency care and is not capable of giving or communicating consent.
- (b) Healthcare organisations could also have emergency access to a consumer's PCEHR, irrespective of whether that consumer is the consumer undergoing medical treatment. Provided that there is a serious and imminent threat to the life of a person, a consumer's PCEHR could be accessed for emergency purposes. To illustrate by example, a parent's PCEHR could be accessed in order to identify if that parent had a suitable blood type to give their child an emergency blood transfusion.
- (c) Basic access settings:
 - (i) Emergency access is not required for consumers with basic level access controls, as the organisation may simply assert that they are providing healthcare services to the consumer.
- (d) Advanced access settings:
 - (i) Emergency 'override' access is required if the consumer has opted to set up advanced access controls which may prevent access to the consumer's PCEHR in an emergency situation (eg a PACC code has been set, the organisation is 'revoked' in the Access List or the consumer has marked information as 'limited access').
 - (ii) Emergency access will add the healthcare organisation to the consumer's Access List and provide the organisation with access to 'limited access' and 'general access' records. After a period of five days from the time of last access to the consumer's PCEHR, the organisations access level will revert back to the previous access level prior to emergency access.
 - (iii) If the time-out occurs and access is still required, the healthcare organisation could either assert emergency access again or obtain a more persistent form of access from the consumer (or their authorised representative).
 - (iv) Before emergency access can be used the authorised user will be provided with a warning message highlighting that they are about to use emergency access and the emergency access will be logged. The authorised user will be required to indicate that they wish to proceed.
 - (v) A 'revoked' organisation is still able to use emergency access to find and access a consumer's PCEHR. If a healthcare organisation is revoked on the Access List,

¹⁰⁸ Con Ops, section 5.5.3 (Advanced access controls)

then the warning message will also highlight that the consumer prefers the organisation not access their PCEHR.

- (e) Suspended PCEHR:
 - (i) Where a consumer or the System Operator has suspended a PCEHR, emergency access is available.
 - (ii) All use of emergency access will be audit logged.

5.5.6 Privacy risks - Authentication of users

- (a) The current design of the PCEHR System delegates to HPI-Os the task of identifying the users to whom it will give access. These users must be their employees' (broadly defined), and can either be healthcare providers with an HPI-I, or 'other authorised users'.
- (b) Although the proposed definition of 'employee' is defined to include people who offer their services in an unpaid capacity, for the sake of clarity we suggest that the legislation explicitly include students undertaking placements. This would still allow the HPI-O to determine which students should have access, according to the nature of their responsibilities.
 - (i) On the basis of our discussions with the Department, we understand that tertiary healthcare students would be considered as Authorised Users. The Department also considers that tertiary healthcare students would fall within the proposed definition of 'employee' in the PCEHR legislation. Whilst recognising that it is the Department's view that students will fit within the proposed definition of 'employee', we have not had the opportunity to review the PCEHR legislation and would suggest reviewing this issue after the legislation is released.
 - (ii) The PCEHR legislation should also define or include guidance as to what constitutes a '*legitimate need*' for other consumers who do not have a HPI-I within a registered healthcare provider organisation to access the PCEHR System.
- (c) There is little in the Con Ops to suggest that a prescriptive approach will be taken to the verification of a proposed user's identity, or their association with a particular HPI-I. By contrast, consumers are expected to demonstrate 100 points worth of evidence of their identity in order to register for a PCEHR.
- (d) There is a risk that without a robust system for verifying a proposed user's identity (and their associated HPI-I), a user could engage in deliberate misconduct without fear of prosecution. For example, a person might use a fake name to seek employment in an administrative role, simply in order to gain access to one or more specific consumers' PCEHR for some benefit (such as tracking down an ex-partner or debtor, or accessing the records of celebrities to sell information to the media), and then resign before any investigation is triggered.
- (e) Recent cases in NSW and the Northern Territory of people successfully posing as doctors and gaining access to patient files over extended periods of time illustrate the risks of failing to verify identity or role-based claims.¹⁰⁹

¹⁰⁹ See 'Fake doctor jailed after abusing trust of friends' 13 August 2011, at <http://www.smh.com.au/nsw/fake-doctor-jailed-after-abusing-trust-of-friends-20110812-1iqwx.html#ixzz1XAccoUSN>; and 'Fake doctor Balaji Varatharaju treated over 400 patients', 28 February 2010, at <http://www.news.com.au/national/fake-doctor-balaji-varatharaju-treated-over-400-patients/story-e6frfkvr-1225835255318#ixzz1XAci25DW>

5.5.7 Recommendations - Authentication of users

- 5.17 That the PCEHR Bill define 'employee' to explicitly include tertiary healthcare students on placement.
- 5.18 That the PCEHR Bill define or include guidance as to what constitutes a 'legitimate need' for other individuals who do not have a HPI-I within a registered healthcare provider organisation to access the PCEHR System.
- 5.19 That the PCEHR Bill set one of the conformance requirements on an HPI-O as an obligation to verify, with 100 points of EOI, the identity of each proposed user (and confirm their proper association to an HPI-I, where applicable).

5.5.8 Phase Two Annotation to recommendation 5.18 (Authorised uses of the PCEHR System)

- (a) In its submission to the Bill, the Australian Medical Association recommended that:
 - (i) *'Amendments should be made to the draft Bill to explicitly clarify that when HPI-Is and HPI-Os authorised to use the PCEHR System delegate activities to administrative staff or other employees or contractors (ie to obtain access and upload information), these delegated activities are also authorised uses of the PCEHR System. Alternatively, this might be clarified in the explanatory memorandum.'*¹¹⁰
- (b) Recommendation 5.18 of this Report suggested that the Bill should include what constitutes an authorised or 'legitimate need' for employees within a registered healthcare provider organisation to access the PCEHR System. Part 4 of the Bill addresses this recommendation, and sets out which types of collection, use and disclosure of a consumer's health information are *authorised* and *unauthorised*. It is important that this distinction between 'authorised' and 'unauthorised' is maintained otherwise there would be a risk that unauthorised access would arise by authorised individuals.

5.5.9 Privacy Risks - Education of users

- (a) A number of submissions to the Con Ops and Legislation Issues Paper raised the question of how healthcare provider users of the PCEHR System would be educated about their privacy responsibilities. Privacy obligations will mean little in practice if users do not understand their obligations, or how they apply in practice.
- (b) Recommendation 8.3, in Chapter 8, proposes that a set of 'PCEHR privacy rules' be applied to all non-consumer participants in the PCEHR System, such as healthcare provider users. We suggest here that users ought be provided with some training in their obligations to comply with those rules, as a condition of gaining access to the system.

5.5.10 Recommendations - Education of users

- 5.20 That the PCEHR Bill set one of the conformance requirements on an HPI-O as an obligation to provide training to their employees on the appropriate access to and use of PCEHRs including the 'PCEHR privacy rules' and any other privacy obligations applying to that organisation.

¹¹⁰ Submission to the Bill from the Australian Medical Association, page 2

5.21 That the PCEHR Bill ensure that the 'PCEHR privacy rules' must be confirmed as understood and accepted by individual users as a condition of their first access to the PCEHR System.

5.5.11 Privacy Risks - Search Parameters

- (a) A key privacy risk for any database is the ease with which a user can search for personal information about an individual, in circumstances which are unauthorised. In the context of the PCEHR system, the particular risk is that an authorised user could search for and find a consumer's personal information and health information, even though the consumer is not in the process of obtaining healthcare from that user's organisation.
- (b) It needs to be recognised that users are human, subject to human frailties and motivations including curiosity, jealousy and greed. These motivations could tempt some users to search for the PCEHR of consumers who are personally known to them (ex-partners, family members, friends, neighbours, debtors and the like), or consumers who are public figures (celebrities, politicians, professional sportsmen and women, etc). Once accessed, information from a consumer's PCEHR could be misused or disclosed without authority.
- (c) The ease with which a consumer's PCEHR can be found by healthcare providers poses an important question of determining the best balance between accessibility for authorised purposes, and privacy protection against unauthorised purposes.
- (d) To ensure maximum privacy protection, one option would be to recommend a change to the HI Service, to require that a Medicare card or DVA file number be entered by the user as a mandatory field, before they can search for a consumer's IHI. This would have the effect of making misuse of the system much more difficult for users otherwise tempted to look up the IHI and then PCEHR of consumers who are not actively seeking healthcare from the user's organisation. However it would also have the effect of denying the benefits of the IHI and PCEHR to consumers who present (conscious or not) for healthcare, without their Medicare or DVA details.
- (e) Instead of making such a recommendation, we suggest a number of other ways here to recognise and mitigate this risk.
- (f) Other recommendations elsewhere in this report also provide ways to further mitigate this risk; see for example recommendations 5.20 and 7.3 in relation to the verification and logging of users' identity, and recommendation 8.2 in relation to criminal offences for the misuse of personal information.

5.5.12 Recommendations - Search Parameters

- 5.22 That consumer communications draw attention to the fact that under the 'Basic' access controls, any authorised user of the system can find their PCEHR so long as the user knows at least the consumer's full name, gender, date of birth, and either their address or their Medicare / DVA number.
- 5.23 That when designing the conformance tests for clinical software seeking to interface with the PCEHR system, the Department and NEHTA give consideration to how a PCEHR can be 'found' in an automated way, with a view to ensuring the clinical software strikes a proper balance between speed of access and surety as to the correct identity of the individual.
- 5.24 That the System Operator use proactive monitoring of the use of exception-based searching for an IHI, to search for possible examples of misuse of the system.

5.25 That the System Operator use proactive monitoring of the audit logs of activity against the PCEHR of public figures, to search for possible examples of misuse of the system.

5.5.13 Privacy Risks - Emergency access

- (a) A number of privacy controls on the PCEHR System are intended to be overridden in 'emergency' situations. The question is how to define such a situation, so as to appropriately balance privacy with competing interests such as personal or public safety.
- (b) In the NPPs, there are two different tests for 'emergency' situations:
 - (i) a *collection* of health information must be 'necessary to prevent or lessen a serious and imminent threat to the life or health of any individual' (NPP 10.1(c)), while
 - (ii) a *use or disclosure* of health information must be 'necessary to lessen or prevent: (i) a serious and imminent threat to an individual's life, health or safety; or (ii) a serious threat to public health or public safety' (NPP 2.1(e)).
- (c) Also, in the NPPs, the *collection* of health information in an 'emergency' situation is only allowed when the subject lacks capacity to give or communicate their consent (NPP 10.1(c)). By contrast, health information may be *used or disclosed* in an 'emergency' situation regardless of the subject's ability to give or withhold their consent (NPP 2.1(e)).
- (d) There were differing views offered in submissions to the LIP as to whether or not the consumer's incapacity to communicate consent should be part of the test for 'emergency access'¹¹¹.
- (e) In our view, the point of an 'emergency override' mechanism is that consent becomes irrelevant, when the circumstances are such that the need to prevent or lessen a serious threat is dictating actions. However the trade-off for allowing users to override, ignore or bypass normal consent protocols should be taking all possible steps to ensure that the circumstances actually reflect an 'emergency need'.
- (f) Case law in NSW indicates that post-hoc justifications for disclosures on the grounds of 'preventing a serious threat' will be treated with considerable scepticism. Judicial tests have been developed to suggest:
 - (i) that there will need to be evidence of sufficient 'gravity of concern' about a threat to health or safety (*Director General, Department of Education and Training v MT (GD)* [2005] NSWADTAP 77 at [75]);
 - (ii) that the threat to health or safety must be 'likely to occur at any moment; impending' (*FM v Vice Chancellor, Macquarie University* [2003] NSWADT 78 at [56]);
 - (iii) that the threat must be acted upon immediately (*NK v Northern Sydney Central Coast Area Health Service* [2010] NSWADT 258); and
 - (iv) that the conduct (of collecting, using or disclosing the information) must be necessary for, and directed towards, actually lessening or preventing the threat from being realised (*MT v Director General, NSW Department of Education & Training* [2004] NSWADT 194).

¹¹¹ See for example the Victorian Health Services Commissioner submission p.3, and the Consumers Health Forum submission p.4

- (g) In each of these cases, the exemption claimed by the respondent agency failed. This suggests that quite specific guidance will be needed for users about the circumstances in which it will be acceptable to trigger the 'emergency override' button in the PCEHR System.

5.5.14 Recommendations - Emergency access

- 5.26 That the PCEHR Bill define the circumstances in which a consumer's access controls and other privacy settings may be overridden as only when the override is 'necessary to prevent or lessen a serious and imminent threat to the life or health of any consumer'.
- 5.27 That the PCEHR System design ensure that access granted via the 'emergency access' override is only temporary.
- 5.28 That users be provided with guidance on the interpretation of the legislative 'emergency access' test, with specific examples developed in consultation with the Australian Privacy Commissioner. This guidance should be clearly available whenever the 'emergency override' button is presented, for example by way of a link or pop-up box.

5.5.15 Privacy Risks - Misuse of the PCEHR

- (a) The risks posed in general by healthcare users inappropriately viewing, using or disclosing personal information or health information stored in or indexed through a consumer's PCEHR - and the possible mitigation of those risks - are dealt with in detail in Chapter 8 of this report.

5.6 Healthcare provider access: upload

5.6.1 Record types

- (a) Initially, the PCEHR System will support the collection of a range of record types, including:
- (i) shared health summaries¹¹²;
 - (ii) Event Summaries¹¹³;
 - (iii) Discharge Summaries¹¹⁴;
 - (iv) Specialist Letters¹¹⁵;
 - (v) Referrals¹¹⁶;
 - (vi) Prescribing and Dispensing information¹¹⁷;
 - (vii) Pathology Result Reports¹¹⁸;
 - (viii) Medicare information including:
 - (A) Medicare claims history (MBS data);
 - (B) PBS data;

¹¹² Con Ops, Section 4.3.1

¹¹³ Con Ops, Section 4.3.2

¹¹⁴ Con Ops, Section 4.3.3

¹¹⁵ Con Ops, Section 4.3.4

¹¹⁶ Con Ops, Section 4.3.5

¹¹⁷ Con Ops, Section 4.3.6

¹¹⁸ Con Ops, Section 4.3.7

- (C) Australian Organ Donor Register; and
 - (D) Australian Childhood Immunisation Register¹¹⁹;
 - (ix) Consumer-Entered Health Summary¹²⁰; and
 - (x) Consumer notes¹²¹.
- (b) Over time, the PCEHR System will support a range of additional record types.¹²²

5.6.2 Upload a record: registered repository operator

- (a) When a consumer seeks healthcare, the healthcare provider would create a record for the consumer in the practitioner's local computer system.¹²³
- (b) We understand that if a healthcare provider is connected to the PCEHR System, the creation of a new record causes a message to be sent from the local system to the System Operator, asking if the consumer has a PCEHR. The message would include:
 - (i) the consumer's IHI;
 - (ii) the healthcare provider's HPI-O; and
 - (iii) the healthcare practitioner's HPI-I.¹²⁴
- (c) Once the System Operator receives this message, the System Operator would proceed to verify the right of the healthcare provider to access the PCEHR System, and determine whether the consumer has a PCEHR. The System Operator then advises the healthcare provider whether the consumer has a PCEHR.¹²⁵
- (d) If the consumer has a PCEHR, the default setting is that the record will be uploaded unless the consumer requests that it is not uploaded.
- (e) Ideally, the healthcare provider should expressly highlight this choice to consumers, where the record could be considered 'sensitive'. When the operational details are clearer, further procedures may need to be considered when handling 'sensitive' information.
- (f) We understand that the consumer would then consent (or not) to uploading the sensitive record.¹²⁶ On a separate but related issue, we note there is existing State/Territory legislation tightly regulating the upload of health information relating to notifiable conditions such as HIV status, irrespective of whether the consumer gives consent.
- (g) If the consumer does not have a PCEHR, we understand that the message would return a response to the healthcare provider notifying them that 'no record was found' (or something similar).
- (h) If the record is not considered sensitive and the consumer consents to the upload, the healthcare provider would then:

¹¹⁹ Con Ops, Section 4.3.8

¹²⁰ Con Ops, Section 4.3.9

¹²¹ Section Con Ops, 4.3.10

¹²² Con Ops, Section 2.8

¹²³ Con Ops, section 4.2 (information model)

¹²⁴ Information flow diagram received from the Department, 8 August 2011 (Upload of documents to the PCEHR System – document to be stored by a repository not part of the National Repositories Service, Step 3)

¹²⁵ Information flow diagram received from the Department, 8 August 2011 (Upload of documents to the PCEHR System – document to be stored by a repository not part of the National Repositories Service, Steps 4 and 5)

¹²⁶ Information flow diagram received from the Department, 8 August 2011 (Upload of documents to the PCEHR System – document to be stored by a repository not part of the National Repositories Service, Steps 6, 6A and 6B)

- (i) save the original of the record in the local system;
 - (ii) upload the record to a registered repository operator; and
 - (iii) label a copy of the record with the relevant IHI, HPI-I and HPI-O.¹²⁷
- (i) We understand that where a consumer uses a pseudonymous IHI, the record would be uploaded to the corresponding pseudonymous PCEHR.
 - (j) When a record is loaded into a registered repository operator, it will be validated against a common set of templates and the registered repository operator will inform the index service that a new record is available.¹²⁸
 - (k) After the registered repository operator receives the record, the registered repository operator would upload a copy of the record and provenance information to the System Operator.
 - (l) We understand that the System Operator would use the copy of the record to create a keyword profile and update the Consolidated View. After this process is complete, the copy of the record is destroyed. The provenance information from the record would be stored as part of the Indexing Service.¹²⁹ We suggest that communications to consumers clearly explain the relationship between a registered repository operator and the PCEHR System, including how a record is associated from the local system to their PCEHR.
 - (m) The provenance information includes:
 - (i) the consumer's IHI;
 - (ii) the consumer's date of birth;
 - (iii) the consumer's sex;
 - (iv) the healthcare provider's HPI-O;
 - (v) organisation name;
 - (vi) organisation address and communication details;
 - (vii) the healthcare practitioner's HPI-I;
 - (viii) name of the author;
 - (ix) healthcare provider speciality/sub-speciality;
 - (x) version number of the record;
 - (xi) unique identifier of any previous version of the record;
 - (xii) record type information (eg Discharge Summary, Event Summary);
 - (xiii) record template used;
 - (xiv) date/time the record was reviewed (or created) by the up-loader; and

¹²⁷ Information flow diagram received from the Department, 8 August 2011 (Upload of documents to the PCEHR System – document to be stored by a repository not part of the National Repositories Service, Step 7) and email from the Department dated 12 September 2011

¹²⁸ Con Ops, section 4.2 (information model)

¹²⁹ Email from the Department dated 12 September 2011

- (xv) unique record identifier (generated by the registered repository operator).¹³⁰
- (n) Any field marked as ‘required’ within a template must be filled in for the record to be valid. If the author does not have information to put into a ‘required’ field, then they will be required to supply a reason. For example, ‘None Known’, ‘Not Asked’ or ‘Not Supplied’ can be used for a ‘required’ field.¹³¹ We understand that if the mandatory fields within a template cannot be completed by the author, the PCEHR System would not accept the upload.¹³²
- (o) After the System Operator receives the record, the System Operator indexes the record and uses information from the record to:
 - (i) create an updated Consolidated View; and
 - (ii) create a key word profile.¹³³
- (p) When another user is ready to find records within a consumer’s PCEHR, they will be able to use their local clinical system (or portal), to obtain authorisation to access a consumer’s PCEHR, search the index and obtain a copy of the relevant records from the pertinent repositories.¹³⁴
- (q) At the conclusion of the indexing service and updating of the Consolidated View, the System Operator discards the copy of the record provided to it for those purposes. The registered repository operator retains its copy of the record, so that it can be retrieved when required by the consumer or a healthcare provider.¹³⁵
- (r) We understand that the System Operator would use the copy of the record to create a keyword profile and update the Consolidated View. After this process is complete, the copy of the record is destroyed. The provenance information from the record would be stored as part of the Indexing Service.
- (s) The process described above is dependent on a minimum level of consistency between records. In order to ensure consistency, each record will use a common set of ‘templates’, which describe the minimum data set for records and ensure consistency around information structure, clinical terminology and healthcare identifiers.
- (t) In addition to common templates for record, the PCEHR System will also be underpinned by common specifications and infrastructure for secure messaging and digital credentials.

¹³⁰ Information flow diagram received from the Department, 8 August 2011 (Upload of documents to the PCEHR System – document to be stored by a repository not part of the National Repositories Service, Step 8) and the Con Ops, section 4.2 (Clinical document types and templates)

¹³¹ Con Ops, section 4.2 (Clinical document types and templates)

¹³² Email from the Department dated 12 September 2011

¹³³ Information flow diagram received from the Department, 8 August 2011 (Upload of documents to the PCEHR System – document to be stored by a repository not part of the National Repositories Service, Step 9)

¹³⁴ Con Ops, section 4.2 (information model)

¹³⁵ Email from the Department dated 13 September 2011

- (u) This consistency ensures that when records are stored within registered repository operators, they can be validated and safely indexed. When an authorised user needs to find a record, they can be found, retrieved and imported into local clinical systems (if required).¹³⁶

5.6.3 Upload a record: National Repositories Service

- (a) The process for uploading a record to the National Repositories Service is similar to how a record is uploaded to a registered repository operator. To the extent that there are any differences, we have highlighted them below.
- (b) Where a consumer has a PCEHR, we understand that the default setting is that the record would be uploaded unless the consumer requests that it not do so. It is up to the healthcare provider to communicate with the consumer about the choice of whether to upload, particularly where the record could be sensitive. After this conversation occurs between a consumer and the practitioner, the consumer consents to the upload (or not).¹³⁷
- (c) At the conclusion of the indexing service and updating of the Consolidated View, the System Operator uploads the record to a National Repository Provider.
- (d) We understand that some key records, including the shared health summary, are strongly recommended to be included in a consumer's PCEHR. A shared health summary is a record sourced from the consumer's nominated healthcare provider, which provides a clinically reviewed summary of a consumer's healthcare status and provides information about a consumer's allergies and adverse reactions, medicines, medical history and immunisations.
- (e) As the shared health summary is a 'point in time' record, it is complemented by the 'Consolidated View' (see Con Ops, section 4.4.2). The Consolidated View presents the shared health summary, together with information from other records received since it was created.¹³⁸
- (f) Over time, extensions to the shared health summary could be implemented, allowing practitioners to upload other types of records.¹³⁹

5.6.4 Privacy positives

- (a) One privacy positive with respect to uploading records to the PCEHR is that a healthcare provider can upload without 'viewing' the PCEHR itself. We understand that consent to upload is considered different to consent to view or download, and either may be granted without the other. The PACC, if the consumer has established one, only constrains a user's ability to view (and download from) the consumer's PCEHR.
- (b) For example, a consumer may see a physiotherapist in relation to a back injury, and may ask their physiotherapist to upload a report because it may be relevant for the consumer's GP or orthopaedic surgeon to see it. However the consumer may not wish their physiotherapist to see their PCEHR because of all the other health information contained in it that is unrelated to their back injury, in which case the consumer can protect their PCEHR with a PACC, and choose not provide the PACC to their physiotherapist.
- (c) This is a significant privacy positive in the PCEHR System design.

