



Australian Government
Department of Health

Privacy Impact Assessment Report – Personally Controlled Electronic Health Record (PCEHR) System Opt-Out Model

The following report is the result of a Privacy Impact Assessment (PIA) commissioned in late 2014 to analyse the flows of personal information and potential privacy risks and impacts of implementing an opt-out approach for participation in the PCEHR as was recommended in the Review of the Personally Controlled Electronic Health Record (PCEHR). The PIA was commissioned following the stakeholder consultations held between July and September 2014, and intended to inform the consideration of options for the implementation of the opt-out recommendation.

The Review of the PCEHR recommended that the PCEHR system transition from an opt-in to an opt-out system for individual participation in the PCEHR system at a national level. This PIA considers the implications of a national opt-out system, and also makes a range of recommendations that would be appropriate at a national level. In conducting this PIA, a range of assumptions have been used to determine the possible flows of information as well as the processes for communication and opting out of the system.

Many of the findings in this PIA have been used in forming the approach to trialling participation arrangements, including opt-out as announced in the 2015-16 Federal Budget. It has also been used to frame the proposed legislative amendments and planning for the trials.

Work is underway with states and territories and Primary Healthcare Networks on the trial site selection, and further detailed planning including the evaluation criteria and methodology. A further PIA will be undertaken specifically for the opt-out trials as funded in the 2015-16 Federal Budget, and will be made available once accepted by the Department of Health.

Privacy Impact Assessment Report

Personally Controlled Electronic Health Record (PCEHR) System Opt-Out Model

Prepared for the Department of Health

20 May 2015

MinterEllison

PIA Report – PCEHR System Opt-Out Model

Table of Contents

Executive Summary	6
Chapter 1 About this report	7
1.1 Scope of this PIA	7
1.2 How should this PIA be used?	8
1.3 The process of assessing privacy impacts	10
1.4 Maintaining adequate security arrangements	12
1.5 Qualifications and assumptions	12
Chapter 2 Description of current PCEHR system	14
2.1 Overview of the current PCEHR system (Opt-In Model)	14
2.2 Key design features of the current PCEHR system	14
2.3 What information is stored in a PCEHR?	16
2.4 Participants in the PCEHR system	17
Chapter 3 Description of Opt-Out Model	18
3.1 Background to the Opt-Out Model proposal	18
3.2 Changes under the Opt-Out Model	19
3.3 Privacy protection mechanisms	20
3.4 Automatic registration	21
3.5 Implementation of Opt-Out Model	22
3.6 Information flows relating to Opt-Out Model	23
3.7 Community expectations	23
Chapter 4 Communicating the opt-out choice	30
4.1 Communications strategy	30

4.2 Privacy risk - collection transparency	31
Chapter 5 Opt-out process	37
5.1 Opt-out channels	37
5.2 Overview of the Online Opt-Out Service	38
5.3 Identity verification	38
5.4 Identifying dependants and existing PCEHRs	43
5.5 Making opt-out and/or cancellation decision	46
5.6 Cancellation of existing PCEHR	47
5.7 Opt-out notification	47
5.8 Telephone and face to face channels	49
5.9 Mail channel	49
Chapter 6 Automatic registration (existing individuals)	50
6.1 Overview of automatic registration process (opt-out transition)	50
6.2 Identification of Automatic Registrants	50
6.3 Creation of shell PCEHR	53
6.4 Privacy control settings	53
6.5 Pseudonymous PCEHR registration	58
Chapter 7 Automatic registration of new Medicare enrolments and IHI registrants	59
7.1 Overview of automatic registration of new Medicare enrolments and IHI registrants	59
7.2 Making the opt-out decision	60
7.3 Submitting the forms	63
7.4 Implementing the opt-out decision	65
7.5 Automatic registration of new persons	66

7.6 Privacy controls	67
Chapter 8 Content and access to records	68
8.1 PCEHR content	68
8.2 Individual access to PCEHR	69
8.3 Data quality	72
8.4 Data security	74
8.5 Privacy complaints, penalties and redress for harm	81
Chapter 9 Conclusions	90
9.1 The Privacy Positives	90
9.2 Privacy risks and recommendations	91
Schedule 1 – Detailed information flows: Online Opt-Out Service	100
Schedule 2 – Detailed information flows: Automatic registration	107
Schedule 3 – Detailed information flow: Automatic registration of new Medicare and IHI registrants	111
Schedule 4 – Current participants in the PCEHR system	117
1. Individual participants	117
2. Healthcare participants	119
3. PCEHR System infrastructure providers/operators	121
Schedule 5 – Sources of information	124
1. Publicly available information	124
2. Information provided by the Department of Health	124
3. Legislation	125
Schedule 6 – Summary of the APPs	126
1. Collection of personal information	126
2. Use and disclosure	127
3. Data quality	127
4. Data security	127
5. Access and correction	127

Schedule 7 – Glossary and acronyms	128
About the authors	135

Executive Summary

A Privacy Impact Assessment (**PIA**) is a detailed analysis of the flows of personal information and potential privacy risks and impacts of a project. The purpose of conducting a PIA is to add value to projects that involve the handling of personal information by mitigating privacy risks, ensuring compliance with legal obligations, and building best privacy practice into a project.

Background

Recommendation 13 of the *Review of the Personally Controlled Electronic Health Record (December 2013)* conducted by Mr Richard Royle, Dr Steve Hambleton and Mr Andrew Walduck (**the PCEHR Review Report**) recommended that the PCEHR system transition from an opt-in to an opt-out model for individual participation.

This PIA assesses a proposal to transition to an opt-out model, for the registration of individuals in the PCEHR system, on a national basis (**Opt-Out Model**). No decision has been made to implement opt-out for individuals on a national basis. Subject to government agreement and relevant legislative amendments, the Department of Health (**the Department**) proposes to implement trials of different individual participation arrangements, including opt-out. Separate privacy analysis will be undertaken of issues arising in relation to trials. Registration of healthcare provider organisations, and other participants such as repository operators, under the *Personally Controlled Electronic Health Records Act 2012* (**PCEHR Act**) will continue to be on an opt-in basis.

PIA recommendations

Our recommendations are set out in full in Chapter 9. The key privacy risks to which our recommendations relate include:

- ensuring that individuals are made aware (through communications and collection notices) how their personal information will be handled and by whom, and how to opt-out or adjust privacy control settings, so they can make informed decisions in relation to the management of their privacy; and
- ensuring that the use and disclosure of identifying information and healthcare identifiers by the System Operator, HI Service Operator and Medicare are addressed and given legislative authorisation under the proposed amendments to the PCEHR Act and the *Healthcare Identifiers Act 2010*.

Minter Ellison

Date: 20 May 2015

Chapter 1 About this report

1.1 Scope of this PIA

1.1.1 What does this PIA cover?

- (a) The purpose of this report is to:
 - (A) analyse the possible new impacts on the privacy of individuals' personal information in an Opt-Out Model, by reference to the Australian Privacy Principles (APPs); and
 - (B) identify and recommend options for managing, minimising or eliminating any new negative impacts.
- (b) This PIA assesses:
 - (i) privacy impacts of moving from a consent-based model for the collection, use and disclosure of personal information within the PCEHR system, to a model where the collection, use and disclosure of personal information is authorised by legislation;
 - (ii) the collection and handling of personal information about third parties in the context of additional security measures that will be implemented as part of the Opt-Out Model; and
 - (iii) updates to existing public-facing privacy material (e.g. privacy notices and information booklets) for the PCEHR system relating to the Opt-Out Model.
- (c) This PIA examines the privacy impacts of implementing the Opt-Out Model, having regard to the following:
 - (i) the type, amount and scope of personal information to be collected, recorded, stored, used and disclosed;
 - (ii) the necessity for collecting the personal information;
 - (iii) the likely disclosure of, and regimes providing access to, personal information collected by the System Operator and the HI Service Operator;
 - (iv) organisations that will receive and/or share the personal information collected; and
 - (v) compliance with obligations with respect to privacy law.

1.1.2 What is not in scope for this PIA

This PIA report does not assess:

- (a) the PCEHR system as a whole, or the existing functionality of the PCEHR system;
- (b) the myGov system which individuals can use to access their PCEHR;
- (c) the collection, use or disclosure of metadata by the System Operator;
- (d) the application of, or compliance with, restrictions on the handling of information under the PCEHR Act, the *Healthcare Identifiers Act 2010 (HI Act)*, the *Health Insurance Act 1973* or the *National Health Act 1953*, other than the extent to which the collection, use and disclosure of personal information will be, or will need to be, 'authorised or required by law' pursuant to those secrecy provisions for the purposes of APPs 3.4(a), 3.6(a)(ii) and 6.2(b);

- (e) compliance with State or Territory health legislation, privacy or secrecy laws; and
- (f) the adequacy of security arrangements for the Opt-Out Model. While ensuring appropriate data security is a critical privacy principle, expert assessment of the adequacy of information security arrangement will be required as the project moves towards a more detailed operational level of design.

1.2 How should this PIA be used?

1.2.1 Summary

- (a) This report provides:
 - (i) an assessment of the proposed controls and safeguards in the design and governance models for the Opt-Out Model;
 - (ii) an identification of risk areas in relation to compliance with the APPs and community expectations; and
 - (iii) recommendations to address those risks by minimising privacy intrusions and maximising privacy protections within the design, policies and procedures for the Opt-Out Model.
- (b) This report is intended as a resource for the Department to assist in finalising the design, legislation and governance of the Opt-Out Model.
- (c) This PIA can also be used to further inform and educate those involved in the design of guidelines, individual communications, educational materials for users, staff training, system design and program evaluation.

1.2.2 Structure and content of this report

- (a) Chapter 3 of this PIA report provides the background and overview of, and the information flows involved in, the Opt-Out Model. The Schedules to this report describe the information flows relating to the following processes:
 - (i) in relation to the transition (for individuals who currently have a verified IHI):
 - (A) the opt-out process via the Online Opt-Out Service (Schedule 1); and
 - (B) automatic registration (Schedule 2); and
 - (ii) registration of individuals who register for Medicare, and other individuals who apply for an IHI (Schedule 3).
- (b) Chapter 4 to Chapter 8 assess the information flows at each stage of the implementation of the Opt-Out Model, and contains findings and recommendations with respect to the privacy impacts in relation to individuals whose personal information is collected, used and disclosed by the System Operator.
- (c) Our conclusions are set out at Chapter 9, which draw on significant themes identified from our analysis and recommendations.

1.2.3 Nature of recommendations

- (a) This PIA report does not provide an opinion on the severity or degree of significance of any particular privacy risk.
- (b) If the Department wishes to undertake a further risk assessment in relation to any of the identified privacy risks, it could consider applying AS/NZS ISO 31000.¹ 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); and
 - (iii) assess the likelihood of the risk event arising and the consequences of the event arising by reference to the specified objectives.

1.2.4 Methodology

- (a) To produce this PIA report, we have examined documents provided to us by the Department, and have had discussions and correspondence with relevant officers of the Department's project team. These documents and discussions are set out in Schedule 5.
- (b) We have not considered any other existing privacy policies, guidelines or manuals, directions, or other internal or administrative documents of the Department or other participants in the PCEHR system.
- (c) We have not directly undertaken consultation with other external agencies, stakeholders or interest groups.

1.2.5 Terminology

- (a) Unless indicated otherwise:
 - (i) references to an 'individual' means a natural person who receives, has received or may receive healthcare; and
 - (ii) terms used in this report which are defined in the PCEHR Act have the same meaning as in the PCEHR Act.
- (b) The 'System Operator' is defined in section 14 of the PCEHR Act as the Secretary of the Department, however in practice the functions and activities of the System Operator are undertaken by the following entities:
 - (i) officers of the Department (delegated by the System Operator);
 - (ii) the Chief Executive Medicare (delegated by the System Operator);
 - (iii) officers in the Department of Human Services (**DHS**) (sub-delegated by the Chief Executive Medicare); and
 - (iv) Accenture, contracted by the System Operator as the National Infrastructure Operator (**NIO**).

¹ Risk management – Principles and Guidelines.

- (c) We also note that DHS officers act in a number of different capacities. For ease of reference and clarity, this report uses the following terms to refer to certain entities.

Term	Definition
Medicare	means the Chief Executive Medicare acting through delegated officers of DHS performing Medicare-related functions under the National Health Act and Health Insurance Act
HI Service Operator	means the HI Service Operator acting through delegated officers of DHS
System Operator (Health)	means the System Operator acting through delegated officers of the Department
System Operator (DHS)	means the System Operator acting through DHS officers, who have been subdelegated by the Chief Executive Medicare
System Operator (NIO)	means the System Operator acting through NIO as its contracted service provider

- (d) Other terms and acronyms used in this PIA report are defined in Schedule 7.