¹³⁶ Con Ops, section 4.2 (Figure 8: Example information flow diagram)

¹³⁷ Information flow diagram received from the Department, 8 August 2011 (Upload of documents to the PCEHR System – document to be stored by the National Repositories Service, Steps 6, 6A and 6B)

¹³⁸ Con Ops, section 4.3.1 (Shared Health Summaries)

¹³⁹ Con Ops, section 2.8 (Potential enhancements)

- (d) Another privacy positive is that a consumer can nominate a healthcare provider ('nominated healthcare provider') to be responsible for establishing and updating their shared health summary as a separate record in the PCEHR. From a privacy perspective, this feature offers a sensible and good solution to the tensions of maintaining data quality and need for clinical moderation of consumer input.

5.6.5 Privacy risks - Data quality of uploaded records

- (a) The April 2011 version of the Con Ops¹⁴⁰ stated that records to be uploaded to the PCEHR *must* contain information about the consumer's 'name, IHI, date of birth, sex, address, communication details and indigenous status', and that record validation will include ensuring 'that the IHI, name, sex and date of birth highlighted in the record has an exact match to the details of the PCEHR it is being loaded into'¹⁴¹.
- (b) The revised August 2011 version of the Con Ops refers instead to a data quality framework which has yet to be finalised.
- (c) We caution against a data quality / record validation process which uses any fields beyond the consumer's IHI. Setting additional data fields for records may force the consumer to tell their clinician information that is not actually needed for that period of care, such as their indigenous status, address, date of birth, or communication details. By collecting more information about a consumer than is necessary, the healthcare provider will be at risk of contravening NPPs 1 and 10.
- (d) A further risk is that consumers may not provide what the PCEHR System considers to be 'accurate' information to each clinician, either to protect their privacy, or because the context is different (eg if the address provided for a particular episode of care was their holiday house). This poses a risk of breaching NPP 3.

5.6.6 Recommendations - Data quality of uploaded records

- 5.29 That the data quality framework for the PCEHR System design should ensure that the only mandatory field for identity/demographic data in relation to records is the consumer's IHI.
- 5.30 That the design makes it clear that the indigenous field status (as a type of 'sensitive personal information subject to special protection) is optional and not required to be completed.

5.6.7 Privacy Risks - When a record should not be uploaded

- (a) Access principles have a presumption that consumers should be given access to all their information held about them. However there is typically an exception in the case that access to one's own records might lead to harm (eg for a consumer suffering a psychotic illness). Access is usually mediated through a practitioner in such cases. (See for example OAIC, *Information Sheet (Private Sector) 21 - 2008: Denial of access to health information due to a serious threat to life or health*, at www.privacy.gov.au).
- (b) We understand that PCEHR System design does not address this issue *per se*; it is seen as a procedural issue for the clinician to manage at the time of deciding whether or not to upload a particular record.

¹⁴⁰ Con Ops, section 4.2.1 (Common fields in all clinical records and minimum core data sets). Con Ops, section 4.2.1 (Data Quality)

¹⁴¹ Con Ops, section 4.6.2 (Ensuring data quality)

- (c) The OAIC raised a number of other examples in which it may be appropriate for a clinician *not* to upload a record to the PCEHR, at least without seeking specific consent from the consumer:

*For example, records which might lead to harm by a consumer with a psychotic illness, or records relating to an episode of care which might be considered particularly sensitive due to possible stigma or discrimination by third parties (eg pregnancy loss or termination, drug and alcohol treatment, sexual health matters, mental health treatment).*¹⁴²

- (d) A similar issue is raised by some State and Territory-based legislation which might place restrictions on when a healthcare provider may upload some records, such as records which contain information about a consumer's HIV status.
- (e) We suggest that healthcare providers may need some guidance on these issues, and that the system design should ensure that local clinical systems do not in any way automatically 'upload' records to the PCEHR.

5.6.8 Recommendations - When a record should not be uploaded

- 5.31 That the conformance tests for clinical software to connect to the PCEHR System should include ensuring that no records are uploaded automatically from the local system to the PCEHR; that is a HPI-I user must make a 'manual' decision in relation to each upload.
- 5.32 That healthcare providers be provided with guidance on what records might not be appropriate to upload including where there are other legal restrictions in place.

5.6.9 Phase Two Annotations to Recommendation 5.31 and 5.32

- (a) In its submission to the Bill, SA Health submitted that requiring healthcare providers to obtain consumers' consent each and every time the healthcare provider wishes to upload information to the consumer's PCEHR creates an onerous burden on healthcare providers and that instead such uploading should be permitted unless the consumer requests otherwise.¹⁴³ Similar concerns were raised by the National Aboriginal Community Controlled Health Organisation¹⁴⁴ and Epworth Healthcare.
- (b) Given that consumers are able to control access to the PCEHR or require the records to be removed from the PCEHR, we consider that the privacy risks will be adequately managed if the Bill is amended so that information is uploaded as a feature of the PCEHR System unless a consumer advised that the record is not to be uploaded.

5.6.10 Phase Two Annotation to Recommendation 5.32 - Healthcare providers: refusing access to a consumer or third parties

- (a) In its submission to the Bill, MDA National recommended that healthcare providers should have the option to refuse access to a nominated representative or other individuals if the healthcare provider forms a view that disclosure would pose a serious threat to the life or health of any individual including the consumer, practitioner, relative, staff or other parties.¹⁴⁵
- (b) MDA National submitted that several of the authorised disclosure provisions of the Bill are inconsistent with existing privacy law. As part of our assessment of privacy principles

¹⁴² Submission from Timothy Pilgrim, Australian Privacy Commissioner of the Office of the Australian Information Commissioner, June 2011, Recommendation 5.14

¹⁴³ Submission to the Bill from SA Health dated 26 October 2011, page 3

¹⁴⁴ Submission to the Bill, undated

¹⁴⁵ Submission to the Bill from MDA National, page 3

outlined throughout this report and in Chapter 3, we note that NPP 6.1(c) allows organisations to refuse access to health information if access would pose a serious threat to the life or health of any individual. In the context of health information, the guidelines to the NPPs specify that a 'serious threat' does not have to be imminent. It can happen at any time. Some examples of a 'serious threat' include bodily injury, threat to mental health, illness or death.¹⁴⁶

- (c) We understand the design of the PCEHR system is such that a person who is not the healthcare provider who uploads the information will not have an ability to know what information is in the PCEHR. We recommend that the Bill be amended so that healthcare providers must comply with any request by a consumer that a document should not be uploaded.¹⁴⁷ This will give the consumer adequate control over access to documents that might pose a serious threat to the health of an individual.

5.7 Third party access

5.7.1 Permissible secondary uses and disclosures

- (a) It is proposed that the secondary uses and disclosures of personal information permitted under the Privacy Act will continue to be allowed in the PCEHR System.
- (b) Those secondary uses and disclosures would include:
 - (i) 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);
 - (ii) use or disclosure to prevent or lessen a serious and imminent threat to life or health;
 - (iii) use or disclosures for law enforcement purposes; and
 - (iv) some research purposes.¹⁴⁸

5.7.2 Research

- (a) In the case of research, the existing design would support participants in clinical trials providing access to their PCEHR to researchers, if they chose to. If the clinical trial is operating by a healthcare organisation, then the PCEHR can be accessed as per current arrangements for healthcare organisations.
- (b) In the case of wider public health research, generally using de-identified data, the PCEHR System has been designed to enable this research to be conducted as part of later releases (see Con Ops, section 4.6 which covers extraction of de-identified data via the Report Service).

5.7.3 Privacy positives

- (a) The design proposed for the PCEHR System precludes any unrelated third parties, such as law enforcement agencies or researchers, from having online access to the system. Any third parties who want access to data held in the PCEHR System would need to apply through the System Operator, which would apply the relevant privacy principles under the Privacy Act, which sets out the conditions under which personal information may be

¹⁴⁶ Guidelines to the National Privacy Principles issued by the then Office of the Federal Privacy Commissioner, Guidelines to NPP 6 – access and correction, September 2001, page 50 (<http://www.privacy.gov.au/law/act/npp>)

¹⁴⁷ Discussion with Department 13 November 2011

¹⁴⁸ Con Ops, section 5.2.3 (Research and other permissible uses)

disclosed for research, for law enforcement purposes, or when obligated under a subpoena or similar instrument.

5.7.4 Privacy risks

- (a) Due to the comprehensive indexing service provided in the PCEHR, we anticipate that a number of parties would seek access to information. Not only researchers and law enforcement agencies, but insurance companies and others involved in litigation with a consumer may find the service an attractive source of data relevant for their purposes.
- (b) The data sought may include records which the consumer has 'Removed from View', and Consumer Notes to which even healthcare providers do not have access.
- (c) A particular issue to be resolved is whether or not a subpoena, warrant, notice to produce or other instrument served on the System Operator could extend to records held in registered repository operators, which the System Operator does not hold, but to which the System Operator has access via the indexing service.
- (d) A related issue is the extent to which healthcare provider users of the system may be considered to be in the possession or control of information they can access through the PCEHR, for the purposes of responding to a subpoena, warrant, notice to produce or other instrument.
- (e) The extent to which the PCEHR is seen as a 'honeypot' of data for insurance companies and law enforcement agencies may impact on the degree of confidence placed in the PCEHR system by consumers.

5.7.5 Recommendations

- 5.33 That the PCEHR Bill prohibit any disclosure of Consumer Notes except where the System Operator is compelled to do so by way of a Court order or similar.
- 5.34 That the PCEHR Bill define the extent to which the System Operator will be considered to 'control' records held in registered repository operators but which are available through its indexing service, for the purposes of responding to a subpoena, warrant, notice to produce or other instrument.
- 5.35 That the PCEHR Bill define the extent to which healthcare provider users of the system will be considered to 'control' any data held in or indexed through the PCEHR, for the purposes of responding to a subpoena, warrant, notice to produce or other instrument.
- 5.36 That the PCEHR Bill prescribe whether the System Operator can allow the disclosure, for research purposes, of records held in registered repository operators but which are available through its indexing service.
- 5.37 That the PCEHR Bill prescribe whether the System Operator can allow the disclosure, for research purposes, of records which the consumer has sought to 'Remove from View'.
- 5.38 That the PCEHR Bill include a note to the effect that the rules under which personal information may be disclosed by the System Operator for research, for law enforcement purposes, or when obligated under a subpoena or similar instrument are to be found in the Privacy Act.
- 5.39 That consumer communications (and in particular, the privacy notice provided at the time of registration) reflect the possibility that information from their PCEHR may be disclosed for research or law enforcement purposes, or when required by law, such as in response to a subpoena if the consumer is involved in litigation.

5.7.6 Phase Two Annotations to recommendations 5.33 to 5.39 (Third party access)

- (a) In its submission to the Bill, Avant Mutual Group noted it was important for an authorised user to have access to health information for legitimate forensic purposes. Avant Mutual Group then recommended that s 61 (Disclosure to Courts and tribunals) be amended to allow this.¹⁴⁹
- (b) In our view, s 61 and s 62 (Disclosure for law enforcement purposes) of the Bill are sufficiently drafted to include disclosure of health information for forensic purposes. The ordinary meaning of 'forensic' includes matters relating to Courts of law and methods used for investigation.¹⁵⁰

5.7.7 Phase Two Annotations to recommendations 5.36, 5.37 and 5.38 (Third party access)

- (a) In its submission to the Bill, the Australian Privacy Foundation requested:

'..... that legislative guidelines be incorporated into the Bills to control researcher access to PCEHR system data stored on health services' clinical information systems for secondary purposes without consumer knowledge or consent'.¹⁵¹
- (b) It would appear that the Australian Privacy Foundation is concerned that a researcher may have access to PCEHR data stored on a healthcare provider's local system and would use that information for secondary purposes without a consumer's knowledge or consent.
- (c) The design of the PCEHR System proposes that 'any information downloaded or printed from the PCEHR System *and stored in a local record* will be managed using local record retention policies and any other locally applicable legal requirements'.¹⁵²
- (d) Recommendation 8.1 of this Report and the accompanying commentary addresses the issue of privacy regulation for information downloaded from the PCEHR System in a nationally consistent manner.

5.7.8 Annotation to recommendations 5.29 and 5.30 (Data quality) and recommendations 5.36 to 5.39 (Research)

- (a) In its submission to the Bill, the National Aboriginal Community Controlled Health Organisation (NACCHO) raised a concern that reporting and analysis of information in the PCEHR System should not be for the purpose of research or statistical modelling or secondary uses without full disclosure and agreement from peak representative bodies because the PCEHR dataset is not complete.¹⁵³
- (b) From a privacy perspective, so long as appropriate consent has been obtained to use the information for secondary purposes (research or otherwise) as envisaged by s 59 of the Bill no additional privacy risk arises.
- (c) If the consumer has granted consent for use of health information only on a de-identified basis and a person subsequently discloses information in a manner that enables the consumer's identity to be ascertained then that person is at risk of having breached the provisions of the Bill and the Privacy Act. To that extent, the Bill and other privacy legislation would seem to address the privacy risk raised by NACCHO.

¹⁴⁹ Submission to the Bill from Avant Mutual Group, page 3

¹⁵⁰ The Oxford Dictionary (<http://oxforddictionaries.com/definition/forensic>)

¹⁵¹ Submission to the exposure draft PCEHR Bill 2011 from the Australian Privacy Foundation, submitted 27 October 2011, page 2

¹⁵² Con Ops , section 4.2.4 (Retention of records: Downloaded and printed information)

¹⁵³ Submission to the Bill from the National Aboriginal Community Controlled Health Organisation, page 3 point 5 and page 7 point 15

- (d) That said, the concerns raised by NACCHO are important and gives weight to the commentary referred to in Phase One of this report that consumer communications (required under NPP 1.3) should be carefully reviewed to ensure that consumers are well informed about what they are registering for and consenting to when they register for a PCEHR.

5.7.9 Phase Two Annotation – Collection, use and disclosure for the management of the PCEHR System

- (a) In its submission on the Bill, NACCHO raised a concern that the consent of the consumer should be obtained for any exchange of health information for the purpose of enabling appropriate management of the PCEHR System.¹⁵⁴
- (b) Clearly a delicate balance must be struck between the potential competing interests of the consumer's privacy and the efficient working of the PCEHR System. Section 56 of the Bill endeavours to achieve this by applying the objective test of what a 'consumer would reasonably expect the participant to collect, use or disclose' for the purpose of the management of the PCEHR System. The Medical Software Industry Association (MSIA) raised a concern that in practice consumers will not know how the PCEHR System should reasonably operate.¹⁵⁵
- (c) Ultimately this will be interpreted by the relevant Courts and tribunals. To assist such forums to apply consistent interpretation of the Bill, the Explanatory Memorandum should list as many examples as possible to explain the intended scope of the section.
- (d) In its submission on the Bill, MSIA recommended that s 44 of the Bill be deleted or amended to list the reasons for compulsory disclosure by a registered repository operator, registered portal operator or contracted service provider to the System Operator so as to mitigate the risk that health information is provided to the System Operator for purposes that are beyond the consumer's reasonable expectations.¹⁵⁶
- (e) Section 44 does not explicitly confine the purposes for which the System Operator may use the health information obtained from the designated entities. Further s 56(2) makes it clear that the use by the System Operator of health information in a consumer's PCEHR under s 44 is not limited by whether such use is within the consumer's reasonable expectation. From a legal perspective (as a matter of statutory interpretation), the System Operator is limited by the Bill to using the health information for the purposes of its functions. This is complicated by the fact that it is intended that, for an interim period, the System Operator will be the Department which has many additional functions.
- (f) We are of the view that the Bill should be amended to better address this privacy risk so that it is clear that the System Operator can only use the information obtained under s 44 of the Bill as is reasonable for the purposes of undertaking its functions in accordance with s 11 of the Bill (Functions of the System Operator). In addition it would be useful for the explanatory memorandum to provide examples of what such uses may be. The Australian Privacy Commissioner has made similar comments in its submission regarding the Bill.¹⁵⁷
- (g) MSIA also recommended that the Bill should specify the type of administrative information envisaged by s 50 of the Bill that would be included in the register.¹⁵⁸ We

¹⁵⁴ Submission undated page 7 point 14

¹⁵⁵ Submission dated 28 October 2011 page 10

¹⁵⁶ Submission dated 28 October 2011 page 9

¹⁵⁷ Submission dated October 2011 pages 14

¹⁵⁸ Submission dated 28 October 2011 page 9

agree that if the type of information is likely to be personal information about a consumer and participant other than the System Operator will have access to that information then that should be clearly specified in the PCEHR Rules so as to ensure the consumer is aware that his or her personal details by be disclosed in that way.

Chapter 6 - PCEHR suspension, deactivation and reactivation

6.1 Overview of suspension, deactivation and reactivation

Set out below is a table summarising the proposals for access and storage that are triggered when a consumer's PCEHR is activated, suspended or reactivated. More detailed descriptions are outlined below.

Status	Trigger	Information seen by consumer/HCP	Information kept	What next?
Active	<ul style="list-style-type: none"> Registration (brand new) Reactivation of suspended or deactivated account 	<ul style="list-style-type: none"> All records (subject to consumer's access settings) 	<ul style="list-style-type: none"> All records 	<ul style="list-style-type: none"> All records kept until account is Deactivated.
Suspended	<ul style="list-style-type: none"> Minors who have turned 18 but not yet registered Voluntary (eg moving overseas) System operator's decision (eg in cases where there is a dispute between authorised representative) 	<ul style="list-style-type: none"> All records can be accessed for emergencies Records can be accessible via the System Operator for maintenance, audit, when required by law and other approved purposes. Otherwise, no records can be accessed 	<ul style="list-style-type: none"> All records – information can still be uploaded 	<ul style="list-style-type: none"> All records kept until account is Deactivated.
Deactivated	<ul style="list-style-type: none"> Voluntary IHI retired (fact of death received, or consumer age is 130) 	<ul style="list-style-type: none"> None. Records will only be accessible via the System Operator for maintenance, audit, when required by law and other approved purposes. 	<ul style="list-style-type: none"> First 90 days – All records kept. After 90 days – All records archived. Archived records will not be retrieved unless required under law. 	<ul style="list-style-type: none"> Reactivated within 90 days – can either be reactivated as was OR can be a new 'clean' record Reactivated after 90 days – new 'clean' record If not reactivated – All records archived for a minimum period (currently 15 years).

6.2 Suspension of a PCEHR

6.2.1 Description of the process

- (a) In some circumstances, a PCEHR can be suspended. This means that the PCEHR cannot be viewed by healthcare providers except in emergencies. Healthcare providers may, however, still upload records into a consumer's suspended PCEHR.

- (b) It is intended that the System Operator will be able to suspend a PCEHR where:
 - (i) the consumer turns 18 and takes no action on whether their PCEHR is reactivated or deactivated;
 - (ii) the consumer voluntarily requests the suspension;
 - (iii) there is a dispute about access between two authorised representatives over the same PCEHR (for example, the guardians of a minor); or
 - (iv) notification of death is received from the HI Service Operator.
- (c) We understand that it is not proposed for the System Operator to suspend PCEHRs for other reasons, other than those described above.¹⁵⁹
- (d) When a minor turns 18, the consumer's PCEHR is suspended until the consumer chooses to either re-register for PCEHR or deactivate their PCEHR.
- (e) At any time, consumers may voluntarily suspend their own PCEHR. For example, consumers who relocate overseas for a number of years may wish to suspend their PCEHR due to a lack of activity. In this case, there would be no necessity for any healthcare provider in Australia to access their PCEHR and the consumer may, due to those circumstances, not be in a position to actively monitor information being uploaded. On their return, they could review their PCEHR, identify any information that may have been uploaded incorrectly, request corrections if necessary, then reactivate their PCEHR.¹⁶⁰
- (f) Where a PCEHR is suspended due to a dispute between authorised representatives, the PCEHR would remain suspended until there is a Court order or agreement between the representatives to govern access to the PCEHR.¹⁶¹ We understand that a copy of the Court order or agreement must be provided or sighted by the System Operator before a PCEHR is reactivated.¹⁶²
- (g) After the death of a consumer, once the fact of death has been established (fact of death is notified by State registries to Medicare, which 'retires' the consumer's IHI and notifies the System Operator), the consumer's PCEHR will be deactivated and all access will be suspended.¹⁶³ The deceased consumer's PCEHR can be accessed when it is required by law, via the System Operator (not via online channels).¹⁶⁴

6.2.2 Access to a suspended PCEHR

- (a) Where a PCEHR is suspended, it cannot be viewed by the consumer, authorised representatives, nominated representatives or healthcare providers. However, the PCEHR can be accessed when emergency access is requested by a healthcare provider. A suspended PCEHR can also be accessed when it is required by law, via the System Operator.

6.2.3 Privacy positives

- (a) The provision of an option for consumers to voluntarily suspend their PCEHR is a privacy positive feature of the PCEHR System. Suspension of all 'view' access to their PCEHR is a straight-forward and sensible option for consumers who need to take action quickly (eg a

¹⁵⁹ Email from the Department dated 13 September 2011

¹⁶⁰ NEHTA response dated 30 August 2011

¹⁶¹ NEHTA response dated 30 August 2011

¹⁶² Email from the Department dated 12 September 2011

¹⁶³ Con Ops, section 3.2.11 (Deceased individuals)

¹⁶⁴ Con Ops, section 3.2.11 (Deceased individuals)

person fleeing harm) and consider more nuanced privacy settings later. For consumers who go overseas or otherwise have an inactive PCEHR for extended periods of time, it also mitigates the risk of unauthorised access to their PCEHR during these dormant periods.

6.2.4 Privacy risks

- (a) We have not identified any particular privacy risks with the suspension process, subject to the comments made in Chapter 4 in relation to the processes by which consumers provide evidence of their identity to the System Operator.

6.2.5 Phase Two Annotations to subparagraphs 6.2.1 to 6.2.4 (Suspending registration of a consumer, healthcare provider or entity)

- (a) In its submission to the Bill, SA Health commented:
*'there does not appear to be any mechanism for immediate suspension of [an entity's] registration in the case of a serious breach. For example, the System Operator should be able to "shut down" a repository operator, portal provider or contracted service provider's access to the PCEHR System as soon as it becomes aware of a serious security breach.'*¹⁶⁵
- (b) As it stands, under the Bill the System Operator must give the consumer and entity at least 14 days notice of an intention to suspend or cancel registration.¹⁶⁶
- (c) The Companion document to the Bill notes an outstanding item for the Bill is the ability of the System Operator to immediately suspend or cancel a participant's registration *in an emergency* subject to providing reasons.¹⁶⁷ If the emergency stems from a breach of the Bill then the issue raised by SA Health will presumably be met. If no such emergency exists then the time imperative may not exist which would allow time for the offending entity to use the complaints process to respond to the proposed suspension or cancellation. This would seem to be a reasonable balance between ensuring protection of privacy rights arising from a breach of the Bill and enabling the 'right to be informed and heard' to be applied before revoking rights to the PCEHR System. This balance will inevitably hinge on the meaning given to 'emergency' which we would expect to be clarified in the Bill and/or Explanatory Memorandum once the outstanding issue is addressed.

6.3 Deactivation of a PCEHR

6.3.1 Overview of the process

- (a) Participating consumers (or their authorised representatives) may choose to withdraw at any time. If a consumer withdraws, their PCEHR will be 'deactivated'. PCEHRs are also deactivated upon fact of death being received from the HI Service Operator, or the consumer's recorded age exceeding 130 years.
- (b) A consumer can deactivate their PCEHR using both assisted and self-service channels.¹⁶⁸ Each of the channels has been dealt with separately (to highlight the differences in information flows between the channels).

¹⁶⁵ Submission to the Bill from SA Health dated 26 October 2011, page 5

¹⁶⁶ Subsection 47(1).

¹⁶⁷ section 3.3.4, page 24.

¹⁶⁸ Con Ops, section 3.2.5 (Ensuring access in a range of situations)

6.3.2 Mail channel

- (a) For deactivation by mail, the process for deactivating a PCEHR is very similar as to registration, where the consumer will assert that they want to deactivate their PCEHR and supply certified copies of EOI records to support that they are indeed the person asking for deactivation. This will be similar for authorised representatives where the authorised representative will assert that they want to deactivate the PCEHR, supplied certified copies of their EOI and certified copies of their authorisation.¹⁶⁹

6.3.3 Face to face channel

- (a) To deactivate in the face to face channel, a consumer or their authorised representative must attend a Medicare shop front. Over time, other avenues may be made available.
- (b) We understand that the process for face to face deactivation of a PCEHR is similar to the registration process, where the consumer will be required to produce sufficient EOI to confirm who they are and then an ARA will use the Administration Portal to deactivate the PCEHR.
- (c) In a co-located Medicare and Centrelink shopfront, the ticketing system used will identify the service required. The ticket will direct the service to the next available officer who has been trained in the process and has access to the required tools. This will generally be Medicare staff in most instances. However, in some smaller and remote localities this may be an officer that performs all the functions. There will be no PORO questions required for this process.¹⁷⁰
- (d) Some consumers may have specific privacy concerns about Centrelink staff facilitating this process, particularly where Medicare and Centrelink shops are co-located, and DHS staff in those shops perform a variety of functions. When the operational details are clearer, we suggest clarifying whether DHS staff would be able to view a consumer's PCEHR. Consumers may have specific privacy concerns about DHS staff viewing their health information.
- (e) Concerns relating to privacy exposures could arise for consumers where:
 - (i) a consumer's eligibility for a benefit depends on the presence of a medical condition eg Carer Payment, Carer's Allowance, Mobility Allowance; or
 - (ii) a consumer's rate of payment depends on both the presence of a medical condition and that medical condition impacts on the consumer's ability to participate in the workforce eg disability pension.
- (f) If a consumer's health information is viewed by a Centrelink officer, some consumers may feel that the disclosure of the health information may adversely impact on their welfare payments, irrespective of whether the DHS officer merely makes an enquiry to the consumer, views a particular record or takes any other further action. Ultimately, this is an issue relating to community expectations, and whether using Centrelink officers for this process would enhance trust and confidence in the PCEHR System, or instead detract from it.
- (g) The 'Administration Portal' enables Service and Support Agents, Authorised Registration Agents and Call Centre staff working in one of the channels (eg call centre, Medicare shop front, etc) to assist consumers with registration, help consumers manage their PCEHR, access support information about the PCEHR System and access the contact management

¹⁶⁹ Email from the Department dated 13 September 2011

¹⁷⁰ Email from the Department dated 13 September 2011

service. The Administration Portal will allow users to assist consumers with deactivating their PCEHR.¹⁷¹

6.3.4 Telephone channel

- (a) To deactivate in the telephone channel, a consumer or their authorised representative must contact the Call Centre.¹⁷²
- (b) The PCEHR System will also provide an 'Administration Portal' to enable Call Centre staff to assist consumers with registration, help consumers manage their PCEHR, access support information about the PCEHR System and access the contact management service. The Administration Portal will also allow users to assist consumers with deactivating their PCEHR.¹⁷³
- (c) The process for the telephone channel would involve the consumer identifying themselves by correctly answering a series of questions and answers. It is proposed that the questions answers are either:
 - (i) 'secret' questions and answers previously established by the consumer; or
 - (ii) PORO questions generated from existing DHS records that would be presented to the consumer.¹⁷⁴
- (d) As with the face to face channel, if the consumer does not meet the minimum threshold to 'claim' their records, the DHS officer will advise the consumer that an insufficient number of points was achieved. The consumer can be asked to answer further questions to attempt to meet the minimum threshold. If the consumer is unable to satisfactorily complete the PORO process, we suggest the consumer be re-directed to the face to face channel for further assistance. We assume that if a consumer was also unable to answer the 'secret' questions and answers, the consumer would also be redirected to the face to face channel for further assistance.

6.3.5 Online channel

- (a) From a registered portal operator, the consumer (or their authorised representative) can also request to deactivate their PCEHR.¹⁷⁵ Where a PCEHR is active, the consumer can request to deactivate their PCEHR. Where a PCEHR is suspended, the consumer would first have to complete registration in order to gain access to their suspended PCEHR. Having done so, they could then deactivate online.¹⁷⁶
- (b) As with the assisted channels, questions are presented to consumers using information from the audit log or other records held in the consumer's PCEHR. When a consumer answers a question, the answer will be marked as correct, incorrect or 'did not answer' by comparing the answer provided by the consumer with the answer held on the consumer's record. At the conclusion of the questions, the consumer's responses will be calculated using a calculator tool.
- (c) If the consumer meets the minimum threshold, the consumer can proceed to finalise the deactivation process.

¹⁷¹ Con Ops, section 6.3.6 (Administration Portal)

¹⁷² Con Ops, section 6.3.5 (Call Centre)

¹⁷³ Con Ops, section 6.3.6 (Administration Portal)

¹⁷⁴ Email from the Department dated 13 September 2011

¹⁷⁵ Con Ops, section 6.2.1 (Conformant Portals)

¹⁷⁶ NEHTA response dated 30 August 2011

- (d) If the consumer does not meet the minimum threshold to 'claim' their records, the consumer will be advised that an insufficient number of points was achieved. The consumer may be asked to answer further questions to attempt to meet the minimum threshold. If the consumer is still unable to complete the PORO process satisfactorily, the consumer is advised to complete the deactivation via an assisted channel (face to face or telephone).

6.3.6 Participation and Authorisation Service

- (a) The 'Participation and Authorisation Service' supports a number of functions including requests to deactivate a PCEHR. The Participation and Authorisation Service also records the status of a PCEHR (eg active, deactivated, reactivated)¹⁷⁷. A consumer's decision to deactivate their PCEHR is stored in a consumer's PCEHR within the Participation and Authorisation Database.¹⁷⁸ The 'Participation and Authorisation Service' and 'Administration Portal' cannot be accessed directly, but through the various Portals and B2B Gateway.
- (b) In a 'deactivated' PCEHR, any information that has been collected up to the point of being deactivated will continue to be stored, but the PCEHR will not be accessible via the PCEHR System to any healthcare providers, the consumer, or their representatives. Records will only be accessible via the System Operator for maintenance, audit and other lawful purposes.
- (c) Any information that a healthcare organisation has obtained from a consumer's PCEHR and added to their local records before the PCEHR has been deactivated will continue to be available to those healthcare providers through their local record.¹⁷⁹

6.3.7 Deactivation: storage

- (a) After a cooling off period (initially proposed to be 90 days), information within a deactivated PCEHR will be archived and retained as per the retention policy described in the Con Ops, section 4.2.4 (Retention of Records). If a consumer changes their mind at anytime during the cooling off period, a consumer can reactivate their PCEHR fully restored or reactivate a 'clean' PCEHR afresh. Records which may have existed in their previous PCEHR are moved to archive storage and are not reinstated into their new PCEHR.
- (b) Any records archived by the System Operator will be held for a minimum period as defined by PCEHR legislation (currently suggested as being a minimum of 15 years since last action on the record or until the consumer turns 30, whichever period is longer). Records will not be retrieved from the archive unless disclosure is required under law.
- (c) Deactivated records are stored in the National Repository and registered repository operators. Records stored in the National Repository are only accessible by the System Operator. Other PCEHR records are stored by external registered repository operators eg pathology laboratories. These registered repository operators may facilitate other access to the information eg via a local system. However, the records would be inaccessible via the PCEHR System.¹⁸⁰
- (d) We note that the storage policies vary between the National Repository and registered repository operators. The System Operator has control over the former but not the latter.

¹⁷⁷ Con Ops, section 6.4.2 (Participation and Authorisation Service)

¹⁷⁸ Response from NEHTA dated 30 August 2011

¹⁷⁹ Con Ops, section 3.2.7 (Withdrawal)

¹⁸⁰ Response from NEHTA dated 30 August 2011

Where access is still available to records held in a registered repository operator, we suggest this is clearly communicated to consumers, to mitigate the risk of a consumer mistakenly thinking their records are not available to anyone except the System Operator. We understand that the Department is considering raising this issue with the National Change and Adoption Partner for further consideration.¹⁸¹

6.3.8 Deactivation: consumers under witness protection

- (a) Where a consumer has been given a new identity (such as people under witness protection or subject to controlled identities such as undercover police officers), the new IHI is not traceable to the consumer's old IHI (and subsequently, their former identity).¹⁸²
- (b) The pseudonymous IHI is issued by specialist DHS staff, which means that the System Operator has no involvement in or knowledge of the establishment of a pseudonymous IHI. The System Operator only becomes aware of pseudonymity if:
 - (i) the consumer volunteers that information; or
 - (ii) the consumer requests the merger of a pseudonymous and non-pseudonymous PCEHR, presumably because they no longer feel the need to use a pseudonym.¹⁸³
- (c) To enhance a consumer's safety and to mitigate the risk of an identity exposure, we suggest that consumers in this situation who later seek to merge their two IHIs and PCEHRs are given sufficient warning of the implications of the merger.

6.3.9 Minors: suspension, reactivation and deactivation

- (a) When a minor turns 18, they take responsibility for their own PCEHR. The PCEHR System will no longer allow a parent or legal guardian to access the consumer's PCEHR unless the consumer grants access to the parent or guardian as a nominated representative.
- (b) When a minor turns 18, they need to go through the registration process in order to take responsibility for their PCEHR. Until this occurs, their PCEHR is suspended by the System Operator.
- (c) Alternatively, if the consumer 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 an Authorised Registration Agent. Also, if a consumer with capacity wants a parent to continue to access their PCEHR, the parent will need to be registered as either a nominated representative or authorised representative.
- (d) There are three options:
 - (i) *no action by the consumer*: if the consumer does nothing, the default position is that the PCEHR is suspended;
 - (ii) *registration and activation*: the consumer wants to 'unlock' their PCEHR and wishes to continue having a PCEHR. The consumer will need to go through the registration process; or
 - (iii) *deactivation*: the consumer wants to opt out and close their PCEHR.
- (e) It is recognised that some minors may wish to take personal control of their PCEHR before turning 18.

¹⁸¹ Email from the Department dated 13 September 2011

¹⁸² Email from the Department dated 12 September 2011

¹⁸³ Email from the Department dated 16 September 2011

- (f) The Change and Adoption Partner is considering a range of educational programs for minors to be delivered through school programs and media to advise them of the PCEHR and their rights of access. This will, hopefully, encourage them to have conversations with their parents or even seek to gain access and control when reaching maturity.¹⁸⁴
- (g) Ideally, from 14 years on, a notification will be delivered when the minor's PCEHR is accessed by a healthcare provider, parent or other authorised representative. This will be in the form of a prompt to advise the consumer that they are now, potentially, in a position to assume control of their record. This notification will, in general, not be delivered to the minor, but will facilitate the prompting of a discussion with them.

6.3.10 Privacy positives

- (a) The provision of an option for consumers to voluntarily deactivate their PCEHR is another privacy positive feature of the PCEHR System.

6.3.11 Privacy risks

- (a) We have not identified any particular privacy risks with the deactivation process, subject to the comments made in Chapter 4 in relation to the processes by which consumers provide evidence of their identity to the System Operator.
- (b) One matter which may require legislative and/or design change is to ensure that child consumers who have taken control of their PCEHR between the age of 14 and 18 will also have the right to suspend or deactivate their record.
- (c) Another matter is yet to be clarified, which is whether 'Active' records will be moved into a 'Suspended' or 'Deactivated' state after a long period of inactivity on the record. If not, it would appear that the data retention period of 15 years will not even begin to run until the System Operator receives notice that the consumer's IHI has been 'retired', and thus the System Operator will effectively maintain health information for the entire life (and then a further 15 years) of the consumer, unless they deactivate their record voluntarily. This is a significant change to current data retention practices at the healthcare provider level, which tend to set a shorter time period for most types of health information, with a few exceptions requiring lifetime data retention.
- (d) The data retention periods for data held by the System Operator, including in the National Repositories Service, also need careful explanation to consumers and healthcare providers in the context of deactivated records.

6.3.12 Recommendations

- 6.1 That the PCEHR Bill ensure that child consumers aged 14 through 17 who seek to take control of their PCEHR have the right to do so, and that their rights include decisions to suspend or deactivate their record.
- 6.2 That the PCEHR Bill set a data retention period for PCEHR records in the 'Active' category which have not been subject to any action on the record (such as any new data being added) for an extended period of time.
- 6.3 That the consumer communications about suspension and deactivation of records clarify that although records held in registered repository operators may no longer be found through a suspended or deactivated PCEHR, they will be held by the registered repository operators and/or in local clinical systems for periods as determined by local data retention requirements.

¹⁸⁴ Response from NEHTA dated 30 August 2011

6.4 That the exception for emergency access is clearly communicated to consumers prior to the PCEHR entering 'suspension mode'.

6.3.13 Phase Two Annotations to Recommendations 6.1 to 6.4

- (a) In its submission to the Bill, the Royal Children's Hospital recommended that consumers have the option to permanently remove a record from their PCEHR and permanently delete their PCEHR. Health information recorded when the consumer was a minor may be embarrassing or irrelevant to the consumer's healthcare as an adult. When a minor reaches adulthood, they should be able to make informed decisions about their PCEHR.
- (b) When a minor reaches adulthood, the consumer has 3 options:
 - (i) remove the record from view after reactivating their PCEHR;
 - (ii) deactivate their PCEHR, archive the records and once archived, no access is available except by the System Operator for maintenance purposes; or
 - (iii) if a consumer chooses to reactivate a deactivated PCEHR, the archived records are not reinstated into the new PCEHR.
- (c) At paragraph 6.3.11, we noted that no particular privacy risks were identified with the deactivation process subject to our comments made in Chapter 4. The options described above aim to balance the interests of giving consumers choices whilst ensuring that local archival and retention requirements are met.

6.4 Reactivation of a PCEHR

6.4.1 Description of the process

- (a) The PCEHR System operates on an opt-in model, where consumers elect to register and create a PCEHR. Consumers may deactivate their PCEHR at any time and subsequently reactivate their PCEHR at any time (Con Ops, section 1.4).
- (b) Reactivation is only relevant where an existing PCEHR was previously deactivated or suspended and the consumer wants to opt in again and reactivate their account.
- (c) From within a registered portal operator, the consumer (or their representative) can request to reactivate a deactivated or suspended PCEHR (Con Ops, section 6.2.1).
- (d) The PCEHR System will also provide an Administration Portal to enable Service and Support Agents, Authorised Registration Agents and Call Centre staff working in one of the channels (eg, call centre, Medicare shop front, etc) to assist consumers with registration, help consumers manage their PCEHR, access support information about the PCEHR System and access the contact management service. The Administration Portal will allow users to assist consumers with reactivating their PCEHR (Con Ops, section 6.3.6).
- (e) If a consumer chooses to reactivate their PCEHR within the 90 day 'cooling off period' following deactivation, the consumer will be given the option of restoring their record to its previous state prior to deactivation, or starting again with a 'clean' PCEHR. After the cooling off period, a reactivated PCEHR will start 'clean', and access to previously collected information will not be available to the consumer (Con Ops, section 3.2.7).

6.4.2 Privacy positives

- (a) Consumers who reactivate their PCEHR within a 'cooling off' period will be offered the choice between re-instating their 'old' record, or starting 'clean' with a new record. This choice is a privacy positive aspect of the proposal.

6.4.3 Privacy risks

- (a) We have not identified any particular privacy risks with the reactivation process, subject to the comments made in Chapter 4 in relation to the processes by which consumers provide evidence of their identity to the System Operator.

Chapter 7 - System Operator

7.1 Governance structure

7.1.1 Description of the process

- (a) The PCEHR System will be operated by a single system operator who will take on the responsibility for operating the national infrastructure.
- (b) It is proposed that the legislation will establish the System Operator, prescribe the System Operator's functions and responsibilities and establish an administrative framework for setting the service levels and operations rules that the System Operator must meet.
- (c) The System Operator will be subject to the future operational governance model of the PCEHR System and be required to meet a common set of service levels (see system attributes described in the Con Ops section 6.1.1).
- (d) The operator also must not perform the role of System Operator unless it is subject to the Privacy Act, or privacy rules based on the Privacy Act, contained in PCEHR specific legislation.¹⁸⁵

7.1.2 Commentary

- (a) The likely governance structure of the System Operator is in too early a stage of development for our analysis to offer any depth on this point. However we do note that, as an Australian Government agency, the System Operator would normally be regulated by the IPPs in the Privacy Act.
- (b) By contrast, most of the healthcare providers likely to participate in the PCEHR System will be regulated by the NPPs, or a set of State-based principles more closely aligned to the NPPs than the IPPs. The NPPs are 'newer' and therefore broader than the IPPs, and are also closer to the likely direction of law reform in the near future.
- (c) We therefore suggest that in order to work towards a 'level playing field' for all participants in the PCEHR System, the System Operator ought to be subject to the NPPs rather than the IPPs.

7.1.3 Recommendation

7.1 That the PCEHR Bill ensure that the System Operator is subject to the NPPs (or rules based on the NPPs) rather than the IPPs in the Privacy Act.
--

7.2 Reporting

7.2.1 Description of the process

- (a) The Report Service is designed to support reporting and analysis of information across the set of personal health information managed by the PCEHR System. In the first release, the report service will only be used for operational reporting and evaluation of the PCEHR System.

¹⁸⁵ Con Ops, section 7.3 (System Operator) and email from the Department dated 13 September 2011

- (b) Key functions of the Report Service include:
 - (i) Data extraction, transformation and loading services to load PCEHR data into a data warehouse;
 - (ii) De-identification services (including the option of making data re-identifiable if required); and
 - (iii) Data warehouse and related data mart services to store data and enable creation of the reports identified in the Con Ops, section 4.6.¹⁸⁶

7.2.2 Re-identified data from a deactivated PCEHR

- (a) In very limited circumstances, records can be re-identified after a consumer's PCEHR is deactivated. Re-identification would be undertaken by Reporting Users.
- (b) In the limited cases where data would be re-identified, the consumer's PCEHR would not be reactivated. There are de-identification methods through which 'cross reference tables' are constructed enabling the System Operator to identify the origin of de-identified data supplied for research purposes and other lawful secondary purposes.¹⁸⁷ When the operational details are clearer, we suggest further reviewing this process for clarification.
- (c) We understand that where data is re-identified, this would not cause a consumer's deactivated PCEHR to be reactivated.¹⁸⁸

7.2.3 Privacy risks

- (a) While most operational reporting on the PCEHR System is likely to focus on metadata about use of the system, some health information from consumers' records may also be used for public health reporting. To the extent that such information is not de-identified prior to its extraction for a report, this will constitute 'personal information' subject to limitations on use and disclosure.
- (b) Secondary use of consumers' health information for operational purposes, including public health purposes, should therefore be appropriately authorised by legislation.

7.2.4 Recommendations

7.2 That the PCEHR Bill establish the System Operator's authority to use and disclose data (including metadata) from a consumer's PCEHR for reporting purposes. The legislation should set out the bodies to whom personal information may or must be disclosed by the System Operator including a reference to reporting obligations created in other legislation.

7.3 Audit logging of access and use

7.3.1 Overview of the process

- (a) One of the measures to ensure accountability is an audit trail. In previous consultations, it was widely agreed that an audit function is essential to ensure confidence by both consumers and healthcare providers.
- (b) The PCEHR System will provide an Audit Service to record all activity on the national eHealth infrastructure services and registered repository operators.