1.3 The process of assessing privacy impacts

1.3.1 Privacy principles used in this assessment

- (a) Privacy is a broader and more flexible concept than confidentiality. Personal information privacy generally refers to a person's ability to control how their personal information is handled (i.e. collected, stored, accessed, checked, used and disclosed) throughout the life cycle of that information.
- (b) Identifying privacy impacts and risks involves an examination of how the Opt-Out Model will *'affect the choices consumers have regarding how information about them is handled, the potential degree of intrusions into the private lives of consumers, compliance with privacy law, and how the project fits into community expectations.'*²
- (c) The Opt-Out Model proposal is assessed in Chapter 5 to Chapter 8 at each point during the transition, and new information flows relating to the registration of new individuals after that period. The assessment is made with respect to compliance with the *Privacy Act 1988* (Cth) (**Privacy Act**), and whether the proposal can meet community expectations.
- (d) 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, which also draws together our conclusions about the privacy impacts – both positive and negative – and risks of the Opt-Out Model.

1.3.2 What are the privacy laws?

- (a) Privacy laws in Australia present a fractured and imperfect picture.
- (b) This PIA report considers the privacy impacts by reference to the APPs, which are summarised in Schedule 6.

² Office of the Privacy Commissioner, *Privacy Impact Assessment Guide*, August 2006, p.xxi.

- (c) The APPs apply to various entities involved in the PCEHR system which handle personal information, including the System Operator, HI Service Operator, Medicare, and all private sector healthcare provider organisations.

1.3.3 What does this PIA consider?

- (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 individuals in society.
- (b) This PIA considers compliance with the APPs, but also community expectations.
- (c) 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.
- (d) For example, under APP 6 there is a general presumption against using or disclosing personal information for purposes other than the purpose for which the information was collected. However, those general principles are waived in certain situations, for example where the use or disclosure is required or authorised by or under law.³
- (e) Therefore, where the proposal undergoing assessment includes enabling legislation, for the most part compliance with the privacy laws will come once that enabling legislation is in force.
- (f) In this regard, we note that:
 - (i) the PCEHR Act and the HI Act currently provide for a number of authorisations for participants in the PCEHR system to collect, use and disclose health information, healthcare identifiers and identifying information (as defined); and
 - (ii) the proposed legislative amendments to the PCEHR Act and the HI Act will provide legislative authority for the collection, use and disclosure of information which is currently based on consent.

1.3.4 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.*⁴
- (c) Furthermore, community expectations about what constitutes an invasion of privacy are not necessarily reflected in the law.

³ APP 6.2(b).

⁴ Malcolm Crompton, "The Trust Cluster", December 2005, p.3; available from the [Information Integrity Solutions website](#) at www.iispartners.com

- (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 the PCEHR system.
- (e) For the purposes of this PIA, our conclusions about the most likely community expectations are based on:
 - (i) submissions made to the PCEHR Review; and
 - (ii) the draft Deloitte *Report on the public consultation into the Review of the PCEHR*; and
 - (iii) the results of community attitude surveys conducted on behalf of the Australian Privacy Commissioner.

1.3.5 Making recommendations

- (a) A PIA should 'identify avoidable risks and suggest means to remove them or reduce them to an appropriate level'.⁵
- (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 operations.

1.4 Maintaining adequate security arrangements

- (a) APP 11 requires agencies to take 'such steps as are reasonable in the circumstances' to maintain the security of the personal information the agency holds.
- (b) While this PIA assesses security features from an information flow perspective (that is, who receives what information, and to what extent do the security features prevent unauthorised persons from handling personal information they should not handle), this PIA does not assess the adequacy of information security arrangements for the Opt-Out Model.
- (c) In order to ensure appropriate data security, expert assessment of the adequacy of information security arrangements should be obtained by the Department.

1.5 Qualifications and assumptions

- (a) This PIA report is subject to the following qualifications and assumptions:
 - (i) any collections, uses and disclosures of personal information required for the Opt-Out Model processes that currently occur on a consent basis will be given legislative authority under the proposed amendments to the PCEHR Act and HI Act (but consent requirements for other aspects of the PCEHR system will not be affected⁶);
 - (ii) we have not undertaken any consultations or investigations other than those set out in the Methodology at section 1.2.4;

⁵ Office of the Privacy Commissioner, *Managing Privacy Risk*, November 2004, p.17.

⁶ For example, section 69(4) of the PCEHR Act.

- (iii) we have not considered any existing privacy policies, guidelines or manuals, directions, or other internal or administrative documents relating to the PCEHR system, other than any documents identified in Schedule 5;
 - (iv) the Online Opt-Out Service will be managed by DHS as delegate of the System Operator;
 - (v) privacy controls will not be able to be set through the Online Opt-Out Service – this will be done through myGov; and
 - (vi) while the System Operator role may transfer from the Secretary of the Department to a new Commonwealth statutory authority (the Australian Commission for Electronic Health (**ACEH**)), we have not reviewed whether this will affect the operation of the system or governance arrangements from a privacy perspective.
- (b) This PIA is based on a number of assumptions about how the Opt-Out Model will be implemented, and the final system design may not reflect the system described in this PIA.

Chapter 2 Description of current PCEHR system

2.1 Overview of the current PCEHR system (Opt-In Model)

- (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 an individual's medical history, stored and shared in a network of connected systems. The PCEHR brings key health information from a number of different systems together and presents it in a single view.
- (c) Information in a PCEHR can be accessed by the individual or their authorised representative, or nominated representatives appointed by the individual. The information is also accessible to healthcare providers who are providing healthcare to the individual, and are authorised by the individual to access their PCEHR or documents in the PCEHR.
- (d) The PCEHR system itself is a network of connected systems which allows the electronic records of a registered individual's medical history to be stored and shared. The PCEHR system does not hold all the information held in an individual's health records, but rather complements the records held by the individual's healthcare providers by making available key information and indexing records held by the National Repositories Service and registered repository operators.
- (e) The PCEHR system relies on healthcare identifiers, which are 16 digit unique numbers assigned to individuals, healthcare provider organisations (HPI-Os) and healthcare provider individuals (HPI-Is) by the HI Service Operator,⁷ to support the accurate linkage of clinical documents to individuals and providers.
- (f) The PCEHR system was commissioned in July 2012, and has approximately 2 million individuals currently registered with a PCEHR.

2.2 Key design features of the current PCEHR system

- (a) As at April 2015, the key functionality of the PCEHR system comprises the following components:
 - (i) registration of individuals;
 - (ii) recognition of authorised representatives of individuals;
 - (iii) registration of healthcare provider organisations;
 - (iv) registration of repository operators and other participants, such as contracted service providers;
 - (v) creation of a PCEHR for individuals that:
 - (A) enables privacy controls to be set by individuals, their authorised representative(s), and those nominated representatives who have been given the ability to set controls (i.e. full-access nominated representatives);

⁷ We understand that in practice, the Australian Health Practitioner Regulation Agency (**AHPRA**) assigns healthcare identifiers to HPI-Is pursuant to subsection 9(2) of the HI Act.

- (B) can be populated with information drawn from Medicare regarding the individual's prescriptions (from Pharmaceutical Benefits Scheme (**PBS**) or Repatriation Pharmaceutical Benefits Scheme (**RPBS**) data), healthcare provider visits (from Medicare Benefits Schedule (**MBS**) or Department of Veterans' Affairs (**DVA**) claims data), immunisations (from the Australian Childhood Immunisation Register (**ACIR**)) and organ donor status (from the Australian Organ Donor Register (**AODR**));
- (C) allows individuals or their authorised representatives to view, upload and remove information, including Personal Health Summaries, Advanced Health Directive Custodian and emergency contact details;
- (D) enables healthcare providers to view and upload information, including Shared Health Summaries, Event Summaries, Discharge Summaries and prescription and dispense information; and
- (E) allows nominated representatives to view (and in the case of full access nominated representatives, to upload and remove) information in the PCEHR.

(b) Key design features of the current PCEHR system are explained in the table below.⁸

The PCEHR system	
is <i>voluntary</i> – if an individual or healthcare provider organisation wants to participate, they need to register with the system.	and not <i>compulsory</i> – both individuals and healthcare provider organisations choose whether or not to participate.
is <i>an enhancement to medical treatment</i> – the PCEHR system allows an individual'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> – an individual's PCEHR may include a shared health summary (which contains basic health information about an individual), and records may be added to that individual's PCEHR.	and not <i>a replacement for normal sharing of information between an individual 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 individual's health, rather than as the complete and authoritative source of current information.
is <i>an information system</i> – where participating healthcare provider organisations can access additional records during a consultation with an individual.	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 individual.

⁸ The table is extracted from: Con Ops, section 2.3 (Vision and concept)

The PCEHR system	
<p>is</p> <p><i>aligned with current privacy obligations</i> – healthcare providers have the same responsibilities in relation to privacy of information in PCEHRs as they currently do in relation to clinical information from other sources.</p>	<p>and not</p> <p><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 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.</p>
<p>is</p> <p><i>a distributed system of service providers working in concert</i> – government and private sector organisations work together to deliver the PCEHR system to individuals and healthcare providers. The PCEHR system is underpinned by a legislative framework that imposes appropriate controls and standards on all the delivery bodies.</p>	<p>and not</p> <p><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.</p>

2.3 What information is stored in a PCEHR?

- (a) As noted above, the PCEHR brings key health information from a number of different systems together and presents it in a single view. The PCEHR system does not hold all the information held in an individual's health records, but rather is intended to complement the records held by the individual's healthcare providers.
- (b) The information comprised in an individual's PCEHR will depend on the circumstances of the individual, such as their access and upload preferences, whether they upload information themselves, and whether they encourage their healthcare providers to upload information.
- (c) Currently, the PCEHR system supports the inclusion of the following information in a PCEHR:⁹
 - (i) ***individual-uploaded information*** – personal details, personal health notes, personal health summaries, emergency contact details, and childhood development information;
 - (ii) ***healthcare provider-uploaded information*** – discharge summaries, event summaries, referral letters, shared health summaries, specialist letters, pathology reports, and diagnostic imaging reports; and
 - (iii) ***registered repository operator-uploaded information*** – MBS, DVA, PBS, RPBS, AODR and ACIR information, and prescription and dispense information.

⁹ This information is extracted primarily from the [Glossary of Terms available on the eHealth website](http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/Content/glossary) (<http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/Content/glossary>)

2.4 Participants in the PCEHR system

- (a) Information in a PCEHR can be accessed by the individual or their authorised representative(s) and the nominated representative(s) the individual appoints.
- (b) Information in a PCEHR is also accessible to healthcare providers who are providing healthcare to the individual, and are authorised by the individual to access their PCEHR or documents in the PCEHR.
- (c) Summaries of the individual participants, healthcare participants and PCEHR system infrastructure providers and operators are set out in Schedule 4.

Chapter 3 Description of Opt-Out Model

3.1 Background to the Opt-Out Model proposal

3.1.1 PCEHR Review

- (a) The PCEHR Review Report noted that, despite the increasing number of individuals being registered for a PCEHR, the level of utilisation of the PCEHR system had plateaued. This utilisation is measured in the frequency that healthcare provider organisations and individuals access the PCEHR system, and view documents that are uploaded into the system.
- (b) To address this issue the PCEHR Review Report made a number of recommendations, including:
 - (i) changing the name of the PCEHR to 'My Health Record' or similar (recommendation 1);
 - (ii) changing the governance of the PCEHR system (recommendations 2 to 10);
 - (iii) moving to an opt-out model (recommendations 13 and 14); and
 - (iv) increasing the medical content that is uploaded to an individual's PCEHR (recommendations 19 to 22).
- (c) The PCEHR Review Report stated that implementing a 'minimum composite of records' to be included in individuals' PCEHRs, and transitioning to an Opt-Out Model would *'dramatically improve the value proposition [of the PCEHR system] for clinicians'*.¹⁰

3.1.2 Current state of play

- (a) To date, approximately 2 million people have registered for a PCEHR.
- (b) The low individual uptake has discouraged healthcare provider organisations from registering given that, on average, only 2 in every 23 patients are likely to have a PCEHR.

3.1.3 Benefits of an Opt-Out Model

- (a) Implementing an Opt-Out Model is expected to achieve improved health outcomes and other benefits across the healthcare system, including reduced costs, by dramatically increasing the number of individuals with an eHealth record that can be shared between healthcare providers.
- (b) The perceived benefits of moving to an Opt-Out Model for individuals include the following:
 - (i) giving individuals access to a PCEHR without having to take any action, which will particularly assist vulnerable individuals who experience challenges in accessing timely and appropriate healthcare;
 - (ii) greater access to information for treating providers for a wider range of individuals, which should lead to improved coordination and provision of healthcare;
 - (iii) improve access to health records for a wider range of individuals, enabling treating healthcare providers to access their records wherever the individual travels in Australia; and

¹⁰ PCEHR Review Report, page 36.

- (iv) healthcare providers will be able to access an individual's record without having to obtain as much information from third party sources, leading to reductions in time spent, cost and number of healthcare visits required by individuals and family members/dependants as unnecessary and duplicate visits and tests are reduced.
- (c) Potential benefits for healthcare providers and other stakeholders include the following:
 - (i) increased efficiency and better management in the provision of healthcare, as providers will have access to more complete and consistent information;
 - (ii) cost savings for healthcare provider organisations that currently provide assisted registration as there will be a reduced need to spend time assisting individuals to register; and
 - (iii) the quality (and potentially price) of clinical solutions offered to healthcare providers may improve as a result of increasing competition between suppliers of those solutions.