¹⁸⁶ Con Ops, section 6.4.6 (Report Service)

¹⁸⁷ NEHTA response dated 30 August 2011

¹⁸⁸ NEHTA response dated 30 August 2011

7.3.2 Privacy Positives

- (a) Comprehensive audit logging of all access to a consumer's PCEHR creates a strong inhibitor of misuse. In addition, providing real-time access to the consumer of a summary version of the audit log will dramatically improve transparency in the handling of health information, and further mitigates the risk of misuse by an identifiable user. Healthcare providers' privacy is also protected, in that the consumer will see the role of the user, but not necessarily their name. However either the name or HPI-I of the user is visible to the System Operator, and can be retrieved in the case of a privacy complaint.
- (b) The audit logging proposals therefore offer significant privacy positives in terms of the Data Security principle (NPP 4) and the Openness and Access principles (NPPs 5 and 6).
- (c) In its submission to the Bill, the Royal Children's Hospital of Melbourne recommended the Bill specify that consumers will have access to the audit trail of their PCEHR and that the Bill should specify that the audit trail will show everyone who has accessed the consumer's PCEHR, not just healthcare provider organisations and government employees.¹⁸⁹ As described elsewhere and in paragraph 7.3.2 of this report, consumers will have real-time access to their audit log. In recommendation 5.19, we also suggested the Bill set one of the conformance requirements on a HPI-O as an obligation to verify, with 100 points of EOI, the identity of each proposed user (and confirm their proper association to a HPI-I, where applicable).
- (d) We note the Minister may make PCEHR Rules that apply to participants in the PCEHR System: s 97(2)(d). In our view, rules could be created that require users to be adequately identified by a HPI-O and associated to a HPI-I where applicable, prior to accessing the PCEHR System.

7.3.3 Privacy Risks

- (a) We have mentioned elsewhere in this report the need for registered healthcare provider organisations to carefully verify the identity and role claims of their users, in order to be able to both deter and properly prosecute any instances of misuse. For similar reasons, it will be essential to ensure that the audit logging function is working as intended. Conformance requirements on HPI-Os will need to be strict, to promote consumer confidence in the system.
- (b) Like other metadata, audit logs constitute 'personal information' subject to limitations on use and disclosure. Legislation will need to establish the System Operator's authority to collect the metadata in the audit logs, and establish how it can use and disclose that data.
- (c) For consumers without online access to their PCEHR, an alternative method should be developed, to allow them a copy of the summary version of their audit log.

7.3.4 Recommendations

- 7.3 That the System Operator ensure strict conformance requirements on HPI-Os to ensure users are uniquely identified to the System Operator at every login.
- 7.4 That the PCEHR Bill establish the System Operator's authority to use and disclose audit log data from a consumer's PCEHR for complaint-handling and law enforcement purposes. The legislation should set out the bodies to whom personal information may or must be disclosed by the System Operator, including the Australian Privacy Commissioner or other privacy regulator in the case of a privacy complaint, or to the

¹⁸⁹ Submission to the Bill from the Royal Children's Hospital of Melbourne, page 2

appropriate law enforcement agency in the case of suspected unlawful use.

- 7.5 That the PCEHR Bill establish the right of a consumer to obtain a copy of the summary version of their audit log through assisted channels, without charge.

7.3.5 Phase Two Annotation to Audit logging of access and use

- (a) In its submission relating to the Bill, the Consumers Health Forum of Australia noted that there was support for consumers to learn the identity of health practitioners who have accessed their record.¹⁹⁰ As we understand the design of the PCEHR System, such information will be able to be obtained from the System Operator if there is a concern about unauthorised use of the PCEHR (see section 7.3 of this Report).

7.4 External audit

- (a) The Audit Service will identify who has accessed the services, what they accessed, when they accessed it and what authorisation they obtained in order to access it.
- (b) The purpose of the audit log is to create a record of all PCEHR System activity to support a range of purposes, including benefits evaluation, capacity planning and monitoring unauthorised access.
- (c) Where the audit log is made available to a consumer, the purpose of the audit log is to provide comfort to the consumer that their PCEHR has been accessed appropriately. We understand that not all information recorded on the audit log may be made available to consumers, to prevent consumers from viewing extraneous information.¹⁹¹
- (d) Key functions of the audit service include:
- (i) add audit entry;
 - (ii) access audit trail summary;
 - (iii) request full audit trail;
 - (iv) archive old audit trail entries; and
 - (v) perform rule-based analysis of audit trail.¹⁹²
- (e) Recording of information in the audit log will be triggered:
- (i) each time a user enquires as to whether a PCEHR exists;
 - (ii) each time access has been attempted (successfully or otherwise);
 - (iii) each 'view' of a PCEHR (which could include downloading);
 - (iv) each time data is added or 'uploaded' or indexed to the PCEHR; and
 - (v) each time a change is made to the consumer's access controls.
- (f) The audit log will record the following information:
- (i) the PCEHR which was accessed (including IHI, name, sex and date of birth);
 - (ii) the Date and time that access was obtained (UTC Time);

¹⁹⁰ Submission in relation to the Bill dated November 2011, page 13

¹⁹¹ Response from NEHTA dated 25 August 2011

¹⁹² Con Ops, section 6.4.4 (Audit Service)

- (iii) the user's name;
 - (iv) the user's role (eg 'self', 'authorised representative', 'nominated representative', 'system operator', HPI-O role, etc.);
 - (v) the system they used to access the PCEHR (eg consumer portal, conformant portal, provider portal, CSP, clinical system, etc.);
 - (vi) in the case of access by a healthcare organisation, the HPI-O for the participating organisation and the HPI-O accessing organisation (where the HPI-O is different from the participating organisation's HPI-O);
 - (vii) whether the PCEHR was accessed using the consumer's PACC, a Transferrable Access Key (**TAK**), by override (emergency or forgotten PACC) obtained by the healthcare provider, representative using the consumer portal, etc; and
 - (viii) details of what was accessed, including information about the action (eg create, read, update, delete) and the item accessed (records, view, personal data, etc.).
- (g) The audit trails will be accessible by both consumers and providers. Based on who is accessing the audit trail, the view will differ as follows:
- (i) consumers (and their representatives) will only be able to see the audit trail relating to their PCEHR. Consumers (and their representatives) will not be able to see the names of Authorised Users (only their role, and the organisation through which they accessed the record). If the consumer wishes to know who accessed their information, they will need to formally request this information from the System Operator;
 - (ii) healthcare providers will only be able to see their own activity in the audit trail via the Provider Portal;
 - (iii) the OMO will be able to see any activity relating to their organisation via the B2B Gateway; and
 - (iv) the CSP and registered portal operator will be able to see any activity relating to their service via the B2B Gateway.

7.4.1 Audit: representatives

- (a) If the nominated representative or healthcare provider does not have access to 'limited access' information (see Con Ops, section 5.5.3), then any audit trail entries related to limited access information will not be visible.
- (b) The information in the audit trail will be utilised in two ways:
 - (i) real time audit rules, based on regularly updated common patterns of misuse, will constantly monitor index usage and notify appropriate parties of a potential breach; and
 - (ii) any user who is authorised to access a consumer's records, including the consumer, authorised representatives and healthcare providers, will be able to request a summary of the audit trail to ensure that access was appropriate.
- (c) If it is suspected that the information has been used inappropriately, it would be escalated to the appropriate body for investigation.

- (d) Information within the audit trail will be retained in accordance with the retention policies described in the Con Ops, section 4.2.4.¹⁹³

7.5 Accountability of the System Operator

7.5.1 Auditing the System Operator and its employees

- (a) We understand that the System Operator is likely to be a body defined as an 'agency' within the meaning of the Privacy Act, s 6 (Definitions).¹⁹⁴
- (b) We have not received information relating to the internal auditing services proposed for the System Operator. However, we note that the System Operator may request an independent audit of data in the PCEHR System.¹⁹⁵
- (c) The System Operator will be responsible for supplying operational capabilities around:
 - (i) Channel Management of the consumer and provider portal, administration portal and the B2B gateway;
 - (ii) management of core services, such as the participation and authorisation service, index and view service, report service, audit service and contact management service;
 - (iii) management of the National Repositories Service; and
 - (iv) supply of operational capabilities around service support, service delivery, infrastructure management, security management, application management, asset management and corporate services (such as HR and finance).
- (d) We understand that the System Operator's employees will mainly perform these roles and functions. The performance of these functions is likely to provide the System Operator's employees with wide access to certain parts of the PCEHR System, including consumer's records. This is particularly relevant for employees participating in the delivery or management of any of the core services described above.
- (e) It will be important to have arrangements in place to ensure that PCEHR records are protected from both external *and internal* unauthorised access. It is generally accepted that unauthorised access by a 'rogue' employee presents a higher risk to an organisation rather than an external threat, mainly because employees tend to have better knowledge of the system and are more likely to know where to locate the information they wish to access.
- (f) Internal unauthorised access can be divided into two categories:
 - (i) deliberate misuse or theft of data; and
 - (ii) accidental or inadvertent disclosure of data.
- (g) For the consumer, the distinction can be irrelevant from a practical perspective, as the net result will be the same – personal information ends up in the wrong hands and a privacy breach may have occurred.

¹⁹³ Con Ops, section 5.7 (Audit)

¹⁹⁴ Email from the Department dated 13 September 2011

¹⁹⁵ Con Ops, section 7.4.3 (Data quality)

- (h) However, different strategies should be employed to deal with the two different sets of issues, and therefore the distinction is useful when dealing with employees and unauthorised access.¹⁹⁶
- (i) Whilst it is extremely difficult (if not impossible) to eliminate the possibility of unauthorised access by rogue employees, there are a number of mitigation strategies that can be used to reduce the risk of an internal unauthorised access. These issues are the appropriate focus for an independent Threat and Risk Assessment, and a corresponding assessment of the information security classification for data to be held or accessible by the System Operator.

7.5.2 Privacy risks

- (a) We note that the Department has received previous advice on ensuring a privacy management framework is in place for the System Operator, and therefore we do not propose to revisit that topic in any detail in this report.
- (b) We further note that there are a number of mitigation strategies that can be used to improve accountabilities and reduce the risk of privacy breaches affecting data held by the System Operator. These issues are the appropriate focus for an assessment of the information security classification for data to be held (or accessible) by the System Operator, and a corresponding independent Threat and Risk Assessment of the security controls proposed as a result.
- (c) One issue worthy of further consideration is the risk that if data storage is outsourced to a provider with a business presence in the USA, the US Government may be able to force the provider to disclose personal information stored in Australia without reference to the System Operator or the subject consumer/s.¹⁹⁷

7.5.3 Recommendations

- 7.6 That prior to finalisation of operational plans for the System Operator, there should be an assessment of the information security classification for data to be held by the System Operator, and data when in transit to or from the System Operator, and a corresponding independent Threat and Risk Assessment of the security controls proposed as a result.
- 7.7 That the Threat and Risk Assessment examine the adequacy of legislative or other protections against the risk of exposure of consumers' personal information to foreign law enforcement bodies.
- 7.8 That the Threat and Risk Assessment be reviewed by the Department's privacy team in conjunction with this and any other PIA reports.

7.5.4 Phase Two Annotation to Auditing the System Operator

- (a) In its submission relating to the Bill, the Australian Privacy Commissioner proposed that the Information Commissioner should be able to compulsorily audit the information handling practices of the System Operator in the same way as it can in relation to compliance with Information Privacy Principles.¹⁹⁸ In our view this would be a privacy positive approach that is consistent with the approach adopted for the Information

¹⁹⁶ Nick Gifford, *Information Security: Managing the Legal Risks*, page 43

¹⁹⁷ See 'Google admits Patriot Act requests; Handed over European data to U.S. authorities', at <http://www.zdnet.com/blog/igeneration/google-admits-patriot-act-requests-handed-over-european-data-to-us-authorities/12191>

¹⁹⁸ Submission dated October 2011 page 8

Commissioner to audit an act or practice that may be an interference with the privacy of an individual under s 29(1) of the HI Act.¹⁹⁹ Whether such audit is performed by the Information Commissioner or the Federal Auditor-General is a matter outside the scope of this report. Otherwise it would be prudent for the Department and the Information Commissioner to have a common understanding as to whether the Bill does indeed vest necessary compulsory audit powers in the Information Commissioner.

¹⁹⁹ See section 27A of the Privacy Act

Chapter 8 - Governance of the broader PCEHR System

8.1 Ensuring enforceable privacy responsibilities for participants

8.1.1 Introduction

- (a) A set of robust and uniform legislation-based privacy rules should apply to the PCEHR System, because existing health privacy laws will otherwise impede the effective cross border operation of the system. The need for a set of 'PCEHR privacy rules' stems from a number of features of the existing privacy regime:
 - (i) SA and WA do not have in place enforceable privacy regime equivalent to those in other States and Territories;
 - (ii) inappropriate 'viewing' of health information is not contrary to NSW privacy law; and
 - (iii) vicarious liability will not apply to employers under NSW and Victorian privacy law.
- (b) We suggest that a solution is best enforced by adopting a model similar to that applied under the HI Act. This chapter sets out the scope of the rules and detailed recommendations.

8.1.2 The need for a set of privacy rules

- (a) The great benefit of the PCEHR System is that it breaks down jurisdictional boundaries for the sharing of health information. However in the absence of a robust framework for the protection of that information, this also creates a significant risk.
- (b) The Australian Privacy Commissioner has noted that:

'the absence of clearly stated privacy protections in PCEHR legislation may make it difficult for consumers to understand the privacy protections that will apply to personal information included in the PCEHR. In turn, this may reduce consumers' ability to make an informed choice about participation in the PCEHR System.'

Moreover, the PCEHR System will transform the way in which health information is shared across jurisdictions. Consumers' health information will be much more easily transferred between, and accessible to, individual healthcare providers, healthcare provider organisations and operators located across Australia. Consumers will therefore have an interest in consistent privacy protections applying to their health information within the PCEHR System, irrespective of where it is uploaded to the system, or accessed from the system.²⁰⁰

²⁰⁰ Submission from Timothy Pilgrim, Australian Privacy Commissioner of the Office of the Australian Information Commissioner, relating to the Legislation Issues Paper, August 2011, pages 13-14

- (c) The nature of privacy protection in Australia is often described as ‘patchwork’. In relation to public sector participants in the PCEHR Scheme in particular, there are currently stark differences in the degree to which privacy rights for the health consumer exist, are enforceable, or offer a remedy to the victim of a privacy breach.
- (d) For example, the victim of a privacy breach involving a NSW public hospital can seek to have an independent tribunal enforce statutory privacy principles against that hospital, and can obtain up to \$40,000 compensation for harm they suffered as a result of a proven breach of those principles. If the hospital were in Victoria the victim could potentially obtain up to \$100,000 in compensation. Yet in South Australia the privacy principles are not based in statute and cannot be enforced by a consumer.
- (e) The applicable privacy laws of NSW, Victoria, Tasmania and the Northern Territory recognise the differing levels of privacy protection offered to consumers in other jurisdictions. They each seek to address this situation by prohibiting the disclosure of health information outside their respective State or Territory, unless it is to a jurisdiction with ‘equivalent’ privacy laws, or the health consumer’s consent is first obtained (see NSW HPP 14, Vic HPP 9, Tas PIPP 9 and NT IPP 9). This is generally interpreted to mean, for example, that a healthcare provider in NSW could disclose a consumer’s health information to a fellow healthcare provider in Victoria, Tasmania or the Northern Territory, but not to one in South Australia – at least not without seeking the consumer’s specific and informed consent.
- (f) In the context of what might be termed ‘one-off’ transfers of health information, this case-by-case approach to ensuring that privacy protection ‘travels’ with the health information is workable, if not ideal. However in the context of a shared e-health record, in which healthcare providers are expected to ‘upload’ health information to the consumer’s PCEHR (ie ‘disclose’ health information to other, unknown future users of that PCEHR) as a matter of routine practice, the absence of a uniform system of privacy protection is more problematic.
- (g) Without legislative authorisation, our view is that healthcare providers in NSW, Victoria, Tasmania and the Northern Territory, both in the public and private sectors, will not be able to add health information to the PCEHR without the consumer’s consent to each upload. (The situation for healthcare providers in NSW is further reinforced by HPP 15, which requires the consumer’s express consent to ‘include health information about an individual in a health records linkage system’.)
- (h) Requiring a consumer’s specific consent to each upload of information to the PCEHR is a more onerous ‘consent model’ than that proposed for the PCEHR System, which is intended to operate on the basis of ‘opt in’ (express consent) to having a PCEHR in the first place, but then ‘opt out’ (implied consent unless the consumer says otherwise) to each upload of information.
- (i) Rather than suggest that the ‘consent model’ for the entire PCEHR System be changed, we suggest instead addressing the problem that the NSW, Victorian, Tasmanian and Northern Territory privacy laws intend to address, by ensuring that privacy protections ‘travel with’ the health information. That is, we suggest that as far as is legislatively possible, healthcare users of the PCEHR System should be bound by a set of robust and uniform privacy obligations in relation to how they use a consumer’s PCEHR.

- (j) In essence, we are recommending that a trade-off be made. In return for relaxing the restrictions created by the privacy provisions applying in NSW, Victoria, Tasmania and the NT, which would otherwise pose a barrier to participation in the PCEHR System, all non-consumer users of the PCEHR System ought be governed by a robust and uniform set of privacy 'rules', against which the consumer can seek an enforceable remedy in the case of a breach causing harm. This suggestion is consistent with the ALRC's recommendation that enabling legislation for a shared EHR should address information privacy issues including 'permitted and prohibited uses and linkages of the personal information held in the systems', a recommendation which has been accepted in principle by the Australian Government.²⁰¹

8.1.3 Scope of the proposed set of privacy rules

- (a) In order to minimise the regulatory burden on participants, we suggest that the set of 'PCEHR privacy rules' be broadly consistent with, although more specific than, the NPPs. This would also have the benefit of providing some clear guidance for users about their obligations, rather than relying on existing privacy principles which are drafted in more general terms and thus subject to differing interpretations when applied in practice.
- (b) For example, NPP 2.1 states:
- 2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:*
- (a) both of the following apply:*
- (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;*
- (ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose ...*
- (c) A set of more specific privacy 'rules' for the PCEHR System could serve to clarify the above obligation, without necessarily displacing it, by setting it within the context of the PCEHR. It could for example set out precisely what is considered to be the primary purpose of use of a consumer's PCEHR (such as treatment or care of the consumer), as well as authorised secondary purposes (such as treatment follow-up, referral, billing, audit or program evaluation).
- (d) The specific rules could also clarify that the primary purpose justifies view, use or disclosure 'only so far as is necessary for the provision of that health service', so as to prevent inappropriate view of the PCEHR after the period of care has ended.²⁰²
- (e) PCEHR-specific privacy rules could also for example clarify that the disclosure provision prohibits a healthcare provider from uploading a record to the PCEHR when the consumer has requested them not to. They could also for example state that there should be no disclosures made from the PCEHR to next-of-kin for 'compassionate reasons', instead requiring healthcare providers to disclose information only from their local records, or refer the family to consumer's nominated healthcare provider for the SHS.

²⁰¹ Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC Report 108, 2008, Recommendation 61-1

²⁰² See for example the harm involved in post-care access to a consumer record in *NK v Northern Sydney Central Coast Area Health Service (No.2)* [2011] NSWADT 81

- (f) We therefore suggest that the 'PCEHR privacy rules' encompass:
 - (i) authorised purposes for searching for or 'viewing' information from a PCEHR;
 - (ii) authorised purposes for copying or 'downloading' information from a PCEHR;
 - (iii) authorised purposes for using information from a PCEHR (whether or not it has been copied or downloaded first);
 - (iv) authorised purposes for adding or 'uploading' information to a PCEHR;
 - (v) obligations to take reasonable steps in the circumstances to protect the data security of the PCEHR; and
 - (vi) obligations to take reasonable steps in the circumstances to ensure the data quality of information added or 'uploaded' to the PCEHR.

8.2 Ensuring enforceable privacy rights for consumers

8.2.1 Enforcement of the proposed set of privacy rules

- (a) In terms of enforcement of the proposed 'PCEHR privacy rules', we suggest an approach modelled on the enforcement of the HI Act.
- (b) The HI Act sets out some authorised uses of an IHI (s 24), and then effectively provides that any other type of use is both a criminal offence (s 26) and an 'interference with privacy' under the Privacy Act (s 29). The 'interference with privacy' provision means that a complaint about a breach of the HI Act triggers the Australian Privacy Commissioner's investigative and conciliation powers, even if the respondent organisation is a State government agency. This provides a clear pathway for the victim of a breach to seek a civil remedy for any harm they have suffered, and ensures uniformity of privacy regulation across all participants.
- (c) We therefore suggest that the proposed 'PCEHR privacy rules' incorporate an enforcement mechanism which provides that a contravention of those rules is an 'interference with privacy' under the federal Privacy Act - and, if the contravention was deliberate, also a criminal offence.

8.2.2 Why not just rely on the HI Act?

- (a) It has been suggested that misuse of a PCEHR would in itself involve a misuse of an IHI (since the IHI is the 'key' to access a PCEHR in the first place), and thus the HI Act could already provide a solution. However we suggest that not all potential privacy harms involving a PCEHR would necessarily involve misuse of the consumer's IHI.
- (b) The types of privacy harms we suggest should be subject to clear, uniform and enforceable obligations include:
 - (i) an Authorised User searching for or viewing a PCEHR they should not (eg looking up the PCEHR of someone who is not in their current care);
 - (ii) an Authorised User viewing a PCEHR that was opened legitimately, but for a purpose that is not legitimate (eg the consumer is in the care of a colleague, but the user is not actually involved and the user is looking at their colleague's computer);
 - (iii) an Authorised User viewing a PCEHR legitimately, but then misusing or disclosing their data in some unauthorised way (eg the consumer is the user's care, but the user discloses information about them to the media);

- (iv) poor data quality practices (eg a healthcare provider being negligent in the way they write or upload data to a PCEHR, such that the PCEHR becomes inaccurate or misleading); and
 - (v) poor data security (eg a healthcare provider being negligent in the way they allow their staff to share log-ins, or have the computer screen viewable in a public waiting room).
- (c) Relying on the HI Act alone would cover the first scenario listed above, because to get to that point the authorised user would first have to misuse the consumer's IHI. However the misuse provisions of the HI Act would not cover the other four scenarios.