3.2 Changes under the Opt-Out Model

- (a) The key change in moving from an Opt-In to an Opt-Out Model is that individuals will be registered for a PCEHR unless they indicate otherwise. This is a significant policy shift which will affect every Australian.
- (b) Other key changes include that, for individuals registered through the transition process, unless the individual indicates otherwise by the end of the Transition Period, from the time of first access to the PCEHR by the individual or a healthcare provider, the individual's Medicare data will be included in the individual's PCEHR as follows:
 - (i) MBS – future and past two years (from time of first access by the individual or a healthcare provider);
 - (ii) DVA – future and past two years (from time of first access by the individual or a healthcare provider);
 - (iii) PBS – future and past two years (from time of first access by the individual or a healthcare provider);
 - (iv) RPBS – future and past two years (from time of first access by the individual or a healthcare provider);
 - (v) ACIR – all; and
 - (vi) AODR – all.
- (c) There will be no change to:
 - (i) the participants in the PCEHR system;
 - (ii) the types of personal information (including health information) held in the PCEHR – although there will be greater content due to the increase in individuals from 2 million to more than 23 million (less those who opt-out of PCEHR registration);
 - (iii) the existing processes for cancelling the registration of an individual; or
 - (iv) the existing processes for re-registering an individual after the Transition Period.
- (d) A recent change which forms part of the context for this PIA is that, from December 2014, pathology and diagnostic imaging information (but not the images themselves) can be

included in a PCEHR. Although this does not represent a change to the types of information (i.e. health information) currently held in PCEHRs, the content is richer.

3.3 Privacy protection mechanisms

- (a) There are a number of existing technical and legislative measures aimed at protecting privacy which will be retained under an Opt-Out Model. These include the following:
 - (i) **Legislative measures:** The PCEHR Act contains provisions which limit the circumstances in which certain information (including health information) may be collected, used or disclosed, as well as civil penalty provisions in relation to non-compliance with those restrictions. In addition:
 - (A) the PCEHR Act provides for mandatory data breach notification requirements;¹¹ and
 - (B) a contravention in connection with health information included in an individual's PCEHR, or a provision in Part 4 or 5 of the PCEHR Act, constitutes an 'interference with privacy' for the purposes of the Privacy Act, and may be investigated by the Privacy Commissioner.
 - (ii) **Technical measures:** There are three key technical measures of the PCEHR system which limit the ability of people to collect, use and disclose information included in an individual's PCEHR otherwise than for the provision of healthcare to the individual:
 - (A) **privacy control settings:** Individuals have the ability to take control of their PCEHR in the following ways:
 - (I) **'access controls'** – controlling who can view the PCEHR or certain documents;
 - (II) **'content controls'** – managing the content of the PCEHR, for example whether to allow the flow of Medicare-provided data, or the inclusion or removal of a particular clinical document; and
 - (III) **'notification settings'** – ensuring that the individual is notified of certain events, for example the first time a healthcare provider accesses the individual's PCEHR.
 - (B) **locating an individual's PCEHR:** In order for a healthcare provider to access an individual's record, they must first locate that record by providing the individual's IHI, or certain details about the individual (i.e. first name, last name, date of birth, sex and Medicare/DVA card number). This is a privacy positive measure as it reduces the risk of a healthcare provider 'trawling' through the PCEHR system to find records relating to individuals who are not the healthcare provider's patients.
 - (C) **access log:** The PCEHR system records access to an individual's PCEHR by a healthcare provider, individual or representatives, and actions undertaken. This information is made available to the individual in their access log. This is also a privacy positive as it informs an individual about who has accessed their PCEHR, and alerts them to any unauthorised or improper activity.

¹¹ PCEHR Act, section 75.

- (b) In addition, it is proposed that legislative and technical amendments will provide additional privacy protection enhancements, for example:
 - (i) replacing the contractual obligations on registered healthcare provider organisations and contracted service providers to comply with the PCEHR Act and PCEHR Rules with a legislative obligation;
 - (ii) providing a clear statutory power for the System Operator to deal with personal information for security purposes; and
 - (iii) adding a new notification privacy control setting, to allow individuals to say if they want to be notified every time their PCEHR is accessed.

3.4 Automatic registration

- (a) The implementation of the Opt-Out Model and automatic registration of individuals will be given legislative authority through amendments to the PCEHR Act and HI Act.
- (b) All individuals who have an active IHI status and verified IHI record status will be registered for a PCEHR, other than individuals who:
 - (i) indicate in the Opt-Out Period that they do not want to be registered for a PCEHR;
 - (ii) are already registered for a PCEHR; or
 - (iii) were registered for a PCEHR but cancelled their registration before the end of the Opt-Out Period.
- (c) Minors and people with limited or no capacity to make their own decisions may be opted out of being registered for a PCEHR if a person:
 - (i) shows that they have the authority to act on behalf of the individual – e.g. because they are their parent, guardian or have a power of attorney; and
 - (ii) pass the identity verification process.
- (d) Individuals who are registered for a PCEHR but cancel their registration before the end of the Opt-Out Period will not be included in the bulk registration. If the person later wishes to re-register for a PCEHR, they can do so in accordance with existing registration processes.
- (e) Individuals who gain a verified IHI after the bulk registration process at the end of the Opt-Out Period (e.g. newborns, immigrants, some visitors to Australia, etc.), will automatically be registered for a PCEHR as soon as their IHI is verified unless they choose to opt-out.
- (f) The System Operator will retain its discretion not to register an individual for a PCEHR if the System Operator is satisfied that registering the individual may compromise the security or integrity of the PCEHR system.¹²
- (g) Individuals (or their authorised representatives) will be able to cancel their PCEHR registration, or re-register for a PCEHR, at any time in accordance with existing processes (i.e. via the online, telephone, face-to-face and mail cancellation and registration channels).

¹² PCEHR Act, subsection 41(2).

3.5 Implementation of Opt-Out Model

The precise timing for the implementation of the Opt-Out Model is yet to be determined and is subject to a number of factors such as trials, government policy approval and the passage of legislation. However, for the purposes of our assessment, the following implementation timeframes are currently proposed.

Phase	Details
<i>Government Announcement</i>	A public awareness campaign will be implemented, directed at the public at large as well as special interest groups.
<i>Business As Usual</i>	<ul style="list-style-type: none"> • There will be no change to the existing opt-in registration and cancellation processes for a period after the announcement. • Individuals will be able to register for a PCEHR, and cancel their PCEHR registration, through the existing channels (online, telephone, face-to-face mail and assisted registration channels, and the online, telephone and face-to-face cancellation channels).
<i>Opt-Out Period</i> (approximately 4 months)	<ul style="list-style-type: none"> • Individuals will be able to indicate that they do not want to be registered for a PCEHR. This will primarily occur online. Telephone, face-to-face and mail channels will also be available. • Individuals will also be able to opt-out their dependants who are on the same Medicare card. • Communications which target individuals more directly will be implemented. • The System Operator will suspend accepting registration applications at the end of this period as part of the opt-out transition.
<i>Bulk Registration and Shell Record Creation</i> (approximately 1 month)	<ul style="list-style-type: none"> • Shell PCEHRs will be created for all Australians with an active IHI status and verified IHI record status, except individuals who opted out during the Opt-Out Period, already have a PCEHR, or had a PCEHR but cancelled it.
<i>Transition Period</i> (approximately 6 weeks)	<ul style="list-style-type: none"> • Individuals will have a period of approximately 6 weeks to access their PCEHR through myGov and set their privacy controls, if they do not wish to use the default access controls. • The default access controls will allow any healthcare provider organisations providing healthcare to the individual to access the individual's PCEHR. Healthcare providers will not be able to access an individual's record during the Transition Period. • During the Transition Period, individuals will be able to 'opt-out' of having Medicare data included in their PCEHR. • Healthcare providers will not be able to upload historical records – that is, records created before the end of the Transition Period. This is to ensure that individuals are able to set access controls in relation to their PCEHR before documents start to be uploaded by the individual's healthcare providers.
<i>Provider Access</i>	From the end of the Transition Period, healthcare providers will be able access PCEHRs, and healthcare providers and repository operators (such as Medicare) will be able to upload records created (subject to any privacy controls set by the individual).

Phase	Details
Registration of Newly Verified IHI	<p>From the end of the Transition Period, when a new IHI is verified the individual will automatically be registered for a PCEHR unless they have opted out. This will occur in three situations:</p> <ul style="list-style-type: none"> anyone registering for Medicare for the first time, the majority of whom will be either: <ul style="list-style-type: none"> newborns: the parents (or guardians) of newborns will have the option, via the relevant form (Newborn Child Declaration), to choose on behalf of the newborn to opt-out of PCEHR registration. If the parents (or guardians) do not opt out, the newborn will be automatically registered for a PCEHR; or immigrants: where a foreign national is issued with an Australian visa or passport that entitles the person to be registered for a IHI, the individual (or their parents or guardians if the individual is a dependant) will have the option of opting-out of PCEHR registration. If the individual (or their parents/guardians) does not opt out, the individual will be automatically registered for a PCEHR; people who are not eligible for Medicare but who nonetheless apply for an IHI; or people for whom DVA enables an IHI to be issued.

3.6 Information flows relating to Opt-Out Model

- (a) Detailed information flows relating to the Opt-Out Model are set out in:
 - (i) Schedule 1 – online opt-out process (Online Opt-Out Service);
 - (ii) Schedule 2 – automatic registration process; and
 - (iii) Schedule 3 – automatic registration of new Medicare enrolments (which include newborns and immigrants) and IHI registrants.
- (b) Detailed information flows for opting out via telephone, face to face or mail channels are not yet available. The Department expects that these processes will be the subject of further privacy analysis in future.

3.7 Community expectations

3.7.1 Addressing public concerns about privacy impacts

- (a) The ultimate privacy control for an individual is to not have a PCEHR at all. In an Opt-In Model, privacy is protected by default, because an individual is only registered for a PCEHR if the individual actively applies for registration.
- (b) However, the Opt-Out Model shifts the key privacy risk onto the individual. Unless the individual acts to stop it, an individual will be registered for a PCEHR. Unless they act to adjust their privacy control settings, all information in their PCEHR will become accessible by any authorised employee accessing the PCEHR on behalf of a registered healthcare provider organisation.

- (c) As discussed in section 3.3 above, there are a number of existing legislative and technical system measures to limit access to and the use of a PCEHR for legitimate reasons relating to the provision of healthcare (further detail is also provided in section 8.4.3 below).
- (d) Nonetheless, the shift from an Opt-In Model to an Opt-Out Model is a significant policy change. There is a risk that the move will be seen by some in the community as heavy-handed. The fact that the health information to be populated in the PCEHR (once the PCEHR has been accessed the first time) will include up to two years retrospective Medicare data (unless an individual proactively opts-out of having that information included) may further exacerbate for individuals a sense of loss of autonomy.
- (e) The stakeholders consulted on behalf of the Department in relation to this proposed change have raised similar concerns such as:

*Some stakeholders were concerned that this could be seen as a somewhat sinister move to force people into a system that would give Governments and others access to confidential health information which could then be used for unknown purposes.*¹³

- (f) The PCEHR has the potential to offer an overall privacy positive for individuals and other stakeholders in the long term, as it replaces other methods of sharing health information. As the Consumers Health Forum of Australia (CHF) stated:

*The privacy issues are really critical and important but should not be a reason not to have this kind of system in place, because there are a lot more concerns around the paper based system we have at the moment in terms of privacy breaches. When you have information sitting on fax machines and in paper records on people's desks, then there is not a secure information exchange that we could potentially have with this system if we get it right.*¹⁴

- (g) That said, respect for the privacy of health information is a value shared by many in the community. Many individuals will currently be operating on the assumption that their health information is only allowed to be shared between healthcare providers proactively, with their consent. There is a risk that any move to shift this paradigm will be of concern to some individuals.
- (h) The Australian Privacy Commissioner has measured community attitudes over time to a range of privacy issues, one of which is the sharing of health information between healthcare providers.
- (i) Research conducted for the Office of the Australian Privacy Commissioner across 2001,¹⁵ 2004,¹⁶ 2007,¹⁷ and 2013¹⁸ has found that:

¹³ Draft Deloitte report p.10.

¹⁴ Ms Carol Bennett, Chief Executive Officer, Consumers Health Forum of Australia, Committee Hansard, 6 February 2012, pp. 16, 22 (cited in the Senate Standing Committee's report at page 27, March 2012).

¹⁵ Roy Morgan Research, "[Community attitudes towards privacy in Australia 2001](#)", prepared for the Office of the Federal Privacy Commissioner – 1,524 respondents; see <http://www.oaic.gov.au/privacy/privacy-archive/privacy-reports-archive/2001-community-attitudes-towards-privacy-in-australia>.

¹⁶ Roy Morgan Research, "[Community Attitudes Towards Privacy 2004](#)", June 2004, prepared for the Office of the Federal Privacy Commissioner – 1,507 respondents; see <http://www.oaic.gov.au/privacy/privacy-archive/privacy-reports-archive/2004-community-attitudes-towards-privacy-in-australia>.

¹⁷ Wallis Consulting Group Research, "[Community attitudes towards privacy 2007](#)", prepared for the Office of the Federal Privacy Commissioner, – 1,503 respondents; see <http://www.oaic.gov.au/privacy/privacy-archive/privacy-reports-archive/community-attitudes-to-privacy-2007>.

- (i) The main reason Australians are reluctant to divulge their personal information is because they consider such requests an invasion of privacy – rather than from fear of their personal information being misused or causing personal threat.
- (ii) When asked in 2004 and 2001 about inclusion in a national health database, the description of which was similar to the PCEHR model, around two-thirds of people stated inclusion should be voluntary (64% in 2004, down from 66% in 2001), and only one-third believed all medical records should be entered as a matter of course (32% in 2004, up from 28% in 2001).
- (iii) Differences in sentiment about inclusion in a national health database could be seen according to gender and age, with men more likely than women to believe that all records should be entered as a matter of course (35% of men compared with 28% of women), and older people were more likely than younger people to feel all records should be entered as a matter of course (37% of people over 50, compared with 25% of 18-24 year olds).
- (iv) When asked in 2013 and 2007 about the circumstances in which 'it would be ok for your doctor to share your health information with other health professionals', 31% (up from 25% in 2007) said that consent should always be sought. Thirteen percent (down from 17% in 2007) accepted sharing 'in serious or life-threatening cases', and 31% (down from 35% in 2007) felt that it would be acceptable 'to treat the specific problem at hand'. Only 25% (similar to the number in 2007) said that they are 'happy for information to be shared between health providers for anything to do with their health'.
- (j) Other research similarly indicates that Australians' attitudes towards, and expectations of, privacy will differ according to gender, age and ethnicity. For example qualitative research has found that people from a non-English speaking background, and Indigenous Australians, have a general reluctance to share information about their health.¹⁹
- (k) These results suggest that:
 - (i) only around 25% of people surveyed would have described an Opt-Out Model, with the current default PCEHR privacy control settings, as acceptable in terms of their general views on the sharing of their health information between healthcare providers; and
 - (ii) those people who may have the most difficulty understanding communications about the shift to an Opt-Out Model, or about the implications of the default privacy control settings and how they can adjust them, may also be the individuals who hold the strongest privacy concerns about the sharing of their health information.
- (l) The government will therefore need to clearly articulate the policy problem it faces, and why it believes that shifting away from a consent-based, Opt-In Model to an Opt-Out Model is one part of the desired solution.²⁰ In particular, the public at large will need to be persuaded that while low take-up of PCEHRs to date *per se* is not the problem, there is a circular, chicken-and-egg problem that a low take-up by individuals means healthcare

¹⁸ Office of the Australian Information Commissioner, [Community attitudes to privacy survey, Research report 2013](http://www.oaic.gov.au/privacy/privacy-resources/privacy-reports/oaic-community-attitudes-to-privacy-survey-research-report-2013) – 1,000 respondents; see <http://www.oaic.gov.au/privacy/privacy-resources/privacy-reports/oaic-community-attitudes-to-privacy-survey-research-report-2013>.

¹⁹ Privacy Victoria, Privacy in Diverse Victoria: Research report into attitudes towards privacy in diverse communities, October 2002.

²⁰ See PCEHR Review Report, pages 6 and 28.

providers do not see the value in looking for, or adding to, an individual's PCEHR, and thus the health benefits are not realised for those individuals with a PCEHR, or for taxpayers as a whole.

- (m) The policy debate will also need to address concerns that the Opt-In Model was not given an adequate chance²¹ to achieve a critical mass of individual up-take, given:
 - (i) the nature of communications with individuals to date mostly targeted particular cohorts (such as parents of newborns, and people with chronic or complex conditions), rather than the population as a whole;²²
 - (ii) some functionalities, such as pathology, have only recently been enabled;²³ and
 - (iii) concerns about the usability of the registration process²⁴ have not yet been addressed.
- (n) Even those individuals who appreciate the rationale for the government to seek to shift the paradigm away from consent may be concerned that in the proposed Opt-Out Model, only individuals will face additional risks. Although the stakeholder consultations with members of the public on this topic have generally favoured the move to opt-out, we understand that individuals also strongly feel that the other side of the equation – clinician involvement – must equally be addressed.
- (o) The (draft) Deloitte *Report on the public consultation into the Review of the PCEHR* (**draft Deloitte report**) notes that:

*The view was put forward in every consumer consultation session that providers, at a minimum, should be subject to the same opt-out model that consumers will be to drive provider participation.*²⁵
- (p) The message will need to be carefully communicated, to avoid the perception that individuals are being asked to accept all the risk alone, without healthcare providers similarly being moved into an Opt-Out Model.
- (q) The government will also need to demonstrate to the public that the shift to an Opt-Out Model will achieve the government's policy objective²⁶ – because if opt-out does not deliver the critical mass needed to deliver value from the PCEHR system (in terms of health benefits to the individual, and improved overall health outcomes, which leads to health system cost saving benefits to the taxpayer), members of the public may perceive themselves as carrying all the risks (individuals with PCEHRs will carry the privacy risks, and taxpayers the financial risks), but without reaping the benefits.

²¹ NEHTA sub p.12: "In terms of digital-technology-enabled transformation, the PCEHR is in its early days of information content and usage. Final assessment is premature, given that complex electronic record systems, particularly those of scale, take many years to evolve and mature into solutions that are content-rich and which can be seamlessly integrated into healthcare workflows."

²² Draft Deloitte report p.9: "Most consumers felt that the current low consumer registration numbers were a result of lack of awareness of the PCEHR, difficulties in registering associated with the current registration processes or apathy on the part of consumers rather than an objection to having a PCEHR."

²³ NEHTA sub p.2: "Increasing participation by key cohorts will drive content creation which has been identified as a key enabler by clinical users, and is the critical next step to drive uptake of the PCEHR to reach a 'tipping point' of use. This involves completing the current workplan to include pathology and diagnostic imaging in the PCEHR, then expanding its use to include allied health professionals and specialists. Consumer registrations must also increase significantly to translate the work to date into beneficial clinical outcomes".

²⁴ See PCEHR Review Report p.55.

²⁵ Draft Deloitte report p.9.

²⁶ See PCEHR Review Report, page 28.

- (r) Various stakeholders have already indicated that their support for the switch to an Opt-Out Model is qualified, or conditional upon other steps also being taken to ensure that the system delivers value.

- (s) For example, the Consumers Health Forum, while supporting an opt-out approach, has warned that:

*An opt-out system for consumers will not deliver the same level of value if the system remains opt-in for health professionals. This can be observed through issues with the UK's Summary Care Record, where less than one percent of patients opted out but access of the records by general practitioners was very low.*²⁷

- (t) Other stakeholders' concerns have similarly led Deloitte to conclude:

*'Opt-out must be accompanied by improved content (and contribution from a broader range of clinicians)',*²⁸

*'It will be critical to address these issues of record utility prior to move to an opt-out model to remove the barriers to provider participation. If the system remains difficult to use when opt-out is introduced, providers will remain reluctant to use the record and consumers will not then realise the benefit of having a PCEHR',*²⁹

and

*'Moving to an opt-out model won't of itself deliver meaningful use. Meaningful use by consumers and providers will only occur when all participants in an individual's care are participating in using the PCEHR by putting content in and drawing content out.'*³⁰

- (u) There also appears to be a lack of clarity in individuals' thinking around what concepts like 'consent' really mean in an opt-out model. Debate on this proposal will therefore also need to address the sometimes conflicting views held by individuals about privacy in relation to their health records. For example the PCEHR Review Report noted:

*It is not uncommon to hear the comment from patients that they already thought their health information was available to all their care providers (and yet) Patients have an expectation that the PCEHR ... will not be shared without their consent.*³¹

- (v) The automatic registration for a PCEHR, and the use of default settings which will allow for the sharing of health information and the inclusion of up to two years of Medicare data, for an individual who has not opted-out cannot reliably be described as having been based on that individual's 'consent'.
- (w) Although the Department understands this (and therefore the legislation will be amended to allow for legislative authority rather than a consent basis to be the legal underpinning for PCEHRs in the future), it would appear that other stakeholders do not.
- (x) For example, the Consumers Health Forum submission supports the move to opt-out, but also states that:

²⁷ CHF sub p.5.

²⁸ Draft Deloitte report p.7.

²⁹ Draft Deloitte report p.14.

³⁰ Draft Deloitte report p.22.

³¹ PCEHR Review Report p.65.

*Consent is at the heart of consumer's understanding of personal control. Consumers have expressed the importance of being able to choose who can access to their record and the particular records that will be contained in it – CHF sees that this is even more important in an opt-out model. If this model is to be considered, discussions need to be held regarding how informed consent can be gained in a way that is realistic, appropriate and places this authority in the hands of consumers.*³²

- (y) The government's explanation of the proposal will need to anticipate these nuances, and ensure that unrealistic expectations or inaccurate beliefs about 'consent' do not lead individuals to a false understanding about what the default privacy control settings will allow in practice.
- (z) Ultimately, these risks can only be managed through the processes involved in the development and passage of the legislation and communication activities. Consultation and transparency will be key to ensuring an informed debate.

3.7.2 Preserving individuals' right to privacy

- (a) There is also likely to be a strong community expectation that a PCEHR continue to offer a range of privacy control settings for the individual to manage. The Australian Medical Association expressed the following view in its submission to the Senate Standing Committee:

*The integrity of the confidentiality of the patient medical record is absolutely essential to developing, enhancing, and underpinning the therapeutic relationship between medical practitioners and their patients. This confidentiality secures the necessary trust and openness that characterises the ongoing communication between doctors and their patients to optimise patient care. Confidentiality is regarded as one of the most important aspects of good medical practice.*³³

- (b) The draft Deloitte report also found:

While consumers are happy to know that personal security and access controls exist for the PCEHR and the content within their record, the majority of consumers consulted are unlikely to use the controls to block access to their record or to particular documents in their record except in very special circumstances (such as ultrasound scan of a dead foetus prior to termination). Providers were concerned about whether the move to an opt-out model would remove the implied consent that exists today and would result in them having to ask for explicit consent to upload content during each instance of treatment.

³² CHF sub p.8.

³³ Submission of the Australian Medical Association to the Senate Standing Committee Inquiry into the PCEHR Bill 2011 and one related Bill, 13 January 2012, page 5.

Recommendation 1

That, in order to ensure transparency and assist public debate about the privacy risks and benefits of implementing the Opt-Out Model, the Department publish:

- (a) the Deloitte *Report on the public consultation into the Review of the PCEHR* (once finalised);
- (b) this PIA report; and
- (c) an exposure draft Bill.

Recommendation 2

That prior to introducing the legislation, the Department conduct further consultation on this proposal with groups representing those most likely to be concerned about the privacy of their health information and other personal information, including both individuals and practitioners in the family violence, mental health and sexual health fields.

Chapter 4 Communicating the opt-out choice

4.1 Communications strategy

4.1.1 Communications for the Opt-In Model

- (a) The PCEHR system was introduced in July 2012 as an 'opt-in' eHealth system.
- (b) The public information communication campaign for the opt-in PCEHR system comprised:
 - (i) *Concept of Operations: Relating to the introduction of a personally controlled electronic health record system (Con Ops)*,³⁴ which was a NEHTA document first published in April 2011 and subsequently revised;
 - (ii) public consultation in relation to the *Legislation Issues Paper* (July 2011), the *Exposure Draft Legislation* (September 2011) and the *Proposals for Regulations and Rules* (March 2012);
 - (iii) the eHealth³⁵ and NEHTA websites³⁶;
 - (iv) hardcopy handouts and brochures, such as the *Connecting your healthcare: a guide to registering for an eHealth record (Health Registration Booklet (Registration Booklet))*,³⁷ which are available in DHS-Medicare shopfronts and were included in some DHS-Medicare-related mail-outs;
 - (v) communications through peak medical bodies and individual groups; and
 - (vi) initiatives conducted by Medicare Locals, which were at the discretion of each Medicare Local, and have typically targeted niche segments of the population.
- (c) The opt-in communications materials highlighted the benefits to an individual in obtaining a PCEHR³⁸ and provided a comprehensive introduction to the PCEHR system.³⁹
- (d) However, although registration in the PCEHR system has continued to increase, there is evidence that most individuals are unaware, or have very little awareness, of the PCEHR system. The draft Deloitte *Report on the Public Consultation into the Review of the PCEHR*, for example, states that:

*Many consumers consulted were unaware of the existence of the PCEHR or did not have a clear understanding of its purpose and potential benefits before the consultation. Consumers felt that there had been no consistent, widespread awareness raising and education of consumers in relation to the PCEHR. What communications there have been were patchy and inconsistent.*⁴⁰

³⁴ [Concept of Operations: Relating to the introduction of a Personally Controlled Electronic Health Record System](http://ehealth.gov.au/internet/ehealth/publishing.nsf/content/PCEHRS-Intro-toc) available at <http://ehealth.gov.au/internet/ehealth/publishing.nsf/content/PCEHRS-Intro-toc>.

³⁵ [eHealth website](http://www.ehealth.gov.au/) available at <http://www.ehealth.gov.au/>.

³⁶ [NEHTA website](http://www.nehta.gov.au/) available at <http://www.nehta.gov.au/>.

³⁷ [‘Applying in other ways’](http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/applicationmethods) available at <http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/applicationmethods>.