8.2.3 Avoiding duplication

As is the case now, complainants may have a choice of jurisdiction in which to pursue their privacy complaint. There are existing legislative and administrative mechanisms in place to prevent complainants from 'double-dipping' (see eg s 41(1)(e) of the Privacy Act). We suggest that these arrangements should continue.

8.2.4 Why not make participation by SA and WA contingent on adoption of the NPPs?

- (a) An alternative approach to the problem of the 'patchwork' nature of privacy protection in Australia would be to instead require the South Australian and Western Australian public health providers to 'opt in' to the NPPs. This would address the problem of the most obvious 'gap' in the patchwork regime of privacy protection, but we believe such an approach would be more onerous for those two States than the model we are proposing, which is limited to use of the PCEHR System. Such an approach would also not address the lack of uniformity in enforcement methods and remedies available across the different jurisdictions.
- (b) There are further weakness in the existing 'patchwork' of privacy protections across Australia, the exposure of which could impact on community expectations of the PCEHR System. For example, the interpretation of the NSW privacy principles to date suggests that the act of 'viewing' health information from a PCEHR on a screen, without downloading a copy into the healthcare provider's own record-keeping systems, might not constitute a 'use' of the information by the user, such as to trigger their privacy obligations.²⁰³
- (c) There is therefore the potential for misuse of the PCEHR without any corresponding penalty for the person who misuses the information, or any remedy for a person who suffers harm as a result. There are further weaknesses in the NSW and Victorian health privacy laws, in the extent to which respondent organisations can avoid responsibility for providing a civil remedy to the victim of a privacy breach if the user responsible for the breach acted improperly.²⁰⁴
- (d) Including a set of specific 'PCEHR privacy rules' as we have proposed is intended as a solution to the 'patchwork' problem which poses the least compliance burden on the SA and WA government healthcare providers, and addresses the weaknesses found to date in NSW and Victorian privacy laws.

²⁰³ *Director General, Department of Education and Training v MT (GD)* [2005] NSWADTAP 77; and *JD v Department of Health (GD)* [2005] NSWADTAP 44

²⁰⁴ See eg *Director General, Department of Education and Training v MT* [2006] NSWCA 270

8.2.5 Recommendations

- 8.1 That the PCEHR Bill include a set of 'PCEHR privacy rules' governing all non-consumer users of the PCEHR System, which should encompass:
- (a) authorised purposes for searching for or 'viewing' information from a PCEHR;
 - (b) authorised purposes for copying or 'downloading' information from a PCEHR;
 - (c) authorised purposes for using information from a PCEHR (whether or not it has been copied or downloaded first);
 - (d) authorised purposes for adding or 'uploading' information to a PCEHR;
 - (e) obligations to take reasonable steps to protect the data security of the PCEHR; and
 - (f) obligations to take reasonable steps to ensure the data quality of information added or 'uploaded' to the PCEHR.
- Note:** We have used the term 'privacy rules' here simply to distinguish our proposal from existing 'privacy principles'. Terms such as 'privacy protocol' or 'privacy standards' may be equally appropriate.
- 8.2 That the 'PCEHR privacy rules' incorporate an enforcement mechanism which provides that a contravention of those rules is an 'interference with privacy' under the federal Privacy Act - and, if the contravening conduct was intentional, also a criminal offence.
- 8.3 That the 'PCEHR privacy rules' cover conduct relating to information gained from a PCEHR by an authorised user of a PCEHR. The scope of regulated conduct should not be limited to conduct done 'in the performance of their duties' (cf s 8(1) of the Privacy Act), and there should be no exception allowing use of the information gained from a PCEHR for 'personal, family or household affairs' (cf s 26(2)(c) of the HI Act). That is, the obligations must extend to the misuse of information by a 'rogue' employee, agent or contractor, who uses or discloses information from a PCEHR for their own, unauthorised purposes. The obligations must also extend to the recipient of information gained from a PCEHR by an authorised user of a PCEHR, so as to ensure that it is an offence for a third party to use or disclose information from a PCEHR which was improperly obtained.
- 8.4 That the 'PCEHR privacy rules' provide that in the case of an alleged contravention, the respondent to a complaint to the Privacy Commissioner shall be the employing organisation, rather than the individual employee, agent or contractor (see s 8(1) of the Privacy Act).
- 8.5 That the criminal penalties for intentional contravention of a 'PCEHR privacy rule' should be as per s 26(1) of the HI Act, namely a maximum two years imprisonment and/or 120 penalty units. Criminal penalties may be applicable to an individual employee, agent or contractor, or to a corporate person.
- 8.6 That the PCEHR Bill authorise healthcare providers to disclose personal information and health information to a PCEHR, such as to authorise non-compliance with NSW HPP 14 and 15, Vic HPP 9, Tas PIPP 9 and NT IPP 9.
- 8.7 That when the draft forms and terms and conditions (versions relating to each of the access channels) are completed, the forms and terms and conditions be reviewed for IPP/NPP compliance.

8.2.6 Phase Two Annotation to Recommendation 8.1

- (a) In his submission relating to the Bill, the Australian Privacy Commissioner proposed that portal operators be subject to the Privacy Act in the same way as a repository operator (on the assumption that such operators are authorities or instrumentalities of a State or Territory).²⁰⁵ We note that information stored within a registered portal operator is treated as a separate record from the PCEHR System and that it is only upon the portal operator loading the information into the PCEHR System that the consumer's information will become part of the PCEHR System and so be subject to the PCEHR Bill.²⁰⁶ Until that point the consumer's information will be subject to the applicable privacy and health information laws that apply to the portal operator's local system.
- (b) The Privacy Commissioner also recommends that the Bill be amended to ensure that privacy protections apply once health information is downloaded from the PCEHR System rather than relying on the application of existing privacy and health laws which may not in fact exist or apply in a particular jurisdiction.²⁰⁷ Recommendations 8.1 and 8.2 of this report would provide a mechanism to ensure national uniformity in regulating use of health information through the PCEHR System.

8.2.7 Phase Two Annotations to recommendation 8.3 (Ensuring enforceable privacy rights for consumers)

- (a) In its submissions to the Bill, The Royal Australasian College of Surgeons (**the College**) raised concerns that the Bill will have the effect of expanding employer responsibility for the deliberate wrongdoings of their employees to the detriment of employers, insurer, specialists, patients and taxpayers that ultimately may inhibit support for PCEHR by clinicians.²⁰⁸
- (b) We do not see that Division 4 of the Bill (Treatment of Certain Entities) has this effect. We note however that s 83 of the Bill effectively makes a body corporate employer vicariously liable for civil penalties where the employee has acted within the 'actual or apparent scope of his or her employment' or within the employer's 'actual or apparent authority'.
- (c) It would seem that in relation to a complainant pursuing other remedies the approach relating to vicarious liability under the Privacy Act applies so that the employer will be liable for unauthorised use of the consumer's health information in a PCEHR if the employee acted in the performance of the duties of the employee's employment (see s 65 of the Bill and s 8(1) of the Privacy Act). To that extent the Bill does not expand the employer's liability. We note however that this result does not go so far as proposed in Recommendation 8.3. We note that in its submission in relation to the Bill The Royal Australasian College of Physicians supported the position that an employer should not be held responsible if it took reasonable steps to prevent employees or contracted healthcare providers from committing a breach of the Bill.²⁰⁹

²⁰⁵ Submission dated October 2011 page 12

²⁰⁶ Final Concept of Operations Section 3.4.3

²⁰⁷ Submission dated October 2011 pages 13-14

²⁰⁸ Submission dated 28 October 2011 pages 2-3

²⁰⁹ Submission dated October 2011 page 3

8.2.8 Phase Two Annotations to recommendation 8.3 (Ensuring enforceable privacy rights for consumers)

(a) In their submissions to the Bill, the Australian Privacy Foundation²¹⁰ and the Medical Software Industry Association²¹¹ raised a concern that the Bill effectively exempts Governments for any contravention of the Bill.

(b) Section 7 of the Bill deals with how the legislation applies to the Crown:

7 Act to bind the Crown

(1) *This Act binds the Crown in each of its capacities.*

(2) *This Act does not make the Crown liable to be prosecuted for an offence or liable to a pecuniary penalty.*²¹²

(c) Government Agencies are bound by the Bill. If the Crown were liable to pay a pecuniary penalty there would be no practical effect because it would be just one arm of the Commonwealth transferring funds to another. However there is other legislation in which Government agencies are held liable to prosecution and payment of a pecuniary penalty (see for example s 10 of the *Work Health and Safety Bill 2011*).

(d) The comments in submissions regarding this point emphasise a legitimate concern that the community expects adequate enforcement measures be in place to safeguard the privacy rights of consumers. There are of course enforcement measures applicable to the System Operator that is a Commonwealth agency (potential actions under Section 70 of the Crimes Act 1914 (Cth), defective administration scheme, judicial review etc). However they are not necessarily the same as will apply to other participants in the PCEHR System. It is not within the scope of Phase Two of this report to consider whether such other enforcement measures are adequate or consistent with the measure proposed in the Bill. Nevertheless we do recommend that:

(i) the Department assess whether the enforcement regime applicable to the System Operator for a breach of the Bill is no less effective than would apply under the Bill for other participants and if not, amend the Bill appropriately; and

(ii) the other enforcement measures are clearly communicated to all participants in the PCEHR System.

(e) As noted in the Companion document to the Bill the Australian Government is currently considering whether Federal legislation should be passed to support a right of an individual to sue another for invasion of privacy for an award of damages or other remedy.

(f) Otherwise the Bill relies upon the enforcement regime under the Privacy Act under which the Information Commissioner may make a determination²¹³ and other remedies available under concurrent legislation and common law (such as breach of confidence).

(g) Given the concerns raised in a number of submissions regarding the Bill we recommend that the Explanatory Memorandum and communications relating to the PCEHR System describe those alternative remedies.

²¹⁰ Submission to the exposure draft PCEHR Bill 2011 from the Australian Privacy Foundation, submitted 27 October 2011, page 3, clause 4

²¹¹ Submission dated 28 October 2011 re section 7 of the Bill

²¹² See also: PCEHR System: Exposure draft legislation Companion Guide, section 3.1 (Part 1 – Preliminary).

²¹³ Such determination may include that a person pay compensation to the complainant. Determinations can be enforced through relevant Courts.

- (h) The Australian Privacy Foundation also requested that penalties apply to unintentional breaches of community information linked by the PCEHR System.
- (i) The civil penalty provisions are designed to ensure that liability does not arise where there is inadvertent or mistaken access to a person's PCEHR.²¹⁴ This policy position is supported by previous inquiries into the issue:
 - (i) The ALRC rejected a suggestion that an action for breach of privacy should be brought for negligent or accidental invasions of privacy.
 - (ii) The ALRC agreed with an earlier view expressed by the New South Wales Law Reform Commission (NSWLRC) that including accidental or negligent acts 'would, arguably, go too far'.²¹⁵
- (j) Imposing penalties and liability for inadvertent or mistaken breaches may reduce the provider's willingness to participate in PCEHR due to the onerous nature of compliance.

Notification of Data breaches

- (k) In its submission in relation to the Bill the MSIA raised a concern as to whether the System Operator should be under an obligation to notify the consumer of any applicable breaches of the Bill rather than merely having to 'consider whether to so notify the consumer (see s 67(4)(c) and (d))'²¹⁶. The OAIC, Consumers Health Forum of Australia²¹⁷ and NSW Council for Civil Liberties also made reference to this issue in their submission relating to the Bill.
- (l) The Australian Privacy Commissioner also considered it appropriate that the entities handling a consumer's health information other than repository operators or portal operators (such as healthcare provider organisations) should be obliged to notify the System Operator of known breaches.
- (m) Whilst the Privacy Act does not expressly require an agency or organisation to notify individuals if personal information is subject to a breach of information security safeguards, from the perspective of managing privacy risk, the preferable outcome would be for the consumer to be notified of the data breach as reasonably practical so that (to paraphrase the OAIC) control over the personal information can be restored to the consumer. The benefits of this approach are well set out in the OAIC's *Guide to Handling Personal Information Security Breaches (the Guide)* as the best practice approach to determine whether to notify the individual of a breach of data security safeguards.
- (n) On balance we are of the view that s 67(4)(c) and (d) the Bill should be amended to qualify the discretion given to the System Operator as to when it notifies the consumer of the breach by invoking reference to the Guide (as amended from time to time). This would maintain consistency with the approach under the Privacy Act whilst providing guidance to consumers about how the System Operator will deal with applicable breaches.

²¹⁴ PCEHR System: Exposure draft legislation Companion Guide, section 3.4.1 (Division 1 – Unauthorised collection, use and disclosure of health information included in a registered consumer's PCEHR)

²¹⁵ Australian Law Reform Commission, *Report 108 – For Your Information: Australian Privacy Law and Practice* (2008) at 2577 citing NSWLRC, *Invasion of Privacy Consultation Paper 1* (2007) at [7.24]

²¹⁶ Submission dated 28 October 2011 page 10

²¹⁷ Submission in relation to the Bill dated November 2011, page 13

8.3 Complaint handling

- (a) We understand that in the first instance, consumers would raise any enquiries or complaints about the privacy of the PCEHR with the System Operator, and that if they are not satisfied with the response from the System Operator, the complaint can be escalated to an appropriate investigative body.
- (b) Which investigative body or bodies that should be has been the subject of consultation and public submissions. We suggest that the Australian Privacy Commissioner is a logical starting point, but that complainants should be able to choose another regulator instead of (but not as well as) the Australian Privacy Commissioner.
- (c) We suggest that the complaint handling process should have the following features:
 - (i) clear communications to consumers about their privacy 'rights', and the privacy 'rules' which participants in the PCEHR System must follow;
 - (ii) a clear, easily communicated pathway for complainants to follow to escalate their complaint;
 - (iii) the System Operator the 'first port of call' for a privacy complaint;
 - (iv) a reasonable time limit for the commencement of complaints with the System Operator, such as 12 months from the time the complainant became aware of the conduct and aware that the conduct could be complained about;
 - (v) the System Operator to have legislated power to disconnect or revoke the access of an authorised representative, ARA, registered portal operator, registered repository operator or HPI-O; or to compel an HPI-O to disconnect or revoke the access of a specific user;
 - (vi) the Australian Privacy Commissioner as the 'second port of call' for a privacy complaint - escalation to be by either the complainant or the System Operator, within a set time period;
 - (vii) the Australian Privacy Commissioner to be adequately resourced to manage any additional workload expected to arise from implementation of the PCEHR System;
 - (viii) the Australian Privacy Commissioner to have legislated power to compel the System Operator to exercise its powers to disconnect or revoke the access of an individual or organisation;
 - (ix) the Australian Privacy Commissioner to advise the complainant if their complaint would be better pursued in another jurisdiction or with a different regulator (eg the Victorian Health Services Commissioner);
 - (x) flexibility to allow complainants to pursue their complaint with a different regulator should they so choose (eg a complainant may instead seek to take action under the NSW HRIP Act because they believe it will be a faster way to secure an enforceable remedy);
 - (xi) State and Territory-based legislation or protocols to allow some flexibility in the application of time limits, so that time limits in other jurisdictions do not start to 'run' until the Australian Privacy Commissioner has advised the complainant of their option to lodge their complaint in that other jurisdiction; and

- (xii) the Australian Privacy Commissioner to exercise existing powers and protocols to ensure complainants cannot 'double dip' (ie a complaint cannot be pursued in more than one jurisdiction).

8.3.1 Recommendations

- 8.8 That the PCEHR Bill provide for a complaint-handling process with clear time limits and pathways, which commences with the System Operator and can then be escalated, by either the complainant or the System Operator, to the Australian Privacy Commissioner.
- 8.9 That the PCEHR Bill not exclude complainants from lodging a complaint or seeking a remedy in any other forum.
- 8.10 That the PCEHR Bill include an obligation on the System Operator to report any data security breaches and any evidence of internal misuse of PCEHR data to the Australian Privacy Commissioner.
- 8.11 That the PCEHR Bill provide the System Operator with the power to disconnect or revoke the access of an authorised representative, ARA, registered portal operator, registered repository operator or HPI-O; or to compel an HPI-O to disconnect or revoke the access of a specific user.
- 8.12 That the PCEHR Bill provide the Australian Privacy Commissioner with the power to compel the System Operator to exercise its power to disconnect or revoke the access of an individual or organisation.
- 8.13 That the Department encourage State and Territory governments to ensure legislation or protocols allow some flexibility in the application of time limits in their jurisdictions, so that their time limits do not start to 'run' until the Australian Privacy Commissioner has advised a complainant of their option to lodge their complaint in that other jurisdiction.
- 8.14 That the Australian Privacy Commissioner to be adequately resourced to manage any additional workload expected to arise from implementation of the PCEHR System
- 8.15 That consumer communications clearly articulate to consumers their privacy 'rights', the privacy 'rules' which participants in the PCEHR System must follow, and the complaint-handling process.

8.3.2 Phase Two - Annotations to recommendation 8.9 (Complaints handling procedures)

- (a) In his submission to the Bill, the Acting Privacy Commissioner of NSW proposes that the PCEHR legislative regime apply to the PCEHR participants so as to displace the existing privacy obligations but only to the extent that they relate to the PCEHR System. The Acting Privacy Commissioner of NSW says this would overcome potential unfair inconsistencies in results determined by different privacy forums dealing with similar circumstances and in the handling of complaints by the various privacy regulators.²¹⁸ SA Health also raised a concern about overlap between the Bill and other health information legislation that contain complaint mechanisms.²¹⁹
- (b) It is fair to say that such inconsistencies may arise under the complaint processes envisaged by the Bill and that consequent actual or perceived unfairness may be a risk that community expectations for maintaining privacy safeguards are not met.

²¹⁸ Submission from the Office of the Privacy Commissioner (NSW) dated 28 October 2011, page 3

²¹⁹ See Submission by SA Health dated 26 October 2011 page 5.

- (c) This privacy risk must be balanced by the positive privacy impact that arise under the proposed complaints process. As is the case now, it remains open to the consumer, who is the person whose interests have been adversely affected, to choose the forum that best suits him or her rather than be 'forced' to a forum that might be the slowest or offer the least beneficial result.
- (d) In our view it would be prudent for the Government to maintain a watching brief on this issue and if appropriate, consider any eventuating privacy risk at the time of the review of the Act in accordance with s 96 of the Bill.

8.3.3 Phase Two Annotation to Recommendations relating to Complaint Handling

- (a) In his submission relating to the Bill the Australian Privacy Commissioner proposed that the Bill be amended to clarify that the Information Commissioner may undertake own motion investigations in relation to possible contravention of the civil penalty provisions.²²⁰ In our view this would be privacy positive in building confidence in the PCEHR System and System Operator.
- (b) The Australian Privacy Commissioner also proposed that the Bill make it clear that the consumer should lodge a complaint to the System Operator in the first instance and then escalated to a privacy regulator.²²¹ This supports the discussion in paragraph 8.3(c)(iii) of this Report.

8.4 Obligations of participating organisations

Accountability of, and public confidence in, the PCEHR System as a whole may be further enhanced by way of mandatory reporting to the Australian Privacy Commissioner.

8.4.1 Recommendation

8.16 That the PCEHR Bill include an obligation on ARAs, registered portal operators, registered repository operators and HPI-Os to report any data security breaches, and any evidence of internal misuse of PCEHR data, to the Australian Privacy Commissioner and the System Operator.

8.5 Data storage

- (a) We understand that the Department's intention is to require all repositories (and possibly also ARAs and registered portal operators) to store all PCEHR-related data in Australia, only access the PCEHR System from within Australia, and to be a registered legal entity in Australia.
- (b) As noted above in Chapter 7, this may not be enough to prevent the exposure of consumers' personal information to foreign law enforcement bodies, if the organisation storing the data also has a business presence in other countries such as the USA. We suggest that this risk be the subject of further consideration as part of a Threat and Risk Assessment of data security requirements.

8.5.1 Recommendation

8.17 That a Threat and Risk Assessment examine the adequacy of legislative or other protections against the risk of exposure of consumers' personal information, held by ARAs, registered portal operators, registered repository operators and HPI Os, to foreign

²²⁰ Submission dated October 2011 page 16

²²¹ Submission dated October 2011 page 19

law enforcement bodies.

8.5.2 Phase Two Annotation to Auditing the System Operator

- (a) The Australian Privacy Commissioner has also proposed that the Bill be amended to require contracted service providers that handle consumer's health information on behalf of a healthcare provider should also be located in Australia. We hold similar concerns and reiterate Recommendation 8.17.

8.5.3 Storage: National Repositories Service

- (a) The National Repositories Service does not consist of a single central data repository. It will consist of a number of nationally operated repositories.
- (b) The National Repositories Service will be able to store the following types of records:
 - (i) shared health summaries;
 - (ii) Event Summaries;
 - (iii) Discharge Summaries;
 - (iv) Specialist Letters;
 - (v) Consumer-Entered Health Summaries; and
 - (vi) Consumer Notes.²²²

8.5.4 Storage: registered repository operator Services

- (a) In addition to the National Repositories Service, the PCEHR System will have the capability to connect to other registered repository operators .
- (b) While the PCEHR System supports a diverse set of record types, the availability of the records from the registered repository operators will depend on the readiness of healthcare provider organisations to participate in the PCEHR Program. All records stored within the registered repository operators are based on a common set of 'templates', which specify the minimum set of data the record is required to support.²²³ Further information about the templates service is below.
- (c) Examples of registered repository operators may include:
 - (i) DHS operated repositories holding:
 - (A) Medicare history;
 - (B) PBS history;
 - (C) organ donor information; and
 - (D) childhood immunisation information;
 - (ii) Pathology service repositories holding Pathology Result Reports; and
 - (iii) Regional or State/Territory operated repositories.²²⁴

8.5.5 Data quality: Templates service

- (a) The Template Service provides a mechanism for sharing, storing, finding, retrieving and managing the lifecycle of templates. A template is used to provide metadata about each of

²²² Con Ops, section 6.6.1 (National Repositories Service)

²²³ Con Ops, section 4.3 (Clinical document types and templates)

²²⁴ Con Ops, section 6.6.2 (Conformant Repositories)

the major record types and includes data definitions, data validation rules, information about how to render a record and links to supporting material (such as implementation guides).

- (b) The PCEHR System uses the template service to ensure that the structure and semantics of different types of records stored within the PCEHR System are consistent with a common set of definitions.
- (c) Information can only be shared via the PCEHR System if it has an approved template and the data is valid for the data validation rules within the template. For example, a shared health summary cannot be loaded into the PCEHR System unless it meets the data validation rules within the template.
- (d) The PCEHR System also leverages the lifecycle management processes within the Template Service to help support governance over information that can be shared via the PCEHR System. New forms of information cannot be shared via the PCEHR System unless an approved template is available via the Template Service.
- (e) Over time, other eHealth applications may use the Template Service in time to publish new templates. For example, the Template Service could be used to publish a range of specialised referral templates.²²⁵

8.6 Protecting privacy into the future

- (a) The PCEHR System is designed to be 'built on over time' (Con Ops April 2011, part 2.7 (Scope)). Potential future enhancements might include pathology requests, diagnostic images, care plans, and data from consumer devices such as blood pressure monitors (Con Ops April 2011, part 2.7 (Scope)).
- (b) There is therefore a risk of function creep for the PCEHR System. The privacy messages given to consumers at the time of registration needs to recognise this potential.
- (c) In particular, draft consumer communications (required under NPP 1.3) should be carefully reviewed to ensure that consumers are well informed about what they are registering for and consenting to when they register for a PCEHR. Consumer communications should also be presented or communicated in ways that a variety of consumers can understand, such as people of a non-English speaking background, people with low literacy levels, consumers with physical or intellectual disabilities.
- (d) Privacy Commissioners around the world encourage the development of 'plain language' rather than 'legalistic' privacy notices. The use of 'layered' or 'short form' notices is a sensible way to communicate key information to the majority of consumers, and more detailed information to the minority who are concerned enough to seek further information. For resources on developing plain language, layered privacy notices, see:
 - (i) UK Information Commissioner, *Privacy notices code of practice*, 2010, at http://www.ico.gov.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications.aspx#notice;
 - (ii) ALRC, *For Your Information: Australian Privacy Law and Practice*, ALRC Report 108, 2008, part 24.75-89 and Recommendation 24-3, at <http://www.alrc.gov.au/publications/24.%20Openness/short-form-privacy-notices>; and

²²⁵ Con Ops, section 6.5.2 (Template Service)

- (iii) Resolution of the 25th International Conference of Data Protection and Privacy Commissioners, 2003, at <http://www.privacyconference2003.org/resolution.asp>.
- (e) Some types of health information such as 'infection status' carry particular privacy risks, the realisation of which may mitigate against the proposed health benefits to a consumer of having a PCEHR. For example, consumers with HIV may fear discrimination or stigma should their HIV status become more widely known, and in order to avoid this outcome, they may withdraw from the PCEHR scheme.
- (f) Withdrawal from the PCEHR could impact on their health outcomes if they have complex or chronic health conditions, the management of which the PCEHR would have otherwise assisted. For this reason, it has been generally accepted that protecting privacy in fact enhances health outcomes, rather than being seen as a 'barrier' to achieving health outcomes. Instead of 'flagging' consumers with particular infections, health policy in Australia has been to promote universal infection prevention controls.
- (g) We note that the Australian Medical Association supports the inclusion of a mandatory infection field status:

*'Given the high risk of medical practitioners being infected by their patients, and the flow on consequences to other patients, it is critical that the patient's infection status is a mandatory field in the PCEHR.'*²²⁶
- (h) We caution against the risk that over time, new types of data could be added to the PCEHR which could significantly impact on consumers' privacy concerns and expectations.
- (i) We suggest that a systematic process of on-going review and Parliamentary scrutiny can help to mitigate against the risk of function creep. Periodic audit is a further mechanism to review compliance and minimise the encroachment of new privacy risks from function creep.
- (j) Publication of this PIA report can also enhance public trust in the PCEHR System through transparency about the system's privacy impacts.

8.6.1 Recommendations

- 8.18 That prior to completion of the operational level design of the PCEHR System and prior to the PCEHR System entering the 'live production' environment, the Department commission further privacy reviews of:
 - (a) the draft operational level design; and
 - (b) the draft consumer communications and terms & conditions, to be developed by the Change and Adoption Partner.
- 8.19 That the PCEHR System include an on-going oversight and governance committee, including representation from the Privacy Officer of the Department as well as State and Territory bodies, to manage the following functions:
 - (a) promote and report on privacy compliance;
 - (b) review any requests to change the audit logging regime or data security controls applying to the PCEHR System;

²²⁶ Submission from the Australian Medical Association to the Department of Health and Ageing relating to the introduction of a Personally Controlled Electronic Health Record System, May 2011, page 4

- (c) review and commission PIAs for:
 - (i) any proposal to enhance, expand or amend the scope of the data to be held in, or indexed through, the PCEHR; and
 - (ii) any proposal to enhance, expand or amend the scope of the PCEHR System as a whole;
- (d) commission regular privacy audits and information security audits of the PCEHR System;
- (e) review privacy complaints arising from use of the PCEHR System; and
- (f) update staff training and user manuals as needs be.

8.20 That this PIA Report be provided to the Australian Privacy Commissioner and all State/Territory Privacy Commissioners or equivalent regulators.

8.21 That this PIA Report be published online by the Department, together with the Department's response to the recommendations.

Chapter 9 - Conclusions & Recommendations

9.1 Phase One Conclusions

9.1.1 Privacy protection will be critical to success

- (a) In its comprehensive review of privacy in 2008, the ALRC recognised the significant potential benefits to healthcare quality and safety that a shared EHR may deliver, but noted that 'such schemes will work effectively only if there is a sufficient degree of public trust and public confidence in the schemes and their administration'.²²⁷
- (b) The success of the PCEHR System will depend on participation by both consumers and healthcare providers. Participation will be affected by the extent of the individual's trust in the system. For the Australian Government to earn consumers' trust, it must demonstrate that it is committed to achieve the appropriate balance between competing objectives. This means minimising any unnecessary and avoidable privacy intrusions, and ensuring that the remaining privacy impacts are proportionate to the risks having regard to the objectives for the PCEHR System, and balanced by positive outcomes.
- (c) Effective privacy protections need to be established as part of the development of a shared electronic health record. Consumers should not be expected to choose between realising the benefits of a PCEHR and protecting their privacy; a well-designed shared EHR system should aim to deliver both.
- (d) This Privacy Impact Assessment has examined both the 'privacy positives' and the privacy risks arising from the design of the PCEHR System. For each identified risk we have also recommended one or more ways in which to remove or mitigate that risk.
- (e) Those recommendations which are most strongly urged are those which can significantly improve privacy protection for health consumers, without significantly impacting on the achievement of the proposal's objectives.

9.1.2 Identifying privacy impacts

- (a) Identifying privacy impacts and risks involves an examination of how the proposal will 'affect the choices individuals have regarding how information about them is handled, the potential degree of intrusiveness into the private lives of individuals, compliance with privacy law, and how the project fits into community expectations'.
- (b) The need to examine issues beyond compliance with privacy laws is partly because in many respects, privacy principles in information privacy laws defer to other legislation that authorises or requires certain data to be collected, used or disclosed. Privacy Impact Assessments therefore respond not only to public concerns about strict compliance with privacy laws, but also to concerns about the wider implications of initiatives that affect the collection, use and disclosure of personal information.
- (c) This PIA has therefore taken the National Privacy Principles as a starting point for analysis, but has not restricted itself to questions only of strict legal compliance with those principles. The process of identifying privacy impacts is outlined further in Chapters 1 and 3 of this report.

²²⁷ Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC Report 108, 2008, part 61.22

9.1.3 Limits to this assessment

- (a) As outlined further in Chapter 1, this PIA has been undertaken by reference to the following:

Intended design	the draft Concept of Operations (NeHTA, version 0.13.6, 8 April 2011) and the revised Concept of Operations (NEHTA, version 0.14.12 August 2011) and as represented by representatives of the Department and NeHTA
Intended legislative underpinnings	as represented in the Legislation Issues Paper (the Department, July 2011)
Possible governance arrangements	as represented and instructed by representatives of the Department and NeHTA

- (b) In particular, it should be noted that:
- (i) this PIA is not an assessment of any draft legislation to support the PCEHR System with the exception of legislative amendments proposed by submitters to the draft Bill, in accordance with the scope of Phase Two (see Chapter 1), in order to mitigate perceived privacy risks; and
 - (ii) this PIA is not an assessment of the adequacy of information security arrangements for the proposed PCEHR System.

9.1.4 The privacy positives

- (a) The development and uptake of the PCEHR has the potential to dramatically improve the ability of consumers to access their own health information in a timely and accessible way. The increased transparency to consumers of their health information, and information about who has been accessing their health information, is a major privacy positive for the PCEHR proposal.
- (b) Other privacy positives are to be found in the manner in which the design of the system has incorporated ways to minimise privacy risks. These features include:
- (i) the central 'privacy promise' made to Australians that having a PCEHR is entirely voluntary;
 - (ii) that consumers can voluntarily suspend, deactivate and reactivate their PCEHR at any time;
 - (iii) a recognition that not all consumers are alike, and that therefore consumers should be offered individual choice in how they wish to balance accessibility of their health information versus protection of their privacy;
 - (iv) the flexible, 'sliding scale' set of access controls and other privacy settings available to the consumer;
 - (v) that a healthcare provider can upload a record without 'viewing' the PCEHR itself;
 - (vi) that a consumer can nominate a healthcare provider to be responsible for establishing and updating their shared health summary as a separate record in the PCEHR;

- (vii) that the design precludes any unrelated third parties, such as law enforcement agencies or researchers, from having online access to the PCEHR System, so that any requests for information will have to go through the System Operator and be subject to the conditions set by the relevant privacy principles under the Privacy Act;
- (viii) that there will be comprehensive audit logging of all access to a consumer's PCEHR, which creates a strong inhibitor of misuse; and
- (ix) that the consumer will have real-time access to a summary version of the audit log, which will dramatically improve transparency in the handling of health information, and further mitigate the risk of misuse by authorised users.

9.1.5 The privacy risks

- (a) Privacy risks have been identified throughout Chapters 4 to 8. We have not rated or ranked these privacy risks.
- (b) Chapters 4 to 6 deal with the privacy risks arising from the nature of the PCEHR System itself: how personal information and health information will be collected, stored, used and disclosed.
- (c) These risks may be briefly summarised as follows:
 - (i) pressure to change the voluntary nature of the PCEHR, and practical limitations to the voluntary nature of the PCEHR (Recommendations 4.1 to 4.5);
 - (ii) practical limitations to the access controls choices and other privacy settings available to the consumer (Recommendations 4.18 to 5.16, Recommendations 5.22 to 5.28);
 - (iii) identity management risks at the point of registration and deactivation (Recommendations 4.6 to 4.17);
 - (iv) identity management risks in relation to verifying the identity or credentials of an authorised user (Recommendations 5.17 to 5.19);
 - (v) unnecessary collection risks through the use of Registered portal operators (Recommendations 5.9 and 5.10);
 - (vi) unnecessary collection risks through setting mandatory data fields for the upload of records (Recommendations 5.29 and 5.30);
 - (vii) indirect collection risks at the point when consumers enter information about other people, such as their emergency contacts (Recommendation 5.3);
 - (viii) use and disclosure risks arising from intentional misuse of a consumer's PCEHR;
 - (ix) disclosure risks arising from the display of a consumer's home address (Recommendations 5.1 and 5.2);
 - (x) disclosure risks arising from the display of irrelevant health information to authorised representatives (Recommendation 5.12);
 - (xi) disclosure risks posed by inappropriate use of 'emergency override' settings (Recommendations 5.26 to 5.28);
 - (xii) disclosure risks of local clinical systems automatically upload records (Recommendation 5.31); and
 - (xiii) data retention risks in relation to records left inactive for long periods of time.

- (d) Chapters 7 and 8 assess the governance and accountability measures proposed for the System Operator and other participants in the system. Recommendations have been made to strengthen the accountability of, and public confidence in, the PCEHR System as a whole (Recommendations 7.1 to 8.21).
- (e) The aim of these recommendations is to achieve the following:
 - (i) ensuring the System Operator has the appropriate authority for, and oversight of, its operations;
 - (ii) ensuring uniform and enforceable privacy responsibilities for participants;
 - (iii) ensuring enforceable privacy rights for consumers;
 - (iv) ensuring a clear and workable system for complaint handling;
 - (v) minimising data security risks in the storage of personal information and health information in the system, and
 - (vi) protecting privacy into the future.

9.1.6 Proposed solutions - legislation

- (a) We have made a number of recommendations aimed at influencing the drafting of the PCEHR Bill. Critical legislative recommendations include:
 - (i) a number of measures to confirm and support the 'opt in' nature of the PCEHR for consumers (Recommendations 4.1 to 4.3);
 - (ii) preventing any extension of the scope of the system, or any change to the 'opt in' nature of the PCEHR, by way of regulation or other subordinate legislation (Recommendation 4.2);
 - (iii) specificity in the evidence of identity rules for consumer registration, including eligibility criteria for authorised representatives (Recommendations 4.6 to 4.17);
 - (iv) obliging HPI-Os to verify the identity of each proposed user, and to provide training to their employees on the appropriate access to and use of PCEHRs (Recommendation 5.20);
 - (v) providing the System Operator with the ability to limit, suspend or revoke access rights of authorised representatives in accordance with an established protocol (Recommendation 5.13);
 - (vi) providing the System Operator with the power to disconnect or revoke the access of an authorised representative, ARA, registered portal operator, registered repository operator or HPI-O; or to compel an HPI-O to disconnect or revoke the access of a specific user (Recommendation 8.11);
 - (vii) defining the circumstances in which a consumer's access controls and other privacy settings may be overridden in an 'emergency' (Recommendation 5.26);
 - (viii) including a set of 'PCEHR privacy rules' governing all non-consumer users of the PCEHR System, which should encompass:
 - (A) authorised purposes for searching for or 'viewing' information from a PCEHR;
 - (B) authorised purposes for copying or 'downloading' information from a PCEHR;

- (C) authorised purposes for using information from a PCEHR (whether or not it has been copied or downloaded first);
 - (D) authorised purposes for adding or 'uploading' information to a PCEHR;
 - (E) obligations to take reasonable steps to protect the data security of the PCEHR, and
 - (F) obligations to take reasonable steps to ensure the data quality of information added or 'uploaded' to the PCEHR (Recommendation 8.1).
- (ix) incorporating an enforcement mechanism which provides that a contravention of the 'PCEHR privacy rules' is an 'interference with privacy' under the Privacy Act - and, if the contravening conduct was intentional, also a criminal offence (Recommendation 8.2);
 - (x) authorising healthcare providers to disclose personal information and health information to a PCEHR, such as to authorise non-compliance with NSW HPP 14 and 15, Vic HPP 9, Tas PIPP 9 and NT IPP 9 (Recommendation 8.6);
 - (xi) ensuring that the 'PCEHR privacy rules' must be confirmed as understood and accepted by individual users as a condition of their first access to the PCEHR System (Recommendation 5.21);
 - (xii) providing for a complaint-handling process with clear time limits and pathways, which commences with the System Operator and can then be escalated to the Australian Privacy Commissioner (Recommendation 8.8); and
 - (xiii) creating obligations on the System Operator and other participating organisations to report any data security breaches and any evidence of internal misuse of PCEHR data to the System Operator and the Australian Privacy Commissioner (Recommendation 8.10).

9.1.7 Proposed solutions - system design

- (a) We have made a number of recommendations aimed at influencing the final technical design of the PCEHR System. Critical design recommendations include:
 - (i) that the system allow the consumer's 'home address' field to be left blank, or accept post box addresses (unless the consumer wants to access their PCEHR via mail) (Recommendation 5.1);
 - (ii) that the design of the 'authorised representative' component of the PCEHR System be reconsidered, with a view to limiting the access of authorised representatives of adult consumers (and authorised representatives of children in some circumstances) to only viewing the shared health summary and Consumer-Entered Health Summary, rather than all records (Recommendation 5.12);
 - (iii) that the system allow some mechanism for adult consumers who have one or more authorised representatives to exercise their privacy rights (such as setting access controls or removing records) while in a state of capacity (Recommendation 5.16);
 - (iv) that there be an assessment of the information security classification for data to be held by the System Operator, and data when in transit to or from the System Operator, and a corresponding independent Threat and Risk Assessment of the security controls proposed as a result (Recommendation 7.6);
 - (v) that over time, the design of the PCEHR System evolve to a situation in which consumers can seek to 'block' access by specific users; and

- (vi) that there be a further review of:
 - (A) the draft operational level design;
 - (B) the detailed plans for online registration, to ensure the online channel offers similar levels of privacy protection and that no channel leaves a consumer substantially more exposed than other channels; and
 - (C) the draft consumer communications and Terms & Conditions (Recommendation 8.18).

9.1.8 Proposed solutions - the System Operator and other participating bodies

- (a) We have made a number of recommendations relating to the role and operations of the System Operator and other participating bodies, including:
 - (i) that the conformance tests for clinical software to connect to the PCEHR System should include ensuring that no records are uploaded automatically from the local system to the PCEHR (Recommendation 5.31); and
 - (ii) that the PCEHR System include an on-going oversight and governance committee (Recommendation 8.19).

9.1.9 Proposed solutions - obligations on healthcare users

- (a) Privacy obligations will mean little in practice if users do not understand their obligations, or how they apply in practice. In this regard, we have recommended that healthcare users be provided with guidance on various matters, including:
 - (i) the 'PCEHR privacy rules' and their obligations as users (Recommendation 5.21);
 - (ii) the interpretation of the legislative 'emergency access' test, with specific examples and clearly available whenever the 'emergency override' button is presented (Recommendation 5.28); and
 - (iii) what records might not be appropriate to upload including where there are other legal restrictions in place (Recommendation 5.32).

9.1.10 Proposed solutions - communications to consumers

- (a) As well as being informed about the benefits of the PCEHR, health consumers will need to understand how best to manage their particular privacy concerns through the various access control and other privacy settings available to them. This information should be available to consumers prior to making the decision to register for a PCEHR. Transparency will be important to engender public confidence in the system.
- (b) Our recommendations in relation to consumer-facing communications include that:
 - (i) consumer communications should explain the registration rules in relation to authorised representatives, including those appointed under enduring guardianship arrangements (Recommendation 4.17);
 - (ii) information about the various access control options and other privacy settings (such as options in relation to the display of home address), and the practical limits to those features, should be available to consumers before they decide to register for a PCEHR (Recommendation 4.28);
 - (iii) consumers should have available to them a 'preview' function which allows the consumer to see how their record will appear to other types of users depending on the access controls they set (Recommendation 4.29);

- (iv) consumer communications should reflect the possibility that information from their PCEHR may be disclosed for research or law enforcement purposes, or when required by law (Recommendation 5.39);
- (v) consumer communications about suspension and deactivation of records should clarify that records will still be held by registered repository operators and/or in local clinical systems for periods as determined by local data retention requirements (Recommendation 6.3);
- (vi) the exception for emergency access is clearly communicated to consumers prior to choosing to 'suspend' their PCEHR (Recommendation 6.4);
- (vii) consumer communications should explain their privacy rights, the privacy rules which participants in the PCEHR System must follow, and the complaint-handling process (Recommendation 8.15), and
- (viii) this PIA Report should be published online by the Department, together with the Department's response to the recommendations subject to appropriate redactions, made in accordance with FOI disclosure rules (eg redact the security sensitive material to avoid publishing security weaknesses) (Recommendation 8.21).

9.1.11 Recommendations in full

Pressure to change the voluntary nature of the PCEHR

- 4.1 That the PCEHR Bill include the requirement for a consumer (or their authorised representative)'s express consent to register for a PCEHR.
- 4.2 That the PCEHR Bill not allow regulations or other subordinate legislation to create an exemption from the express consent requirement.
- 4.3 That any plans for transition of data from existing shared EHR systems incorporate a 'fresh' express consent process.

Practical limitations to the voluntary nature of the PCEHR

- 4.4 That the PCEHR Bill prohibit:
 - (1) inducing a consumer to register for a PCEHR (other than by reference to the benefits of the PCEHR itself);
 - (2) inducing a consumer to provide a copy of their PCEHR to a third party;
 - (3) consumers being placed at a disadvantage (financially or in relation to access to healthcare) if they do not have a PCEHR; and
 - (4) consumers being placed at a disadvantage (financially or in relation to access to healthcare) for declining to provide permission for a healthcare provider to access their PCEHR.
- 4.5 That advice be provided to registered portal operators, to ensure that their marketing, privacy notices and terms and conditions clearly reflect the distinction between the PCEHR System and any services offered by the portal provider.

Online registration - verification of identity

- 4.6 That there be a further review of the detailed plans for online registration, to ensure the online channel offers a similar level of privacy protection as the assisted registration channels, particularly in terms of collection necessity and data security.
- 4.7 That the PCEHR Bill clearly describe the type of information to be used and disclosed to verify

consumer identity, by whom it will be used or disclosed, and for what purposes.

- 4.8 That there be a further review of the detailed plans for face to face registration of a minor, to ensure the face to face channel offers a similar level of privacy protection as the online channel, particularly in terms of data security and association to the correct guardian.
- 4.9 That there be a further review of the purpose of asking 'challenge and response' questions, noting that verification can alternatively occur by entering an IVC number, irrespective of whether the questions are answered correctly.