³⁸ For example, the Consumer Registration Booklet states (page 2): "Having an eHealth record means you, and any doctors or other healthcare professionals involved in your care can, subject to your access controls, quickly access a summary of your important health information, helping them to make better, safer decisions about your care."

³⁹ For example, the Consumer Registration Booklet provides an overview of the entities which make up the PCEHR System and how it works.

⁴⁰ Draft Deloitte report, p.7.

4.1.2 Proposed communications for the Opt-Out Model

- (a) The Department intends to implement a significant public awareness campaign to notify individuals of the change from an Opt-In Model to an Opt-Out Model.
- (b) We are instructed that the Department is still in the process of planning the communications campaign and no formal decisions have yet been made, however it is anticipated that a national campaign will be implemented which includes the following types of activities:
 - (i) written materials, such as bulk mail-outs to Australian households;
 - (ii) letters and emails to the current registered individuals to make them aware of the change to an Opt-Out Model;
 - (iii) the provision of information about the PCEHR system via television advertising, radio, print media and social media;
 - (iv) informative articles to healthcare providers and individual publications;
 - (v) updating the eHealth website; and
 - (vi) other communications through peak bodies, such as NEHTA and the Privacy Commissioner.
- (c) The Department also intends to have certain targeted communications, such as to disadvantaged groups, or groups which do not typically engage in mainstream media.
- (d) At this stage, the Department proposes to deliver the communications campaign in two stages:
 - (i) **Stage 1:** Immediately upon the announcement of a government decision to implement an Opt-Out Model, communications which focus on providing information to the public at large will be rolled out, such as print media and television, as well as communications targeting special interest groups; and
 - (ii) **Stage 2:** When the Online Opt-Out Service goes live, communications which target individuals more directly will be implemented, such as mail-drops or mail-outs.

4.2 Privacy risk - collection transparency

4.2.1 APP 5 collection notice obligations

- (a) As noted in Chapter 3, moving the PCEHR system from an Opt-In to an Opt-Out Model is a significant policy shift. It will involve a process by which personal information, including the 'sensitive' category of health information, will begin to be collected and used by Australian Government agencies for the first time, as well as made available to many potential healthcare providers for the first time, for millions of people.
- (b) A key privacy right under Australian privacy law is for individuals to be made aware of what personal information is going to be collected about them, for what purposes. This is usually done by way of what is typically known as a 'privacy notice'.
- (c) The subject of a privacy notice should include what personal information will be collected (either from the individual themselves, or from other sources), if it is required or authorised by law, the purposes for which the information will be used, who else it may be disclosed to (including any overseas recipients), the consequences for the individual if their information is not collected, the individual's rights of access and correction, and how they may make a privacy complaint.

- (d) APP 5 states that an agency 'must take such steps (if any) as are reasonable in the circumstances' to notify the individual, or to 'otherwise ensure that the individual is aware' of certain matters, 'at or before the time or, if that is not practicable, as soon as practicable after' their personal information is being collected.

- (e) The APP Guidelines provide the following guidance in relation to APP 5:

The reasonable steps for an APP entity will depend on circumstances that include:

- *the sensitivity of the personal information collected. More rigorous steps may be required when collecting 'sensitive information' ... or information of a sensitive nature*
- *the possible adverse consequences for an individual as a result of the collection. More rigorous steps may be required as the risk of adversity increases*
- *any special needs of the individual. More rigorous steps may be required if personal information is collected from an individual from a non-English speaking background who may not readily understand the APP 5 matters*
- *the practicability, including time and cost involved. However, an entity is not excused from taking particular steps by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.⁴¹*

- (f) We also note that to the extent that the collection is authorised by law (e.g. the PCEHR Act or HI Act), that fact and the name of the law should be notified to the individual (APP 5.2(g)).
- (g) In an Opt-In Model, the individual is proactively involved in the PCEHR registration, and therefore there is a clear opportunity to notify the individual about what is going to happen to their information, and what choices they have about that.
- (h) However in an Opt-Out Model, the greatest challenge will be delivering an appropriate privacy notice to the millions of affected individuals, so that they have sufficient opportunity to understand the change that is about to occur, and what choices they have in terms of the choice to opt-out, or the choice to adjust their privacy control settings (and how to set those privacy control settings).
- (i) This communication challenge is not only in relation to ensuring compliance with APP 5, but also to meet community expectations. The PCEHR system, and the government's ability to manage it, could face significant reputational damage if large numbers of individuals could successfully argue that they were never notified, and therefore were not given the chance to opt-out or adjust their privacy control settings before their health information was disclosed without their knowledge or consent.
- (j) Effective communication also assists individuals to make informed choices about their privacy (i.e. whether to opt-out, and what privacy control settings to use), and can increase public confidence.

⁴¹ Office of the Australian Information Commissioner, [Australian Privacy Principles guidelines](http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/), paragraph 5.4, at <http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/>, accessed 24 April 2015.

4.2.2 Direct and targeted communications

- (a) A risk scenario that arises with implementing an Opt-Out Model is large numbers of individuals asserting that they were unaware of the change and its implications. For example, *'I was never told the government was going to start sharing all my health information; if I had known I never would have agreed to that, and now X person knows I have Y illness'*.
- (b) Privacy 'heat' may also be generated where people are taken by surprise about how their personal information is being handled. This can take the form of formal privacy complaints, stories in the media or complaints from constituents to local MPs. Indeed, a statistical analysis of privacy complaints from NSW suggests that the disclosure of health information is the single most likely scenario to generate a privacy complaint, compared with other categories of personal information and other privacy principles.⁴²
- (c) Health information is a category of 'sensitive information' recognised by the Privacy Act as worthy of additional protection. The APP Guidelines (as extracted above) suggest that the steps that will be considered 'reasonable' in the context of a proposal to begin disclosing individuals' health information in a way which they would not otherwise expect, and which could lead to adverse consequences for the unaware individual, will need to be rigorous and comprehensive.
- (d) As outlined above, the Department has proposed a communications strategy to tell individuals about the change to an Opt-Out Model, and to let them know how they can opt-out or otherwise act on their preferences by adjusting their privacy control settings. Whether or not the communications strategy will include contacting all adult Medicare card holders by name, or other techniques such as a 'To The Householder' mail-out, is yet to be determined. We appreciate that the chosen strategy will have significant cost implications.
- (e) Although a 'To The Householder' mail-out is less costly than mailing individual letters to every adult Medicare account holder, experience from the UK suggests that a broad-brush approach will fail to reach the majority of individuals. Glossy brochures which look like junk mail are too easily discarded by the individual without reading them.⁴³
- (f) We suggest that a shift to an Opt-Out Model can only be achieved without significant community disquiet if serious effort is made to contact, by name, the 22 million people who will be affected.
- (g) Even with named letters, there will be many individuals for whom a letter will not be enough. There will be people for whom Medicare does not have a current or reliable home address, including travellers, homeless people and many Indigenous people. There will be others who may receive the letter, but struggle to read or understand it, including

⁴² See the NSW Privacy Commissioner's report as part of the [NSW Information & Privacy Commission 2013-14 Annual Report](http://www.ipc.nsw.gov.au/annual-reports), at <http://www.ipc.nsw.gov.au/annual-reports>, accessed on 10 December 2014, and the 2002-03 Annual Report of Privacy NSW, not available online. Statistics from the Australian Privacy Commissioner do not provide enough detail to draw these types of conclusions, although complaints about the combined Use & Disclosure principle represented 43% of all complaints in 2013-14; see the [2013-14 Annual Report](http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201314/chapter-seven-privacy-compliance#s3) at <http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201314/chapter-seven-privacy-compliance#s3>, accessed 10 December 2014.

⁴³ A 'To The Householder' mail-out about the care.data NHS initiative to place GPs' patient information into a national database was criticised for failing to reach health consumers. [One survey found that 67% of respondents did not remember receiving the leaflet](http://www.theguardian.com/healthcare-network/2014/mar/11/caredata-nhs-trust-doctor-patient-leaflet). See <http://www.theguardian.com/healthcare-network/2014/mar/11/caredata-nhs-trust-doctor-patient-leaflet>, accessed 10 December 2014.

people from a non-English speaking background, people who are illiterate, and adults who have limited capacity.

- (h) These people already represent some of the most disadvantaged and marginalised individuals in our community. It has been recognised that these are the groups of people who struggle now to register for a PCEHR, and therefore automated registration will help these individuals reap the benefits of having a PCEHR. However, these individuals may also face significant privacy risks arising from the sharing of their personal information, often compounded by their social disadvantage or isolation. Every effort must be made to notify these individuals about the change that is about to occur, and what they can do to manage their particular privacy concerns.
- (i) We have therefore made recommendations about how to best reach the millions of individuals to be affected by the proposal, to ensure that the Department can satisfy the requirement to take 'reasonable steps' to notify people about how their personal information will be handled.
- (j) Also relevant are **Recommendations 10 and 11** (information and collection notice on the eHealth website and Online Opt-Out Service), which also seek to promote informed decision-making by the individual before they decide whether or not to opt-out.

Recommendation 3

That a letter, addressed to the named individual, is sent to every Medicare card holder, about the change to an Opt-Out Model. The letter should explain:

- that unless they opt out by X date, they will be registered for a PCEHR (i.e. a PCEHR will be created for them);
- what the default privacy control settings allow;
- how they can opt out or adjust their privacy control settings if they wish;
- who to contact if they have an enquiry; and
- who to contact, including the Privacy Commissioner, if they have a privacy complaint.

Recommendation 4

That the Department investigate how other forms of direct communications could also be utilised, without leading to additional collections of personal information, for example by sending an email to the 6 million existing myGov account holders.⁴⁴

Recommendation 5

That the Department ensure its communication strategy includes measures to reach vulnerable and disadvantaged individuals who may not receive or understand a letter, such as individuals from a non-English speaking background, Indigenous people, the illiterate, homeless, and adults with limited or no capacity.

⁴⁴ We understand from the Department that as of 31 March 2015, there were 6,552,671 active myGov accounts, of which 4,292,423 have at least one linked service. This means that over 4 million people have undergone some kind of identification process in order to link their myGov account with services operated by the ATO, Medicare, PCEHR, etc online. Of these, there are 758,109 PCEHRs linked to a myGov account.

Recommendation 6

That the Department ensure its communication strategy includes measures to reach other people who may not receive a named letter, such as leaflets at Australian Immigration counters or other government shopfronts during the Opt-Out and Transition Periods, to target returning travellers and other individuals.

Recommendation 7

That the system design include, for any individuals who were automatically registered (and who have not already taken action to set their own privacy controls), a communication direct to the individual, which is triggered the first time their PCEHR is accessed by a healthcare provider.⁴⁵ The communication should explain that their PCEHR is now 'live', what the default privacy settings allow, how they can adjust their privacy control settings if they wish, who to contact if they have an enquiry, and who to contact (including the Privacy Commissioner), if they have a privacy complaint. The communication could be sent by email or SMS if the individual has previously provided such details (see also **Recommendation 30**), or otherwise by mail to the Medicare-provided address.

Recommendation 8

That the Department consider whether it is technically feasible and appropriate for the PCEHR system to be designed to allow medical software providers' systems to generate a pop-up message the first time an individual's PCEHR is viewed⁴⁶ by a healthcare provider, which the healthcare provider could then print out for the individual who is present with them.

4.2.3 Other public communications

- (a) The current proposed communications strategy contemplates making information about the opt-out change and process via the ehealth.gov.au website, among other mechanisms.
- (b) The current PCEHR Privacy Policy broadly addresses the handling of personal information by the System Operator and HI Service Operator. However, the distinction between the different capacities in which DHS acts in the PCEHR context is not clear. For example:
 - (i) the policy suggests that the only time DHS acts as delegate of the System Operator is via the use of DHS customer service officers. In the opt-out world, DHS' involvement as delegate of the System Operator seems likely to increase significantly, particularly if the Online Opt-Out Service is hosted by DHS, accessible via a DHS website and information is stored on DHS systems.
 - (ii) The Chief Executive Medicare's role as the HI Service Operator is mentioned twice in the PCEHR Privacy Policy, but only briefly.

⁴⁵ The conditions for triggering this communication should be the same as the conditions which will trigger the 'flow' of Medicare-provided data to begin – i.e. either a healthcare provider views the PCEHR, or a system uploads a clinical document to it, such as a hospital discharge summary.

⁴⁶ We do not suggest that this mechanism should be triggered when a clinical system generates an upload to a consumer's PCEHR without a healthcare provider also viewing the record, as in the case of an automated upload of a hospital discharge summary, because the consumer would not be present at the time.

- (c) The privacy risk is that individuals will not understand what entities are handling their personal information, and who to approach if they want to seek access or correction of a record or make a privacy complaint.

Recommendation 9

The PCEHR Privacy Statement on the eHealth website should be reviewed and updated to ensure that it addresses the relevant entities that will be handling personal information and in what capacity (i.e. System Operator, HI Service Operator and NIO), and the purposes for which information will be collected, used and disclosed by those entities.

Recommendation 10

That the Online Opt-Out Service include a clear summary about how the opt-out process works and the implications of opting out (or not opting out), as well as information about the ability to set privacy controls.

Recommendation 11

That the Department develop an appropriate collection notice to include in the Online Opt-Out Service which explains how a person's personal information will be handled (collected, used and disclosed) by and between various entities (i.e. the System Operator, HI Service Operator, NIO, Medicare and Document Verification Service (DVS)) during the opt-out process and automatic registration process. The collection notice should also address the use and disclosure of existing information held by the System Operator, the HI Service Operator and Medicare for the purpose of implementing an individual's decision to opt-out or cancel a PCEHR (including identity verification processes), and to automatically register relevant individuals for a PCEHR.

Chapter 5 Opt-out process

5.1 Opt-out channels

5.1.1 Overview of opt-out channels

- (a) During the Opt-Out Period, an individual will be able to choose not to be registered for a PCEHR via various channels, which are expected to be:
 - (i) online via the Online Opt-Out Service (**online channel**);
 - (ii) over the telephone with the System Operator (DHS) – i.e. via a DHS Customer Service Operator (**telephone channel**);
 - (iii) in person via the System Operator (DHS) – i.e. at a DHS service centre offering Medicare services (**face to face channel**); and
 - (iv) by post using a hard copy form (**mail channel**).
- (b) An individual (e.g. parent or guardian) who is at least 14 years old will also be able to opt-out his or her dependants where:
 - (i) the dependant is listed on the individual's Medicare card;
 - (ii) the dependant is under 18 years of age; and
 - (iii) the individual is at least 14 years older than the dependant.⁴⁷
- (c) An individual will be able to opt-out a dependant without having to opt-out themselves.

5.1.2 Limits to choice of channel

Authorised representatives

- (a) Where an individual (the **first individual**) wishes to opt-out another individual (the **second individual**) who is:
 - (i) under 18 years of age and is not listed on the first individual's Medicare card; or
 - (ii) over 18 years of age and lacks capacity to make decisions for themselves,the first individual will be unable to opt-out the second individual via the online or telephone channels. Instead, the first individual will have to use the face to face or mail channels. This requirement is due to the existing verification procedures needed to establish the first individual as an authorised representative and, if necessary, the second individual's capacity.
- (b) Parents and guardians will be able to opt-out their dependant(s), but will need to prove their identity and have the same Medicare card number as their dependant(s).

Persons who are unable to provide a primary identity document

- (c) The requirements for verification of identity are discussed below. If an individual does not have a primary identity document that can be verified via the Document Verification Service (**DVS**), or the name on the primary identity document does not match the name on their Medicare card, the individual will need to use the face to face or mail channels to

⁴⁷ Arrangements will also be in place to enable an individual (e.g. parent or guardian) to opt-out dependants where the individual is less than 14 years old or less than 14 years older than the dependant.

opt-out. The Department is investigating the possibility of making a telephone channel available for this purpose.

5.2 Overview of the Online Opt-Out Service

- (a) The Online Opt-Out Service is proposed to be available for a four month period to allow individuals to exercise their choice to opt-out of PCEHR registration in relation to themselves and/or their dependants (or, if the individual or a dependant has an existing PCEHR, to cancel their PCEHR registration).
- (b) The Online Opt-Out Service will be hosted by the System Operator (DHS). As at April 2015, a decision is yet to be made as to how the Online Opt-Out Service will be accessed (e.g. access via the eHealth website, which is hosted by the Department).
- (c) We have assumed that personal information submitted through the Online Opt-Out Service will be stored by the System Operator (DHS).
- (d) The information flows relating to the online opt-out process are set out in detail in Schedule 1.

5.3 Identity verification

5.3.1 Overview of identity verification process

- (a) The proposed method of verifying an individual's identity for opt-out purposes is by way of an 'enhanced bronze level assurance' check. The Department has assessed the proof of identity (**POI**) requirements in accordance with the benchmarks set out in the Australian Government's *National Identity Proofing Guidelines 2014*,⁴⁸ and considers this to be adequate having regard to the fact that no health information will be disclosed during the opt-out process.
- (b) An individual will access the Online Opt-Out Service and enter their first name, last name, date of birth, sex, Medicare/DVA card number, and the document number of an accepted Australian evidence of identity (**EOI**) document: either a driver licence, passport or Immicard number. This information is collected by the System Operator (DHS).
- (c) There will be two forms of verification:
 - (i) a check to confirm with the HI Service Operator that the individual's details match the information recorded in the HI Service System, and that the individual has an active IHI status and verified IHI record status (**IHI Lookup**); and
 - (ii) a DVS check to verify the authenticity of the identity document details provided by the individual (i.e. driver licence, passport or Immicard). The DVS is operated by the Attorney-General's Department.

5.3.2 IHI Lookup

- (a) The IHI Lookup involves the following information flows:
 - (i) the disclosure of personal information (i.e. the individual's first name, last name, sex, date of birth and Medicare/DVA card number) by the System Operator (DHS) to the HI Service Operator;

⁴⁸ [National Identity Proofing Guidelines](http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/NationalIdentityProofingGuidelines.pdf) available at <http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/NationalIdentityProofingGuidelines.pdf>

- (ii) the collection and use of that information by the HI Service Operator, as well as the use of existing personal information held by the HI Service Operator in the HI Service System, to locate the individual's IHI; and
- (iii) the disclosure of the individual's IHI, IHI record status (e.g. 'verified'), and IHI status (e.g. 'deceased') by the HI Service Operator to (and collection of that personal information by) the System Operator (DHS).

System Operator (DHS)

- (b) As outlined above, the individual will submit their first name, last name, sex, date of birth and Medicare/DVA card number through the Online Opt-Out Service. The purpose for which this personal information is collected is so that the System Operator (DHS) can implement the individual's decision to opt-out, which includes verifying the individual's identity and IHI.
- (c) The Department advises that the personal information disclosed to the HI Service Operator in this verification process is the minimum amount of data required by the HI Service Operator to identify the individual's IHI. On that basis, we consider that in relation to the System Operator (DHS):
 - (i) the collection of personal information from the individual, and the individual's IHI, IHI record status and IHI status (or if there is not an exact match, an error message) from the HI Service Operator, is reasonably necessary to implement the individual's opt-out decision, and therefore will comply with APP 3.1;
 - (ii) the disclosure of personal information to the HI Service Operator is for the primary purpose of collection (noting that the individual's IHI is required to implement the opt-out decision), and therefore will be in accordance with APP 6.1; and
 - (iii) the collection of an individual's IHI, IHI record status and IHI status from the HI Service Operator will be permitted under APP 3.6(b) as it would not be reasonably practicable to collect that information directly from the individual, having regard to the online environment in which the opt-out process occurs and fact that individuals who do not already have a PCEHR are unlikely to know their IHI.

HI Service Operator

- (d) We consider that the collection by the HI Service Operator of the individual's personal information from the System Operator (DHS):
 - (i) will be authorised under APP 3.1, on the basis that the personal information is the minimum data that is reasonably necessary for the HI Service Operator to locate the individual's IHI; and
 - (ii) will be permitted under APP 3.6(b) as it would be unreasonable or impracticable in the circumstances for the HI Service Operator to deal directly with the individual, having regard to the real-time online environment of the Online Opt-Out Service (which the individual has chosen to use).

5.3.3 Privacy risk – use and disclosure of personal information

Use of personal information

- (a) The process of looking up an individual's IHI involves the use of the following information by the HI Service Operator:

- (i) the personal information received from the System Operator (DHS) – this will be in accordance with APP 6.1 on the basis that the information will be used for the primary purpose of collection (i.e. to implement the individual's opt-out decision); and
 - (ii) existing information (including an individual's IHI, IHI record status and IHI status) held by the HI Service Operator in its database.
- (b) The Department has advised that the primary purpose of the HI Service Operator previously collecting the information held in its database is to ensure that entities provide, and individuals who receive, healthcare are correctly matched to health information that is created when healthcare is provided. There are several aspects to this, including the allocation of healthcare identifiers and identity verification.
- (c) Although the opt-out process involves identity verification, it is not in the context of ensuring that healthcare information is correctly matched to individuals and healthcare providers. In our view, there is a risk that identity verification in the context of opt-out (i.e. where an individual has specifically signalled that they do not want to have their health information matched in the PCEHR system) would be considered a secondary purpose.
- (d) Consequently, the use of the information for identity verification in the opt-out process may be for a secondary purpose and, in the absence of the individual's specific consent, raises a privacy risk in relation to APP 6 compliance by the HI Service Operator.
- (e) We have assumed that the information that will be used by the HI Service Operator in this step is 'identifying information' of an individual, as defined in section 7 of the HI Act. The HI Act authorises the HI Service Operator to use:
 - (i) identifying information for any purpose for which the System Operator is authorised to collect, use or disclose identifying information under Division 2A (section 11A of the HI Act); and
 - (ii) a healthcare identifier for a purpose for which the System Operator is authorised to collect, use or disclose the healthcare identifier under Division 2A (section 19A of the HI Act).
- (f) Currently, pursuant to section 22A of the HI Act (which is in Division 2A), the System Operator is only authorised to collect, use and disclose identifying information and a healthcare identifier of an individual for the purpose of verifying identity where an individual 'is applying, or has applied' for registration or is registered. A person opting out of PCEHR registration will obviously not be applying for registration. Consequently, section 22A of the HI Act would need to be amended to broaden its scope to enable the APP 6.2(b) 'authorised by law' exception to be relied upon by the HI Service Operator. We understand that such an amendment is being proposed by the Department.⁴⁹

Recommendation 12

That the drafting instructions for the proposed amendments to the HI Act ensure that section 22A of the HI Act is amended so that the scope of the provision allows the HI Service Operator to use identifying information and healthcare identifiers of individuals for the purpose of implementing an individual's choice to opt-out.

⁴⁹ Department of Health, 'Initial drafting instructions for amendments to the PCEHR and HI Act – 28 November 2014'.

Disclosure of personal information

- (g) The HI Service Operator will disclose to the System Operator (DHS) the individual's IHI, IHI record status and IHI status (or an error message, indicating that an exact matching IHI record for the individual cannot be found). As indicated above, there is a risk that disclosure of the information to the System Operator (DHS) for identity verification in the context of opt-out may be considered to be a secondary purpose.
- (h) To allow the HI Service Operator to disclose the individual's IHI and other information, one option is to obtain the individual's consent at the time they indicate their choice to opt-out (i.e. by checking a box in the Online Opt-Out Service). However, this may cause unnecessary concerns amongst individuals in relation to the handling of their information, and discourage them from exercising their right to opt-out. Also, we understand that the intention is to support the implementation of the Opt-Out Model with legislative authority (being a shift from the current consent-based approach).
- (i) The HI Service Operator is authorised to disclose a healthcare identifier to the System Operator for a purpose for which the System Operator is authorised to collect, use or disclose the healthcare identifier under Division 2A of the HI Act (section 19A of the HI Act). The HI Service Operator is also authorised to disclose 'identifying information' for any purpose for which the System Operator is authorised to collect, use or disclose identifying information under Division 2A (section 11A of the HI Act).
- (j) For the reasons discussed in paragraph 5.3.3(f), section 22A of the HI Act would need to be amended to broaden its scope to allow the HI Service Operator to disclose an individual's IHI and identifying information to the System Operator (DHS). We refer to **Recommendation 12**.
- (k) In addition, it is not clear that IHI record status and IHI status would be covered by the definition of 'identifying information'. As at the date of writing, no amendment to section 7 of the HI Act appears to be proposed.

Recommendation 13

Subject to consideration of any secondary implications of changing the definition of 'identifying information' in section 7 of the HI Act, that the drafting instructions for the proposed HI Act amendments ensure that the definition of 'identifying information' is amended to include IHI record status and IHI status.

Recommendation 14

That the drafting instructions for the proposed HI Act amendments ensure that section 22A of the HI Act is amended so that the scope of the provision allows the HI Service Operator to disclose identifying information and healthcare identifiers of individuals for the purpose of implementing an individual's choice to opt-out.

Collection notice

- (l) To ensure compliance with the APP 5 obligations of the System Operator (DHS) and the HI Service Operator, information about the collection, use and disclosure of personal information by those entities should be covered by the scope of the Online Opt-Out Service collection notice. We refer to **Recommendation 11**.

5.3.4 DVS check

- (a) The DVS check involves the following information flows:
 - (i) the disclosure of personal information (i.e. the individual's first name, last name, date of birth, sex⁵⁰, and driver licence, Immicard or passport number) by the System Operator (DHS) to DVS; and
 - (ii) the collection of personal information about the individual by the System Operator (DHS) from DVS, namely a 'yes' or 'no' response indicating whether DVS has a record of a 'real' document relating to the individual.
- (b) The handling of personal information by DVS is out of scope for the purposes of this PIA.
- (c) The individual is advised by the Online Opt-Out Service if the IHI and/or DVS check failed (i.e. by an error message). A system design decision is yet to be made as to whether an individual will be given a certain number of opportunities to re-enter their details. For security reasons (APP 11), we recommend that there be a limit to the number of times that a user of the Online Opt-Out Service may attempt to verify their identity through the online channel.

Recommendation 15

That the Online Opt-Out Service design limit the number of times that a user of the Online Opt-Out Service may attempt to verify their identity.