Assisted Registration – verification of identity

- 4.10 That ARAs for the PCEHR be encouraged to utilise the national Document Verification Service, instead of recording details of the EOI records presented.
- 4.11 That the PCEHR Bill provide that ARAs for the PCEHR may not keep copies of EOI records, and that any such copies must be securely destroyed as soon as the registration process is complete.
- 4.12 That the PCEHR Bill clarify whether ARAs for the PCEHR may or must keep a record of a record of the EOI record number.
- 4.13 That the PCEHR Bill require consumers seeking to register via mail to post certified copies of the EOI records (not just a statement from a JP about sighting the records).
- 4.14 That the arrangements with ARAs ensure that there are physical privacy protections for consumers using their shop fronts, such as timed logouts and privacy screens on public-facing computers.
- 4.15 That the arrangements with ARAs ensure that there are administrative and technical privacy protections, such as appropriate staff screening, staff training in privacy obligations, and audit logging of staff registration transactions.

Registration via authorised representative

- 4.16 That the PCEHR Bill provide that in order to register an adult consumer, an authorised representative must provide:
- certified copies of 100 points worth of evidence of their own identity;
 - certified copy of documentary evidence of legal authority to act on behalf of the consumer eg certified copy of guardianship order;
 - the Medicare card of the consumer; and
 - where the evidence of their position as a representative of the adult consumer is unclear as to the consumer's current state of capacity, further evidence that the consumer currently lacks the capacity to make a decision about registration, or manage their PCEHR, themselves.
- 4.17 That communications to consumers explain the registration rules in relation to authorised representatives, including those appointed under enduring guardianship arrangements.

Pre-population of Medicare Data

- 4.18 That the PCEHR Bill authorise the disclosure of each 'stream' of Medicare held data (MBS, PBS, organ donor status and/or childhood immunisation records) to a consumer's PCEHR, upon confirmation that the consumer has provided a positive consent to that 'stream'.
- 4.19 That the final design allow a consumer who consents to the MBS and/or PBS data stream to choose whether they wish the data stream to include data already collected up to two years prior to the date of their consent, with the default position being 'no back dated data'.
- 4.20 That the PCEHR Bill clarify which data 'streams' can be populated with data that pre-dates the

commencement of the consent decision.

- 4.21 That consumer communications advise consumers who are concerned about the privacy of specific illnesses or episodes of care (such as a pregnancy termination), that unless they are very health literate and prepared to 'remove from view' specific data items, their best option may be to not consent to the disclosure of the MBS / PBS data streams into their PCEHR.

'Not Findable' Feature

- 4.22 That the default position for consumers be that the existence of their PCEHR will be 'flagged' within local clinical systems unless the consumer chooses otherwise.
- 4.23 That there be a name change to the 'not findable' access control, to instead be called 'not flagged'.

The Access List

- 4.24 That consumer communications carefully explain the practical limits of the 'Revoke' access control option.
- 4.25 That the PCEHR Bill prohibit healthcare organisations from recording a consumer's PACC or PACC-X for future use (ie in the event that the organisation is moved to 'Revoked' status).
- 4.26 That one option for the range of optional consumer notifications (SMS messages or emails) should be to receive a notification if an organisation on their 'Revoke' list changes their HPI-O in some way.
- 4.27 That the Department develop some incentive for organisations to set their HPI-Os (for the purposes of the Access List) at a level which reflects the management of records within the organisation itself.

Complexity for consumers

- 4.28 That consumer communications about the various privacy control settings and the limits to those settings be available to consumers before they decide to register for a PCEHR.
- 4.29 That consumers have available to them a 'preview' function which allows the consumer to see how their record will appear to other types of users depending on the access controls they set.

Creating nominated representatives

- 4.30 That the design of the system include some prompt every few years (such as a screen prompt on next log in) to consumers with nominated representatives to review their choices and check the accuracy of their information.

Consumer-Entered information

- 5.1 That the design of the PCEHR System allow the consumer's 'home address' field to be left blank, or accept postal box addresses.
- 5.2 That consumer communications advise consumers of their choices regarding the address entered in their PCEHR, but also warn them that their home address might be contained in records indexed through the PCEHR.
- 5.3 That the design of the PCEHR System remind a consumer, at the point of data entry about their emergency contacts, that all other users including authorised representatives and nominated representatives will see that data; that the PCEHR System provide a notice to consumers, recommending that consumers take reasonable and practical steps to obtain consent from those other people, where appropriate.
- 5.4 That a privacy notice be visible when a consumer seeks to enter data in their private 'Notes' area,

explaining the circumstances (if any) in which third parties could gain access to that information.

- 5.5 That the design of the PCEHR System include a mechanism by which a consumer can exercise their privacy right of correction, by associating a statement with an indexed record, such as through the Consumer-Entered Health Summary.
- 5.6 That the design provide for appropriate anti-hacking measures such as a maximum number of attempts before the PCEHR System 'locks out' the consumer and that mechanisms are in place for consumers to then reset their password or be re-directed to an assisted channel (eg face to face or telephone).
- 5.7 That consumers are given advice on the suitability of questions and answers, eg the answer should only be known by the consumer and the answer remains true over time.
- 5.8 That special authentication mechanisms are put in place for consumers with a nominated representative (to allow Call Centre employees to distinguish between the consumer and a nominated representative). To mitigate this, the importance of 'secret questions and answers' set at registration by the consumer must be clearly communicated to consumers ie do not record the answers in your PCEHR.

Collection of personal information by registered portal operators

- 5.9 That the PCEHR Bill prohibit registered portal operators from recording a consumer's IHI.
- 5.10 That the design of the PCEHR System include a 'PCEHR-specific' portal, such that consumers need not expose their personal information to any other organisation in order to gain access to their PCEHR online.

Access to personal information by Call Centre staff

- 5.11 That regulations under the PCEHR Bill set controls over the System Operator's Call Centre including requirements for staff security screening the monitoring of calls and how much of a consumer's data can be 'viewed' in what circumstances.

Access to personal information by authorised representatives

- 5.12 That the design of the 'authorised representative' component of the PCEHR System be reconsidered, with a view to limiting the access of authorised representatives of adult consumers (and authorised representatives of children in some circumstances) to only viewing the shared health summary and Consumer-Entered Health Summary, rather than all records.
- 5.13 That the PCEHR Bill establish the eligibility rules for authorised representatives of both child and adult consumers, as well as providing the System Operator with the ability to limit, suspend or revoke access rights of authorised representatives in accordance with an established protocol.
- 5.14 That the System Operator develop a protocol for dealing with complaints by or about 'competing' authorised representatives, including the circumstances in which the System Operator may limit, suspend or revoke access rights of authorised representatives, such as on presentation of evidence such as an apprehended violence order.
- 5.15 That the design of the 'authorised representative' component of the PCEHR System include technological design and procedural protocols to ensure regular reviews (such as every three years) of the continued validity of instruments asserting the eligibility of authorised representatives of adult consumers with intermittent or fluctuating capacity.

Consumers with intermittent capacity

- 5.16 That the design of the 'authorised representative' component of the PCEHR System be reconsidered to allow some mechanism for adult consumers who have one or more authorised representatives to

exercise their privacy rights (such as setting access controls or removing records) while in a state of capacity. This mechanism would need to be time critical for example when in the presence of a healthcare provider who can make a judgment about their capacity at that immediate time.

Authentication of users

- 5.17 That the PCEHR Bill define 'employee' to explicitly include tertiary healthcare students on placement.
- 5.18 That the PCEHR Bill define or include guidance as to what constitutes a 'legitimate need' for other individuals who do not have a HPI-I within a registered healthcare provider organisation to access the PCEHR System.
- 5.19 That the PCEHR Bill set one of the conformance requirements on an HPI-O as an obligation to verify, with 100 points of EOI, the identity of each proposed user (and confirm their proper association to an HPI-I, where applicable).

Education of users

- 5.20 That the PCEHR Bill set one of the conformance requirements on an HPI-O as an obligation to provide training to their employees on the appropriate access to and use of PCEHRs including the 'PCEHR privacy rules' and any other privacy obligations applying to that organisation.
- 5.21 That the PCEHR Bill ensure that the 'PCEHR privacy rules' must be confirmed as understood and accepted by individual users as a condition of their first access to the PCEHR System.

Search Parameters

- 5.22 That consumer communications draw attention to the fact that under the 'Basic' access controls, any authorised user of the system can find their PCEHR so long as the user knows at least the consumer's full name, gender, date of birth, and either their address or their Medicare / DVA number.
- 5.23 That when designing the conformance tests for clinical software seeking to interface with the PCEHR system, the Department and NEHTA give consideration to how a PCEHR can be 'found' in an automated way, with a view to ensuring the clinical software strikes a proper balance between speed of access and surety as to the correct identity of the individual.
- 5.24 That the System Operator use proactive monitoring of the use of exception-based searching for an IHI, to search for possible examples of misuse of the system.
- 5.25 That the System Operator use proactive monitoring of the audit logs of activity against the PCEHR of public figures, to search for possible examples of misuse of the system.

Emergency access

- 5.26 That the PCEHR Bill define the circumstances in which a consumer's access controls and other privacy settings may be overridden as only when the override is 'necessary to prevent or lessen a serious and imminent threat to the life or health of any consumer'.
- 5.27 That the PCEHR System design ensure that access granted via the 'emergency access' override is only temporary.
- 5.28 That users be provided with guidance on the interpretation of the legislative 'emergency access' test, with specific examples developed in consultation with the Australian Privacy Commissioner. This guidance should be clearly available whenever the 'emergency override' button is presented, for example by way of a link or pop-up box.

Data quality of uploaded records

- 5.29 That the data quality framework for the PCEHR System design should ensure that the only mandatory field for identity/demographic data in relation to records is the consumer's IHI.
- 5.30 That the design makes it clear that the indigenous field status (as a type of 'sensitive personal information subject to special protection) is optional and not required to be completed.

When a record should not be uploaded

- 5.31 That the conformance tests for clinical software to connect to the PCEHR System should include ensuring that no records are uploaded automatically from the local system to the PCEHR; that is a HPI-I user must make a 'manual' decision in relation to each upload.
- 5.32 That healthcare providers be provided with guidance on what records might not be appropriate to upload including where there are other legal restrictions in place.

PCEHR Bill

- 5.33 That the PCEHR Bill prohibit any disclosure of Consumer Notes except where the System Operator is compelled to do so by way of a Court order or similar.
- 5.34 That the PCEHR Bill define the extent to which the System Operator will be considered to 'control' records held in registered repository operators but which are available through its indexing service, for the purposes of responding to a subpoena, warrant, notice to produce or other instrument.
- 5.35 That the PCEHR Bill define the extent to which healthcare provider users of the system will be considered to 'control' any data held in or indexed through the PCEHR, for the purposes of responding to a subpoena, warrant, notice to produce or other instrument.
- 5.36 That the PCEHR Bill prescribe whether the System Operator can allow the disclosure, for research purposes, of records held in registered repository operators but which are available through its indexing service.
- 5.37 That the PCEHR Bill prescribe whether the System Operator can allow the disclosure, for research purposes, of records which the consumer has sought to 'Remove from View'.
- 5.38 That the PCEHR Bill include a note to the effect that the rules under which personal information may be disclosed by the System Operator for research, for law enforcement purposes, or when obligated under a subpoena or similar instrument are to be found in the Privacy Act.
- 5.39 That consumer communications (and in particular, the privacy notice provided at the time of registration) reflect the possibility that information from their PCEHR may be disclosed for research or law enforcement purposes, or when required by law, such as in response to a subpoena if the consumer is involved in litigation.

Suspension, deactivation and reactivation

- 6.1 That the PCEHR Bill ensure that child consumers aged 14 through 17 who seek to take control of their PCEHR have the right to do so, and that their rights include decisions to suspend or deactivate their record.
- 6.2 That the PCEHR Bill set a data retention period for PCEHR records in the 'Active' category which have not been subject to any action on the record (such as any new data being added) for an extended period of time.
- 6.3 That the consumer communications about suspension and deactivation of records clarify that although records held in registered repository operators may no longer be found through a suspended or deactivated PCEHR, they will be held by the registered repository operators and/or in local clinical systems for periods as determined by local data retention requirements.

- 6.4 That the exception for emergency access is clearly communicated to consumers prior to the PCEHR entering 'suspension mode'.

Governance of the System Operator

- 7.1 That the PCEHR Bill ensure that the System Operator is subject to the NPPs (or rules based on the NPPs) rather than the IPPs in the Privacy Act.
- 7.2 That the PCEHR Bill establish the System Operator's authority to use and disclose data (including metadata) from a consumer's PCEHR for reporting purposes. The legislation should set out the bodies to whom personal information may or must be disclosed by the System Operator including a reference to reporting obligations created in other legislation.
- 7.3 That the System Operator ensure strict conformance requirements on HPI-Os to ensure users are uniquely identified to the System Operator at every login.
- 7.4 That the PCEHR Bill establish the System Operator's authority to use and disclose audit log data from a consumer's PCEHR for complaint-handling and law enforcement purposes. The legislation should set out the bodies to whom personal information may or must be disclosed by the System Operator, including the Australian Privacy Commissioner or other privacy regulator in the case of a privacy complaint, or to the appropriate law enforcement agency in the case of suspected unlawful use.
- 7.5 That the PCEHR Bill establish the right of a consumer to obtain a copy of the summary version of their audit log through assisted channels, without charge.

Threat and Security Risk Assessment

- 7.6 That prior to finalisation of operational plans for the System Operator, there should be an assessment of the information security classification for data to be held by the System Operator, and data when in transit to or from the System Operator, and a corresponding independent Threat and Risk Assessment of the security controls proposed as a result.
- 7.7 That the Threat and Risk Assessment examine the adequacy of legislative or other protections against the risk of exposure of consumers' personal information to foreign law enforcement bodies.
- 7.8 That the Threat and Risk Assessment be reviewed by the Department's privacy team in conjunction with this and any other PIA reports.

Governance of the broader PCEHR System

- 8.1 That the PCEHR Bill include a set of 'PCEHR privacy rules' governing all non-consumer users of the PCEHR System, which should encompass:
- (1) authorised purposes for searching for or 'viewing' information from a PCEHR;
 - (2) authorised purposes for copying or 'downloading' information from a PCEHR;
 - (3) authorised purposes for using information from a PCEHR (whether or not it has been copied or downloaded first);
 - (4) authorised purposes for adding or 'uploading' information to a PCEHR;
 - (5) obligations to take reasonable steps to protect the data security of the PCEHR; and
 - (6) obligations to take reasonable steps to ensure the data quality of information added or 'uploaded' to the PCEHR.

Note: We have used the term 'privacy rules' here simply to distinguish our proposal from existing 'privacy principles'. Terms such as 'privacy protocol' or 'privacy standards' may be equally

appropriate.

- 8.2 That the 'PCEHR privacy rules' incorporate an enforcement mechanism which provides that a contravention of those rules is an 'interference with privacy' under the federal Privacy Act - and, if the contravening conduct was intentional, also a criminal offence.
- 8.3 That the 'PCEHR privacy rules' cover conduct relating to information gained from a PCEHR by an authorised user of a PCEHR. The scope of regulated conduct should not be limited to conduct done 'in the performance of their duties' (cf s 8(1) of the Privacy Act), and there should be no exception allowing use of the information gained from a PCEHR for 'personal, family or household affairs' (cf s 26(2)(c) of the HI Act). That is, the obligations must extend to the misuse of information by a 'rogue' employee, agent or contractor, who uses or discloses information from a PCEHR for their own, unauthorised purposes. The obligations must also extend to the recipient of information gained from a PCEHR by an authorised user of a PCEHR, so as to ensure that it is an offence for a third party to use or disclose information from a PCEHR which was improperly obtained.
- 8.4 That the 'PCEHR privacy rules' provide that in the case of an alleged contravention, the respondent to a complaint to the Privacy Commissioner shall be the employing organisation, rather than the individual employee, agent or contractor (see s 8(1) of the Privacy Act).
- 8.5 That the criminal penalties for intentional contravention of a 'PCEHR privacy rule' should be as per s 26(1) of the HI Act, namely a maximum two years imprisonment and/or 120 penalty units. Criminal penalties may be applicable to an individual employee, agent or contractor, or to a corporate person.
- 8.6 That the PCEHR Bill authorise healthcare providers to disclose personal information and health information to a PCEHR, such as to authorise non-compliance with NSW HPP 14 and 15, Vic HPP 9, Tas PIPP 9 and NT IPP 9.
- 8.7 That when the draft forms and terms and conditions (versions relating to each of the access channels) are completed, the forms and terms and conditions be reviewed for IPP/NPP compliance.
- 8.8 That the PCEHR Bill provide for a complaint-handling process with clear time limits and pathways, which commences with the System Operator and can then be escalated, by either the complainant or the System Operator, to the Australian Privacy Commissioner.
- 8.9 That the PCEHR Bill not exclude complainants from lodging a complaint or seeking a remedy in any other forum.
- 8.10 That the PCEHR Bill include an obligation on the System Operator to report any data security breaches and any evidence of internal misuse of PCEHR data to the Australian Privacy Commissioner.
- 8.11 That the PCEHR Bill provide the System Operator with the power to disconnect or revoke the access of an authorised representative, ARA, registered portal operator, registered repository operator or HPI-O; or to compel an HPI-O to disconnect or revoke the access of a specific user.
- 8.12 That the PCEHR Bill provide the Australian Privacy Commissioner with the power to compel the System Operator to exercise its power to disconnect or revoke the access of an individual or organisation.
- 8.13 That the Department encourage State and Territory governments to ensure legislation or protocols allow some flexibility in the application of time limits in their jurisdictions, so that their time limits do not start to 'run' until the Australian Privacy Commissioner has advised a complainant of their option to lodge their complaint in that other jurisdiction.
- 8.14 That the Australian Privacy Commissioner to be adequately resourced to manage any additional

workload expected to arise from implementation of the PCEHR System

- 8.15 That consumer communications clearly articulate to consumers their privacy 'rights', the privacy 'rules' which participants in the PCEHR System must follow, and the complaint-handling process.
- 8.16 That the PCEHR Bill include an obligation on ARAs, registered portal operators, registered repository operators and HPI-Os to report any data security breaches, and any evidence of internal misuse of PCEHR data, to the Australian Privacy Commissioner and the System Operator.
- 8.17 That a Threat and Risk Assessment examine the adequacy of legislative or other protections against the risk of exposure of consumers' personal information, held by ARAs, registered portal operators, registered repository operators and HPI Os, to foreign law enforcement bodies.
- 8.18 That prior to completion of the operational level design of the PCEHR System and prior to the PCEHR System entering the 'live production' environment, the Department commission further privacy reviews of:
 - (1) the draft operational level design; and
 - (2) the draft consumer communications and terms & conditions, to be developed by the Change and Adoption Partner.
- 8.19 That the PCEHR System include an on-going oversight and governance committee, including representation from the Privacy Officer of the Department as well as State and Territory bodies, to manage the following functions:
 - (1) promote and report on privacy compliance;
 - (2) review any requests to change the audit logging regime or data security controls applying to the PCEHR System;
 - (3) review and commission PIAs for:
 - (a) any proposal to enhance, expand or amend the scope of the data to be held in, or indexed through, the PCEHR; and
 - (b) any proposal to enhance, expand or amend the scope of the PCEHR System as a whole;
 - (4) commission regular privacy audits and information security audits of the PCEHR System;
 - (5) review privacy complaints arising from use of the PCEHR System; and
 - (6) update staff training and user manuals as needs be.
- 8.20 That this PIA Report be provided to the Australian Privacy Commissioner and all State/Territory Privacy Commissioners or equivalent regulators.
- 8.21 That this PIA Report be published online by the Department, together with the Department's response to the recommendations.

9.2 Phase Two Recommendations

In our view it is appropriate for the Department to consider amending the Bill and the Explanatory Memorandum in light of the Legislation Submissions reviewed by us to address the following:

- 9.1 Make it clear whether the authorised representative is required to have a verified healthcare identifier (4.7.6(a)).

- 9.2 The PCEHR Rules should accommodate concurrent access to the PCEHR by the consumer and authorised representative (4.7.6(b)).
- 9.3 Make it clear that the PCEHR Rules will specify the default access controls (4.9.4) and the consumer's ability to correct errors in the PCEHR (5.1.10(a)).
- 9.4 Make it clear that information is uploaded as a feature of the PCEHR System unless a consumer advises otherwise (5.6.9).
- 9.5 Make it clear that healthcare providers must comply with a request by a consumer that a document should not be uploaded (5.6.10).
- 9.6 Make it clear that the System Operator can only use information obtained under s 44 in accordance with its functions. In addition it would be useful for the explanatory memorandum to provide examples of what such uses may be (5.7.9(f)).
- 9.7 Make it clear that the PCEHR Rules should specify the nature of the information to be included in the register (5.7.9(g)).
- 9.8 Ensure that the enforcement regime that applies to the System Operator for a breach of the Bill (whether through the Bill and/or other laws) is as effective as the enforcement regime that will apply to other participants who breach the Bill (8.2.8(e)).
- 9.9 The Explanatory Memorandum describe the alternative remedies available under concurrent legislation and common law (such as breach of confidence) (8.2.8(f)).
- 9.10 The System Operator should be required to refer to the OAIC's Guide to Handling Personal Information Security Breaches when considering whether to notify a consumer of a breach of data security safeguards (8.2.8(n)).