- (d) The Department advises that the personal information that is sent by the System Operator (DHS) to DVS is the minimum amount of data required by DVS to authenticate a person's EOI credential document. On that basis, we consider that:
 - (i) the collection by the System Operator (DHS) of the individual's personal information, and the 'yes' or 'no' response from the DVS (indicating whether or not the EOI document is genuine), is reasonably necessary to implement the individual's opt-out decision, and therefore will comply with APP 3.1;
 - (ii) the disclosure of personal information to the DVS is for the primary purpose of collection (noting that it is necessary to verify a person's identity before implementing the opt-out decision), and therefore will be in accordance with APP 6.1; and
 - (iii) the collection of a 'yes' or 'no' response from the DVS will be permitted under APP 3.6(b) as it would not be reasonably practicable to collect that information directly from the individual, having regard to the necessity of independent authentication of identity documents to reduce the risk of fraud.
- (e) To satisfy the APP 5 obligations of the System Operator, the scope of the Online Opt-Out Service collection notice should cover the DVS check process. We refer to **Recommendation 11**.

⁵⁰ Sex will only be provided to DVS if the consumer is relying on a passport as their primary identity document. The DVS may use gender rather than sex in relation to passport verification. If so, arrangements will be in place for individuals whose sex does not match their gender (e.g. to use different identification or a different channel to opt-out).

5.4 Identifying dependants and existing PCEHRs

5.4.1 Identification process

- (a) An individual will be able to opt-out eligible dependants listed on their Medicare card. If the individual or any of the relevant dependants has an existing PCEHR, the individual will be able to cancel the PCEHR through the opt-out process (i.e. rather than having to go through a separate cancellation process). We consider that this is a privacy positive aspect of the Online Opt-Out Service channel, as it simplifies the individual's ability to exercise their choice not to have a PCEHR (i.e. rather than having to go through the separate existing cancellation process, which is a more involved process).
- (b) The steps relating to the identification of dependants and existing PCEHRs involve the following information flows:
 - (i) The individual discloses to the System Operator (DHS) the first and last names of any dependants they would like to opt-out.
 - (ii) The System Operator (DHS) discloses to Medicare the individual's first name, last name, sex, date of birth and Medicare/DVA card number (being the personal information collected from the individual when they accessed the Online Opt-Out Service) and the first and last names of the dependants.
 - (iii) Medicare collects and uses the personal information of the individual and dependants, and also uses existing personal information about the individual and dependants held in the Medicare system, to identify the relevant dependants (i.e. dependants listed on the individual's Medicare card).
 - (iv) Medicare discloses to the System Operator (DHS) the first name, last name, sex, date of birth and Medicare/DVA card number for each relevant dependant (under 18 years of age) which the individual is able to opt-out (according to the business rules) and matches the names provided by the individual.
 - (v) The System Operator (DHS) discloses to the HI Service Operator the first name, last name, sex, date of birth and Medicare/DVA card number of each of the relevant dependants. The HI Service Operator collects and uses that information, as well as existing information held by the HI Service Operator in the HI Service System, to locate each dependant's IHI. The HI Service Operator then discloses to the System Operator (DHS) (and the System Operator (DHS) collects) each relevant dependant's IHI number, IHI record status and IHI status (or an 'error' message if there is no match) (**Dependant IHI Lookup**).
 - (vi) The System Operator (DHS) uses the first name, last name, sex, date of birth, Medicare/DVA card number, IHI number, IHI record status and IHI status of the individual and each of the relevant dependants by providing that information (or making it available to) the System Operator (NIO).
 - (vii) The System Operator (NIO) uses that personal information, as well as existing information held in the PCEHR system, to check whether the individual or any of the dependants have an existing PCEHR (and, if so, whether they have taken control of their PCEHR), and to advise the System Operator (NIO) of the outcome.
- (c) The Dependant IHI Lookup process is the same as the IHI Lookup process for the individual discussed in sections 5.3.2 and 5.3.3. We refer to **Recommendations 12, 13 and 14**.

System Operator (DHS)

- (d) We consider that in relation to the System Operator (DHS):
 - (i) the disclosure of personal information about the individual (and any dependants) to Medicare will be in accordance with APP 6.1 on the basis that:
 - (A) one of the primary purposes for which the personal information will have been collected is to implement the individual's opt-out choice (which may include a choice to opt-out one or more of the individual's dependants); and
 - (B) the disclosure of that information to Medicare is for the purpose of identifying the individual's dependants for which an opt-out decision may be made;
 - (ii) the collection of personal information about the individual and relevant dependants from the individual and Medicare will be permitted under:
 - (A) APP 3.1, as the collection is reasonably necessary to implement the individual's decision to opt-out their dependants; and
 - (B) APP 3.6(b), as it would be unreasonable and impracticable to collect the information directly from the dependants having regard to the real-time online environment, the important need to have independent information from Medicare about which dependants are listed on the individual's Medicare card for authentication of the status as dependants, and the fact that the dependants may be young children; and
 - (iii) the use of personal information (i.e. by providing information to the System Operator (NIO)) will be in accordance with APP 6.1 on the basis that:
 - (A) one of the primary purposes for which personal information about the individual and dependants will have been collected is to enable the individual to exercise their opt-out choice by cancelling an existing PCEHR relating to themselves or a dependant; and
 - (B) the use of that information is for the purpose of ascertaining whether the individual or any dependants have an existing PCEHR (and, if so, whether they have taken control of their PCEHR).

Medicare

- (e) In relation to Medicare, we consider that the collection of the personal information of the individual and any dependants from the System Operator (DHS) will be permitted under:
 - (i) APP 3.1, on the basis that the information collected is the minimum data set reasonably necessary for Medicare to locate the individual's Medicare record and identify the relevant dependants listed on the individual's Medicare card; and
 - (ii) APP 3.6(b), on the basis that it would be impracticable to collect the information directly from the individual having regard to the real-time online environment (and the inconvenience to the individual themselves if they had to deal with the System Operator (DHS) and Medicare separately).

System Operator (NIO)

- (f) We consider that:
 - (i) the use of personal information about the individual and dependants (provided by the System Operator (DHS)) will be in accordance with APP 6.1 for the reasons discussed in paragraph 5.4(d)(iii); and
 - (ii) the use of existing information held in the PCEHR system would be permitted under APP 6.1(a) (consent). This is because by choosing to opt-out themselves and their dependants (including potentially cancelling any existing PCEHR registration), the individual could be taken to have given their implied consent to the System Operator (NIO) checking whether the individual or any dependants have an existing PCEHR (and, if so, whether they have taken control of their PCEHR).

5.4.2 Privacy risk – use and disclosure of personal information

- (a) In order to identify and notify the System Operator (DHS) of the relevant dependants, Medicare will use:
 - (i) the information about the individual provided by the System Operator (DHS) – this use will be for the primary purpose of collection, and therefore will be in accordance with APP 6.1; and
 - (ii) existing personal information held in the Medicare system.
- (b) Personal information held in the Medicare system would have been collected by Medicare for Medicare-related purposes (e.g. Medicare enrolment and processing Medicare claims). The use and disclosure of that data to identify dependants of the individual in the opt-out process will be for a secondary purpose.
- (c) Even if the individual's consent were to be obtained, there is a risk that this would not be sufficient to rely on APP 6.1(a), as there may be dependants who have the capacity to give consent for themselves. Further, consent may not be valid because the user may not in fact be the relevant individual but pretending to be that person. In any case, we understand that the implementation of the Opt-Out Model (including the opt-out process) is intended to be supported by legislative authority.
- (d) Medicare could use and disclose information in the Medicare system under APP 6.2(b) if it were 'authorised or required by law'.
- (e) The Department advises that all of the information handled by Medicare in this step is 'identifying information' within the meaning of subsection 9(3) of the PCEHR Act. The Chief Executive Medicare is authorised to use and disclose to the System Operator identifying information about an individual if:
 - (i) the individual is applying for, or has applied for, registration; and
 - (ii) the use or disclosure is for the purpose of verification by the System Operator of the identity of the individual (subsection 58(1) of the PCEHR Act).
- (f) In our view, the use and disclosure of identifying information by Medicare is not likely to be for the purposes of verification by the System Operator of the identity of the dependant. The purpose of the process is to identify a link between the individual/authorised representative (who has already gone through an identity verification process) and the dependant.

- (g) A person opting out (or opting out their dependant) will not be applying for registration. Consequently, section 58 of the PCEHR Act would need to be amended to broaden its scope to enable the APP 6.2(b) 'authorised by law' exception to be relied upon by Medicare. We understand that such an amendment is being proposed by the Department.⁵¹
- (h) We also recommend further amendments (which do not currently seem to be proposed) be made to section 58 of the PCEHR Act to broaden the permitted purposes of uses and disclosures beyond identity verification.

Recommendation 16

That the drafting instructions for the proposed amendments to the PCEHR Act ensure that section 58 is amended so that the scope of the provision:

- allows Medicare to use and disclose identifying information for the purposes of implementing the individual's choice to opt-out their dependants; and
- allows for purposes of uses and disclosures beyond identity verification.

Collection notice

- (i) To ensure compliance with the APP 5 obligations of the System Operator and Medicare, information about the collection, use and disclosure of personal information by those entities should be covered by the scope of the Online Opt-Out Service collection notice. We refer to **Recommendation 11**.

5.5 Making opt-out and/or cancellation decision

- (a) The Online Opt-Out Service will display to the individual the first and last names of the individual and relevant dependants, as well as an indication of whether the individual or any of their listed dependants have an existing PCEHR. Dependants who have taken control of their own PCEHR will be included in the disclosed list, however the individual will not be able to opt-out for them. This involves a disclosure of personal information about dependants to the individual. We note that only the names of dependants are shown, and not the age and sex. We consider that this is a privacy positive measure that promotes APP 11. This is because if, despite the identity verification process being passed, a user of the Online Opt-Out Service is not the true authorised representative (e.g. a malicious user) that person would only find out limited information about the dependants that is shown on the Medicare card. Therefore the level of privacy impact of any unauthorised access to that information by a third party user would be reduced.
- (b) We consider that the disclosure of the names of dependants will be for the primary purpose that the System Operator (DHS) collected the information (i.e. to enable an individual to opt-out their dependants) or a directly related secondary purpose (preventing the opting-out of those dependants who have taken control of their own PCEHR), and therefore will be in accordance with APP 6.1.
- (c) By selecting the individuals for whom the individual wishes to opt-out or cancel an existing PCEHR (i.e. the individual and/or any relevant dependants) and submitting those choices, the System Operator (DHS) will collect personal information about the individual and their dependants from the individual. The individual will also need to provide an assertion of parental responsibility in relation to any dependants for whom they wish to

⁵¹ Department of Health, 'Initial drafting instructions for amendments to the PCEHR and HI Act – 28 November 2014'.

opt-out or cancel a PCEHR. This collection by the System Operator (DHS) will be permitted under:

- (i) APP 3.1, as the collection is reasonably necessary to implement the individual's decision to opt-out themselves and/or their dependants, or cancel an existing PCEHR; and
 - (ii) APP 3.6(b), as it would be unreasonable and impracticable to collect the personal information about dependants directly from the dependants given their status, and having regard to the real-time online environment.
- (d) The Online Opt-Out Service will display a notification to the individual to advise that the opt-out / cancellation process was successful. The message will include the time, date and Transaction Reference Number (TRN) of the transaction, but not any personal information.
- (e) For the purposes of APP 11, we consider that the potential risk of a person opting out or cancelling a PCEHR for a dependant without legal authority will be mitigated by:
- (i) the fact that a person can only opt-out dependants on their Medicare card grouping; and
 - (ii) the requirement that the person provides an assertion of parental responsibility.

5.6 Cancellation of existing PCEHR

- (a) To give effect to a PCEHR cancellation decision, the System Operator (DHS) will:
- (i) provide the relevant individual's IHI, first name, last name, sex and date of birth to the System Operator (NIO); and
 - (ii) direct the System Operator (NIO) to cancel the PCEHR registration of those individuals.
- (b) Accenture acts as the NIO in its capacity as a contracted service provider to the System Operator. The provision of the above information by the System Operator (DHS) to the System Operator (NIO) would constitute a 'use' for the purposes of the Privacy Act, and will be for the primary purpose of collection, that is to implement the individual's PCEHR cancellation decision in respect of themselves and/or any dependants. Accordingly, this use by the System Operator (DHS) will be in accordance with APP 6.1.
- (c) The cancellation of a PCEHR by the System Operator (NIO) is an existing process, and is out of scope for this PIA.

5.7 Opt-out notification

5.7.1 Notification process

- (a) The individual/authorised representative will be sent a notification by Medicare to confirm that the individual and/or their dependants have been opted-out of automatic PCEHR registration. The notification will be sent to the individual's pre-existing Medicare-registered postal address, or email address held by Medicare or myGov.
- (b) The opt-out notice would be separate from any notice regarding cancellation.
- (c) The System Operator (NIO) will disclose to Medicare the following information for the purpose of notifying an individual/authorised representative of the opt-out outcome:

- (i) IHI, first name, last name, sex and date of birth of the individual/authorised representative; and
 - (ii) if relevant, the IHI, first name, last name, sex and date of birth of any dependants.
- (d) We understand that all of this information (including IHIs) is reasonably necessary for Medicare to send out the opt-out notices. On that basis, we consider that the collection by Medicare will be permitted under:
- (i) APP 3.1 as the information is reasonably necessary for Medicare to notify the individual of their opt-out decision; and
 - (ii) APP 3.6(b) as it would be impracticable to collect this information directly from the individual given:
 - (A) the electronic environment and arrangements; and
 - (B) that the reason that contact address details held by Medicare are used in this process is to leverage an independent source of contact information in case the user is not in fact the individual/authorised representative.