Schedule 1 List of Consultations and submissions reviewed

Submissions to Concept of Operations (version 0.13.6) ²²⁸	Office of the Australian Information Commissioner
	Australian Privacy Foundation
	Consumers Health Forum of Australia
	Royal Australian College of General Practitioners
	Pharmaceuticals Industry Council
	Australian Medical Association
	Australian General Practice Network
Submissions to the Legislation Issues Paper ²²⁹	Office of the Australian Information Commissioner
	Office of the Information Commissioner, Queensland
	Victorian Health Services Commissioner
	SA Health Services Commissioner
	Australian Privacy Foundation
	Queensland Council for Civil Liberties
	Council of Social Service of NSW (NCOSS)
	Consumers Health Forum of Australia
	IBM
	South Eastern Sydney and Illawarra Area Health Service
	Australian General Practice Network
	Australian Medical Association
	Consumer eHealth Alliance
Submissions to the Bill	Australian Privacy Foundation
	Office of the Australian Information Commissioner
	Royal Australian College of Physicians
	Minister for Health of Victoria
	WA Health
	SA Health
	Office of the Privacy Commissioner of NSW
	Health Services Commissioner of Victoria

²²⁸ and one confidential stakeholder submission

²²⁹ and confidential submissions from four stakeholders

	Pharmacy Guild of Australia
	Australian Medical Association
	Royal Australian College of Surgeons
	Royal Australian College of General Practitioners
	Australian Nursing Federation
	Consumers Health Forum of Australia
	National Aboriginal Community Controlled Health Organisation
	Medical Software Industry Association
	Medibank Private*
	Royal Children's Hospital of Melbourne*
	Avant Mutual Group*
	Epworth Healthcare*
	NSW Council for Civil Liberties Inc*
	MDA National*
	Aboriginal Medical Services Alliance of the Northern Territory*
	Royal Australian and New Zealand College of Psychiatrists*
	Microsoft*
	Australian Dental Association Inc*
	Royal College of Pathologists of Australia*
	Australian Private Hospitals Association*
	Australian Psychological Society Ltd*
	NSW Privacy Commissioner*

* - confined to the issues from these submissions identified by the Department

Schedule 2 Privacy Legislation Considered (Phase One)

Legislation considered (Cth)	<ul style="list-style-type: none"> • <i>Privacy Act 1988</i>
Legislation considered (NSW) Privacy/ Government information legislation:	<ul style="list-style-type: none"> • <i>Government Information (Public Access) Act 2009</i> • <i>Government Information (Public Access) Regulation 2009</i> • <i>General Disposal Authority 17</i> • <i>Ombudsman Act 1974</i> • <i>Privacy and Personal Information Protection Act 1998</i> • <i>Privacy and Personal Information Protection Regulation 2005</i> • <i>Privacy Code of Practice (General) 2003</i> • <i>Public Sector Employment and Management Regulation 2009</i> • <i>State Records Act 1998</i>
Legislation considered (NSW) Health Legislation:	<ul style="list-style-type: none"> • <i>Ambulance Services Regulation 2005</i> • <i>Drug and Alcohol Treatment Act 2007</i> • <i>Health Care Complaints Act 1993</i> • <i>Health Care Liability Act 2001</i> • <i>Health Records and Information Privacy Act 2002</i> • <i>Health Records and Information Privacy Code of Practice 2005</i> • <i>Health Records and Information Privacy Regulation 2006</i> • <i>Mental Health (Forensic Provisions) Regulation 2009</i> • <i>Mental Health Act 2007</i> • <i>Poisons and Therapeutic Goods Act 1966</i> • <i>Poisons and Therapeutic Goods Regulation 2008</i> • <i>Public Health Act 1991</i> • <i>Veterinary Practice Act 2003</i>
Legislation considered (VIC)	<ul style="list-style-type: none"> • <i>Health Records Act 2001</i> • <i>Health Records Regulations 2002</i> • <i>Freedom of Information Act 1982</i> • <i>Charter of Human Rights and Responsibilities (Public Authorities) Regulations 2009</i> • <i>Charter of Human Rights and Responsibilities Act 2006</i> • <i>Commissioner for Law Enforcement Data Security Act 2005</i> • <i>Health Practitioner Regulation National Law Regulations 2010</i> • <i>Mental Health Act 1986</i> • <i>Public Health and Wellbeing Act 2008</i> • <i>Guardianship and Administration Act 1986</i> • <i>Pharmacy Regulation Act 2010 (s 32 – requirements for dispensing and recording of prescriptions)</i> • <i>Crimes (Mental Impairment and Unfitness to be Tried) Act 1997</i> • <i>Health Practitioner Regulation National Law Regulations 2010</i> • <i>Health Professions Registration Act 2005 (mandatory disclosure in certain circumstances)</i>
Legislation considered (QLD)	<ul style="list-style-type: none"> • <i>Health Services Act 1991, Part 7</i> • <i>Information Privacy Act 2009</i> • <i>Information Privacy Regulation 2009</i> • <i>Mater Public Health Services Act 2008</i> • <i>Public Health Act 2005</i> • <i>Public Records Act 2002</i> • <i>Right to Information Act 2009</i>

	<ul style="list-style-type: none"> • <i>Right to Information Regulation 2009</i> • <i>Queensland Health (Clinical Records) Retention and Disposal schedule: QDAN 546 v3</i>
Legislation considered (TAS)	<ul style="list-style-type: none"> • <i>Archives Act 1983</i> • <i>Guardianship and Administration Act 1995</i> • <i>Health Complaints Act 1995</i> • <i>Health Practitioners Tribunal Act 2010</i> • <i>HIV/AIDS Preventive Measures Act 1993</i> • <i>Personal Information Protection Act 2004</i> • <i>Public Health Act 1997</i> • <i>Teachers Registration Act 2000</i> • <i>Workers Rehabilitation and Compensation Act 1988</i>
Legislation considered (SA)	<ul style="list-style-type: none"> • <i>Freedom of Information Act 1991</i> • <i>State Records Act 1997</i> • <i>Health and Community Services Complaints Act 2004</i> • <i>Health Care Act 2008</i> • <i>Public and Environmental Health Act 1987</i>
Legislation considered (WA)	<ul style="list-style-type: none"> • <i>Freedom of Information Act 1992 (FOI Act)</i> • <i>Mental Health Act 1996</i> • <i>Health (Western Australian Cancer Register) Regulations 2011</i> • <i>Health and Disability Services (Complaints) Act 1995</i> • <i>Health (Notification of Intussusception) Regulations 2007</i> • <i>Health (Notification of Stimulant Induced Psychosis) Regulations 2010</i> • <i>Health (Western Australian Register of Developmental Anomalies) Regulations 2010</i>
Legislation considered (ACT)	<ul style="list-style-type: none"> • <i>Privacy Act 1988 (Cth)</i> • <i>Australian Capital Territory Government Service (Consequential Provisions) Act 1994</i> • <i>Health Professionals Act 2004</i> • <i>Health Records (Privacy and Access) Act 1997</i> • <i>Human Rights Act 2004</i> • <i>Freedom of Information Act 1989</i> • <i>Territory Records Act 2002 (public records)</i> • <i>Human Rights Act 2004 (right to privacy)</i> • <i>Public Health Act 1997</i> • <i>Workplace Privacy Act 2011</i>
Legislation considered (NT)	<ul style="list-style-type: none"> • <i>Health and Community Services Complaints Act 1998</i> • <i>Health Practitioners Act 2004</i> • <i>Information Act 2002</i> • <i>Public Health (Medical and Dental Inspection of School Children) Regulations 1960</i>

Schedule 3 - Glossary and acronyms

Term	Definition
Access List	means a list of participating organisations the individual has authorised to access their PCEHR. Each organisation includes a level of access: 'general access', 'limited access' and 'revoked'. Consumers which have opted for only basic access controls will not be able to set the level at 'limited access' or 'revoked'. These are advanced features only.
ACIR	means Australian Childhood Immunisation Register, a national register administered by the Department of Human Services Medicare program that records details of vaccinations given to children under seven years of age who live in Australia.
Administration Portal	means a portal to enable Service and Support Agents, Authorized Registration Agents and Call Centre Agents working in one of the channels (eg call centre, Medicare shop front, etc) to assist individuals with registration, help individuals manage their PCEHR, access support information about the PCEHR System and access the contact management service.
advance care directive	means a statement by a competent person expressing decisions about his or her future care should he or she become incapable of participating in medical treatment decisions.
ALRC	means the Australian Law Reform Commission, a federal agency that reviews Australia's laws to ensure they provide improved access to justice for all Australians by making laws and related processes more equitable, modern, fair and efficient.
AODR	means Australian Organ Donor Register, the only national register for organ and/or tissue donation for transplantation. The AODR keeps a record of the individual's donation decision and of the organ and tissue the individual agrees to donate.
APPs	means the Australian Privacy Principles, the privacy principles that will replace the current IPPs (for the Commonwealth public sector) and the NPPs (for the private sector).
ARA	means authorised registration agent, a person who supports assisted registrations. Authorised registration agents may for example work within a Medicare shop front or call centre, or work within registered healthcare provider organisations (for example, in a maternity ward, aged care facility or aboriginal healthcare service).
authentication	means validating that the user wishing to access the PCEHR is who they claim to be. In electronic environments this is achieved by providing a user with a credential such as a user-id + password, a smart card or a one time password device.
authorised representative	<ul style="list-style-type: none"> has the meaning given by section 6 (Definition of authorised

Term	Definition
	representative of a consumer) of the Bill.
Authorised User	means a person authorised by the healthcare organisation to access the PCEHR System on behalf of the participating organisation.
Bill	means the <i>Exposure Draft Personally Controlled Electronic Health Records Bill 2011</i> .
carer	has the same meaning as in the <i>Carer Recognition Act 2010</i> (Cth), as amended from time to time.
CCA	means Compliance, Conformance and Accreditation.
Con Ops	means the Concept of Operations relating to the introduction of a Personally Controlled Electronic Health Record System (NEHTA version number 0.13.6 dated 8 April 2011, version number 0.14.12 dated 12 August 2011).
Consolidated View	means a view intended to provide a summary of an individual's PCEHR. It presents information from the shared health summary and also indicates if other related information from other records is available.
consumer	means an individual who has received, receives or may receive healthcare. This is the same meaning given by section 5 (Definitions) of the Bill.
Consumer-Entered Health Summary	means summary information that a consumer wishes to share with their providers into the PCEHR via the consumer portal or a registered portal operator. The Consumer-Entered Health Summary may contain: <ul style="list-style-type: none"> • Allergies (including the substance/medicine/device name and the reaction they have had to it) (optional). • Medications (including the branded name of the product (optional)).
Consumer Note	means a note provided as a memory aid for individuals and their representatives and are not visible to healthcare providers. The PCEHR System will accept consumer-entered notes as a level 1, 2 or 3 record.
CSP	means a contracted service provider of a healthcare provider organisation that provides: <p>(a) information technology services relating to the PCEHR system; or</p> <p>(b) health information management services relating to the PCEHR system;</p> <p>to the healthcare provider organisation under a contract with the healthcare provider organisation.</p>
Department	means the Department of Health and Ageing.
DHS	means the Department of Human Services (Commonwealth) and includes the Centrelink, Child Support and Medicare programs.
Discharge Summary	means a record that can be used when a consumer is discharged from a healthcare provider organisation. When a healthcare provider creates a

Term	Definition
	Discharge Summary, it will be sent directly to the intended recipient, as per current practices, and a copy of the Discharge Summary may also be sent to the PCEHR System. A Discharge Summary maybe provided as a level 1, 2 or 3 record.
employee	of an entity includes, but is not limited to, the following: <ul style="list-style-type: none"> (a) an individual who provides services for the entity under a contract for services; (b) an individual whose services are made available to the entity (including services made available free of charge).
EOI	means Evidence of Identity.
Event Summary	is a record used to capture key health information about significant healthcare events that are relevant to the ongoing care of an individual. Any participating healthcare provider can submit Event Summaries to the PCEHR System. For example, a dentist, an emergency department, afterhours GP clinic, an outpatient clinic, a community pharmacy or an allied health clinic could use it. An event summary is intended to be the ‘default’ record type and is used when none of the other types of record are appropriate.
Fed IPPs	means the information privacy principles, found in the Privacy Act.
Finance	means the Department of Finance and Deregulation.
healthcare	means: <ul style="list-style-type: none"> (a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it: <ul style="list-style-type: none"> (i) to assess, record, maintain or improve the individual’s health; or (ii) to diagnose the individual’s illness or disability; or (iii) to treat the individual’s illness or disability or suspected illness or disability; or (b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist. <p>Note: This is substantially the same as the definition of health service in the Privacy Act.</p>
healthcare provider	means: <ul style="list-style-type: none"> (a) an individual healthcare provider; or (b) a healthcare provider organisation.
healthcare provider organisation	means an entity that has conducted, conducts, or will conduct, an enterprise that provides healthcare (including healthcare provided free of charge).

Term	Definition
health information	<p>means:</p> <p>(a) information or an opinion about:</p> <ul style="list-style-type: none"> (i) the health or a disability (at any time) of an individual; or (ii) an individual's expressed wishes about the future provision of healthcare to him or her; or (iii) healthcare provided, or to be provided, to an individual; that is also personal information; or <p>(b) other personal information collected to provide, or in providing, healthcare; or</p> <p>(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body 1 parts, organs or body substances; or</p> <p>(d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.</p> <p>Note: This is the same as the definition of health information in the Privacy Act.</p>
HI	means health identifier.
HI Act	means the <i>Health Identifiers Act 2010</i> (Cth).
HI Information Set	<p>means the minimum amount of personal information required by the HI Service Operator to locate the unique IHI for a consumer.</p> <ul style="list-style-type: none"> (i) name; (ii) date of birth; (iii) sex; and (iv) Medicare or DVA file number.
HI-PDS	means HI Provider Directory Service, a voluntary provider directory service provided as part of the HI Service.
HI Service	is a service that enables consistent identifiers to be created for individuals and healthcare providers across the Australian health system through the introduction of unique healthcare identifiers — see IHI, HPI-I and HPI-O.
HI Service Operator	is the Chief Executive, Medicare
HPI-I	means Healthcare Provider Identifier for individuals (HPI-I), a 16 digit unique number used to identify providers who deliver healthcare in the Australian healthcare setting.
HPI-O	means Healthcare Provider Identifier for Providers (HPI-O), a 16 digit unique number used to identify organisations who deliver care in the

Term	Definition
	Australian healthcare setting.
HR Act	means <i>Health Records Act 2011</i> (VIC)
HRIP Act	means <i>Health Records and Information Privacy Act 2002</i> (NSW)
IHI	means Individual Healthcare Identifier (IHI), a 16 digit unique number used to identify individuals who receive care in the Australian Health system.
index service	means the index service maintained by the System Operator for the purposes of the PCEHR system, as mentioned in section 11(a) (Functions of the System Operator) of the Bill.
Index View	means a view listing all records available in a PCEHR.
IVC	means Identity Verification Code
JP	means Justice of the Peace
LIP	means Legislation Issues Paper
MBS	means Medicare Benefits Schedule
NASH	means National Authentication Service for Health, a national digital credential management service for healthcare providers and healthcare organisations.
National Repositories Service	means the service referred to in section 11(h) (Functions of the System Operator) of the Bill.
NEHTA	National E-Health Transition Authority
NOC	means Notice of Connection, a notice issued by the System Operator indicating that a system is ready to connect to the PCEHR System.
nominated healthcare provider	<p>of a consumer means an individual: shared health summary</p> <p>(a) who has agreed with the consumer to be the consumer’s nominated healthcare provider; and</p> <p>(b) in relation to whom a healthcare identifier has been assigned under paragraph 9(1)(a) of the Healthcare Identifiers Act 2010; and</p> <p>(c) who is one of the following:</p> <ul style="list-style-type: none"> (i) a medical practitioner within the meaning of the National Law; (ii) a registered nurse within the meaning of the National Law; (iii) an Aboriginal health practitioner, a Torres Strait Islander health practitioner or an Aboriginal and Torres Strait Islander health practitioner within the meaning of the National Law; (iv) an individual prescribed by the regulations for the purposes of this subparagraph.
nominated representative	of a consumer means an individual who has agreed with the consumer to be the consumer’s nominated representative for the purposes of their

Term	Definition
	PCEHR.
NPPs	means the national privacy principles, found in the Privacy Act.
NSW HPPs	means the health privacy principles, found in the HRIP Act.
NSW IPPs	means the information protection principles, found in the PPIP Act.
NT IPPs	means the information privacy principles, found in the Information Act (NT).
OAIC	means the Office of the Australian Information Commissioner.
OMO	means Organisation Maintenance Officer, a person within an organisation responsible for maintaining information about the organisation within the HI Service, as defined in the HI Act.
PACC	means a code (ie PIN or passphrase) an individual can provide to an authorised user in order to have the participating organisation added to the Access List.
PACCX	means a code (ie PIN or passphrase) an individual can provide to an authorised user in order to have the participating organisation to have access to 'limited access' records.
participant in the PCEHR system	means any of the following: <ul style="list-style-type: none"> (a) the System Operator; (b) a registered healthcare provider organisation; (c) the operator of the National Repositories Service; (d) a registered repository operator; (e) a registered portal operator; (f) a registered contracted service provider, so far as the contracted service provider provides services to a healthcare provider.
Pathology Result Report	means a report that supports collection of Pathology Result Reports. An essential requirement of the PCEHR System is to ensure that appropriate Pathology Result Reports are released to the PCEHR System after a healthcare provider has reviewed them, as per current clinical practice.
PBS	means an Australian Government scheme aimed at providing all Australians with affordable access to a wide range of prescription medicines.
PCEHR	means a personally controlled electronic health record.
PCEHR Rules	has the meaning given by section 97 (Minister may make PCEHR Rules) of the Bill.
PCEHR System	means a system: <ul style="list-style-type: none"> (a) that is for: <ul style="list-style-type: none"> (i) the collection, use and disclosure of information from many sources

Term	Definition
	<p>using telecommunications services and by other means, and the holding of that information, in accordance with consumers' wishes or in circumstances specified in this Act; and</p> <p>(ii) the assembly of that information using telecommunications services and by other means so far as it is relevant to a particular consumer, so that it can be made available, in accordance with the consumer's wishes or in circumstances specified in this Act, to facilitate the provision of healthcare to the consumer or for purposes specified in this Act; and</p> <p>(b) that involves the System Operator.</p>
personal information	has the same meaning as in the Privacy Act.
personally controlled electronic health record	<p>of a consumer means the record of information that is created and maintained by the System Operator in relation to the consumer, and information that can be obtained by means of that record, including, but not limited to, the following:</p> <p>(a) information included in the entry in the Register that relates to the consumer;</p> <p>(b) health information connected in the PCEHR system to the consumer (including information included in a record accessible through the index service);</p> <p>(c) other information connected in the PCEHR system to the consumer, such as information relating to auditing access to the record.</p>
PES	means the Prescription Exchange Service.
PORO	means Proof of Record of Ownership, a process used to validate evidence (eg in the form of shared knowledge/secrets of documentary) and used to substantiate that the presenting party has an existing relationship with the relying party (is already the 'owner' of a digital identity on the relying party's system).
PIIP Act	means <i>Privacy and Personal Information Protection Act 1998</i> (NSW).
Prescribing and Dispensing information	<p>includes information relating to a consumer's prescriptions. The PCEHR System will enable the collection of Prescribing and Dispensing information.</p> <p>Participating prescribers and dispensers who have access to the PCEHR System will be able to upload a copy of Prescription and Dispensing information to the PCEHR System. This information is a copy of information that is also sent to the Prescription Exchange Service (PES).</p>
Privacy Act	means the <i>Privacy Act 1988</i> (Cth).
Provider Portal	complements existing local health record systems by providing an alternative form of access to the PCEHR. In the first release the Provider Portal will be primarily a read-only system. Records can only be created from Clinical systems. Access to the Provider Portal by healthcare providers needs to be authorised by the participating healthcare organisation.

Term	Definition
record	includes a database, register, file or document that contains information in any form (including in electronic form).
registered healthcare provider organisation	means a healthcare provider organisation that is registered under section 38 (Registration of a healthcare provider organisation) of the Bill.
registered portal operator	means a person that: <p>(a) is the operator of an electronic interface that facilitates access to other parts of the PCEHR system; and</p> <p>(b) is registered as a portal operator under section 43 (Registration of a repository operator, a portal operator or a contracted service provider) of the Bill.</p>
registered repository operator	means a person that: <p>(a) holds, or can hold, records of information included in personally controlled electronic health records for the purposes of the PCEHR system; and</p> <p>(b) is registered as a repository operator under section 43 (Registration of a repository operator, a portal operator or a contracted service provider) of the Bill.</p>
registration	means the processes associated with the creation by a consumer of their PCEHR. Registration will include processes covering verification of identity and evidence of entitlement (ie meeting the criteria for participation, such as having an IHI).
report	means data extracted from one or more records from one or more PCEHRs for reporting purposes.
Revoked List	means a list that enables individuals to mark organisations on their Access List as being 'revoked'. <p>If an organisation is marked as being 'revoked', then they will not be able to access the individual's PCEHR, unless the individual either provides them with a PACC or they use emergency access. The other option is for the individual to change the organisations access level via the consumer portal. An individual does not need to set up a PACC to use this feature.</p>
SaaS	means software that is either supplied as a cloud based service or deployed over the Internet to run locally. Licenses and support for SaaS systems are commonly provided on a subscription basis, but other models are also used.
shared health summary	means a record that is: <p>(a) prepared by the consumer's nominated healthcare provider; and</p> <p>(b) described by the consumer's nominated healthcare provider as the consumer's shared health summary.</p>
Specialist Letter	includes a record created by a Specialist. The PCEHR System will support the collection of Specialist Letters. When a specialist creates a

Term	Definition
	Specialist Letter, it will be sent directly to the intended recipient, as per current practices, and a copy of the Specialist Letter may also be sent to the PCEHR System.
System Operator	has the meaning given by section 10 (Identity of the System Operator) of the Bill.
Tas PIPPs	means the personal information protection principles, found in the Personal Information Protection Act 2004 (TAS).
TDS	means Trusted Data Source.
TIS	means the Australian Government Translating and Interpreting Service.
Vic HPPs	means the health privacy principles, found in the HR Act.
View	includes data extracted from one or more records within an individual's PCEHR for the purposes of supporting the information needs of an individual or healthcare provider.

About the authors

1. Minter Ellison

Minter Ellison is one of the largest full-service law firms in the Asia Pacific region, with more than 290 partners and 1,000 legal staff working throughout Australia, the People's Republic of China, New Zealand and the United Kingdom. Minter Ellison's experience in the health sector covers both corporate and Government clients. We represent over 150 different government departments, agencies and statutory authorities at federal, state, territory and local government levels, throughout Australia, New Zealand and the Asia Pacific including in the health sector.

2. Salinger Privacy

This report has been prepared with the assistance of Anna Johnston, Director of Salinger Privacy.

Ms Johnston was previously the Deputy Privacy Commissioner of NSW. She holds a first class honours degree in Law, a Masters of Public Policy with honours, a Graduate Certificate in Management, a Graduate Diploma of Legal Practice, and a Bachelor of Arts. Ms Johnston was admitted as a Solicitor of the Supreme Court of NSW in 1996, and is an accredited mediator.