5.7.2 Privacy risk – use and disclosure of personal information

Disclosure by the System Operator (NIO)

- (a) The System Operator (NIO) will have collected the individual's personal information to process their opt-out request. The disclosure of personal information to Medicare could be characterised as being for a secondary purpose because the individual's opt-out request has already been actioned by this stage in the process. Although we consider notification to be related to the primary purpose, it is unclear whether the disclosure by the System Operator (NIO) to Medicare would be within the reasonable expectation of the individual for the purposes of relying on APP 6.2(a). This risk could be mitigated by ensuring that various communications with individuals – including the collection notice on the Online Opt-Out Service – explain the various disclosures that occur in the context of implementing an opt-out request.
- (b) We refer to **Recommendation 11**.

Use by Medicare

- (c) Medicare will use the Medicare database to identify the postal address of the individual, and to send a notification to the individual. The independent source of contact for the individual held by Medicare is intended to be a risk mitigation measure in case the Online Opt-Out Service user was an imposter.
- (d) A potential APP 11 security risk arises if the individual's Medicare-registered address is out of date and the notification is sent to the incorrect address. This risk can be mitigated by the mailed notification containing limited personal information of the individual and any relevant dependants. We understand that Medicare's practice is to note against an individual's Medicare record if Medicare or PCEHR related mail sent to the individual is returned, and Medicare does not send any further Medicare or PCEHR related mail to that address until the issue is resolved. This provides some protection against the security risk of using stored addresses.
- (e) We assume that the individual's mailing address (as stored in the Medicare database) was collected for Medicare-related purposes. The use for the purposes of the PCEHR system is unlikely to have been consented to by the individual, and we doubt that it would be within the individual's reasonable expectation that their address would be used by Medicare for PCEHR-related purposes when it was provided to Medicare.

- (f) The individual's address is 'identifying information' within the meaning of that term in subsection 9(3) of the PCEHR Act. For the reasons discussed in paragraphs 5.4.2(e)-5.4.2(g), we do not consider that the scope of section 58 is sufficiently broad to authorise the use of the individual's identifying information for PCEHR notification purposes. We refer to **Recommendation 16**.

5.8 Telephone and face to face channels

- (a) The Department advises that at this stage, it is anticipated that the information flows in relation to the telephone and face to face channels will be substantially the same as the online channel. The differences are that:
 - (i) in the face to face channel, a DVS check will not be required; and
 - (ii) alternative methods of providing individuals with an APP 5 collection notice will need to be developed for the telephone and face to face channels.
- (b) We understand the Department is currently considering EOI processes for the telephone channel. The privacy impacts will need to be assessed once that EOI process is determined, as well as the opt-out process in the telephone and face to face channels generally.

Recommendation 17

That the Department, in conjunction with DHS, develop a scripted message for telephone and face to face opt-out channels which identifies the specific information handling arrangements that arise during the opt-out process.

Recommendation 18

That the Department develop, or update existing, written materials (brochures, booklets etc.) to provide information about the opt-out process and the handling of personal information in that context.

5.9 Mail channel

We understand the Department is currently considering the opt-out process via mail channel. The privacy impacts will need to be assessed once that process is determined. We expect that one of the relevant privacy considerations will be the content of an opt-out paper form.

Chapter 6 Automatic registration (existing individuals)

6.1 Overview of automatic registration process (opt-out transition)

- (a) The information flows relating to automatic registration of the relevant existing individuals, including the creation of a 'shell' PCEHR and setting privacy controls, are described in detail in Schedule 2.
- (b) In summary:
 - (i) At the end of the Opt-Out Period, there will be automatic registration for a PCEHR, and a 'shell' record will be created, for all 'Automatic Registrants', which will be all individuals with a valid IHI, except for those individuals who:
 - (A) opted out during the Opt-Out Period;
 - (B) already have a PCEHR; or
 - (C) had a PCEHR, but cancelled their PCEHR registration prior to the commencement of the bulk automatic registration process (including those individuals whose PCEHR registration was cancelled during the Opt-Out Period).
 - (ii) Automatic Registrants will have a six week window (the Transition Period) to access their PCEHR via myGov and set their privacy controls before the PCEHR will become available for healthcare providers to access.
- (c) At the discretion of the System Operator (DHS), individuals who are deemed to be a risk to the security or integrity of the PCEHR system will not be registered.⁵²
- (d) The bulk registration process will occur at the end of the Opt-Out Period. From that date:
 - (i) registered individuals will need to cancel their registration in accordance with the existing process if they no longer want a PCEHR; and
 - (ii) the opt-out choice will only be available to individuals that become newly eligible for PCEHR registration, i.e. individuals who register for Medicare (e.g. newborns and immigrants) or register with the HI Service (see Chapter 7 for further discussion).

6.2 Identification of Automatic Registrants

6.2.1 Identification process

- (a) The System Operator (NIO) will request the HI Service Operator to provide the following information ('**HI Data Set**') for all individuals registered with the HI Service that have an active IHI status and verified IHI record status:
 - (A) IHI number, IHI record status and IHI status;
 - (B) first name and last name;
 - (C) sex;

⁵² PCEHR Act, section 41(2).

- (D) address (except where the individual is under 18 years); and
 - (E) date of birth.
- (b) The HI Service Operator will locate and disclose the HI Data Set of each 'active' individual to the System Operator (NIO). As the HI Data Set would not have been collected by the HI Service Operator for the purpose of facilitating automatic registration, we consider that the use and disclosure of the HI Data Set to the System Operator (NIO) in this context would constitute a secondary purpose. This raises a privacy risk in relation to compliance with APP 6, which is discussed in section 6.2.2 below.
- (c) The System Operator (NIO) will also request that the System Operator (DHS) send the same HI Data Set of the individuals that opted out of automatic PCEHR registration ('**Opt-Out Individuals**'). As NIO is a contracted service provider to the System Operator, we consider that:
 - (i) the provision of the HI Data Set for Opt-Out Individuals to the System Operator (NIO) will constitute a 'use' by the System Operator (DHS) and
 - (ii) this use by the System Operator (DHS) will be in accordance with APP 6.1 on the basis that the information is being provided for the primary purpose of collection, that is, to ensure that Opt-Out Individuals are not automatically registered for a PCEHR in accordance with their opt-out choice.
- (d) In relation the collection of the HI Data Sets by the System Operator (NIO) from the HI Service Operator, we consider that:
 - (i) for the purposes of APP 3.1, the collection is reasonably necessary for, and directly related to, the functions of the System Operator (NIO) in relation to implementing automatic registration, on the basis that this information is the minimum data required by the System Operator (NIO) to identify the Automatic Registrants and create PCEHRs for those individuals; and
 - (ii) the indirect collection of individual information from the HI Service Operator would be permitted under APP 3.6(b), on the basis that it would be unreasonable or impracticable for the System Operator (NIO) to deal directly with individuals having regard to:
 - (A) the excessive time and cost of dealing with individuals directly;
 - (B) the purpose of the opt-out system being an automatic registration of individuals who have not opted out of PCEHR; and
 - (C) the fact that individuals will not necessarily know their IHI number, IHI record status and IHI status.
- (e) The System Operator (NIO) identifies the Automatic Registrants by removing the Opt-Out Individuals, and individuals who have or had a PCEHR, from the list of 'active' individuals provided by the HI Service Operator. This involves a use by the System Operator (NIO) of:
 - (i) the personal information collected from the HI Service Operator – this use will be for the primary purpose of collection (i.e. to identify, and only register, Automatic Registrants), and therefore will be in accordance with APP 6.1;
 - (ii) the personal information received from the System Operator (DHS) – this information is used for the primary purpose that the System Operator collected the information (i.e. to implement opt-out decisions of individuals), and therefore will be in accordance with APP 6.1; and

- (iii) existing personal information held in the PCEHR system about individuals who have an existing or cancelled PCEHR – this existing data would not have been collected for the purposes of identifying Automatic Registrants, and therefore a privacy risk arises in relation to the use of that data for a secondary purpose. This is discussed further in section 6.2.2 below.

6.2.2 Privacy risks – use and disclosure of personal information

Use and disclosure of HI Data Set by HI Service Operator

- (a) We understand that the Department intends to rely on legislative authority rather than consent to facilitate the automatic registration of Automatic Registrants.
- (b) As discussed in paragraph 5.3.3(i), the HI Service Operator is authorised to disclose to the System Operator:
 - (i) a healthcare identifier for a purpose for which the System Operator is authorised to collect, use or disclose the healthcare identifier under Division 2A of the HI Act (section 19A of the HI Act); and
 - (ii) 'identifying information' for any purpose for which the System Operator is authorised to collect, use or disclose identifying information under Division 2A (section 11A of the HI Act).
- (c) For the reasons discussed in paragraphs 5.3.3(f) and 5.3.3(k), we consider that:
 - (i) section 22A of the HI Act would need to be amended to broaden its scope to allow the HI Service Operator to disclose an individual's IHI, IHI record status and IHI status to the System Operator in these circumstances; and
 - (ii) section 7 of the HI Act should be amended to ensure that IHI record status and IHI status will be covered under the definition of 'identifying information'.
- (d) We refer to **Recommendations 12, 13 and 14**.

Use of information by the System Operator (NIO)

- (e) We have assumed that the only existing information used in the PCEHR system falls within the definition of 'identifying information' in section 9(3) of the PCEHR Act.
- (f) There is currently no authorisation for the System Operator (NIO) to use identifying information (as defined in subsection 9(3) of the PCEHR Act) where:
 - (i) the use relates to the performance of functions or the exercise of powers by the System Operator in respect of the PCEHR system; and
 - (ii) the information has not been collected from the HI Service Operator.
- (g) We note, however, that an amendment to section 58 of the PCEHR Act is proposed, which would have the effect of authorising the System Operator to use identifying information about an individual (even where such information does not come from the Chief Executive Medicare, DHS, DVA or the Department of Defence) where that use relates to the performance of functions or the exercise of powers by the System Operator (NIO) in respect of the PCEHR system.

Recommendation 19

Further to **Recommendation 16**, that the proposed amendment to section 58 of the PCEHR Act allows the System Operator/NIO to use identifying information for the purposes of identifying Automatic Registrants and implementing automatic registration.

6.3 Creation of shell PCEHR

- (a) The System Operator (NIO) will create a 'shell' PCEHR for each Automatic Registrant by using the HI Data Set collected from the HI Service Operator. This use will be in accordance with APP 6.1 on the basis that it is for the primary purpose of collection.
- (b) By setting the default access and content control settings for the shell PCEHR, the System Operator (NIO) will also effectively 'collect' personal information by making a record about what default settings apply in respect of the individual's PCEHR. This will be permitted under APP 3.1 as establishing an individual's PCEHR privacy control settings is reasonably necessary for the functions and activities of the System Operator (NIO) in relation to the operation of the PCEHR system.

6.4 Privacy control settings

6.4.1 Existing privacy control settings

- (a) The PCEHR system currently allows individuals to 'control' their PCEHR by providing a wide range of adjustable privacy controls over both content and access, which include:
 - (i) Record Access Code (**RAC**) to restrict access by healthcare providers (at organisation level) from being able to access an individual's PCEHR;
 - (ii) Limited Document Access Code (**LDAC**) to restrict access by healthcare providers (at organisation level) from accessing certain documents in an individual's PCEHR;
 - (iii) removing or reinstating documents from a record;
 - (iv) the visibility of information (including MBS, DVA, PBS, RPBS, ACIR and AODR information); and
 - (v) restricting and managing access by nominated representatives.
- (b) In addition, there are a range of existing adjustable notification settings so an individual can request email or SMS notifications about access or PCEHR content changes, for example:
 - (i) a new healthcare provider organisation accessing the PCEHR for first time;
 - (ii) a new Shared Health Summary being uploaded to the PCEHR;
 - (iii) a nominated representative accessing the PCEHR;
 - (iv) access by a healthcare provider who is asserting a medical emergency (i.e. declared serious threat to life, health or safety); or
 - (v) a new myGov account has been linked to the PCEHR.

- (c) If the individual does not set any privacy controls, the default access and content control settings are that all healthcare providers involved in the individual's care will be able to access, view all documents, and upload documents to the customer's PCEHR. The individual will not receive any notifications if they have not 'turned on' any notification settings.

6.4.2 Privacy control settings for Automatic Registrants

- (a) During the Transition Period, and before the PCEHRs become available for healthcare providers to access, Automatic Registrants will be able to access their PCEHR through myGov and set their privacy control and notification settings.
- (b) Automatic Registrants can also opt-out of the automatic flow of Medicare data that will be included in the PCEHR (see section 8.1.1 of this report).
- (c) A six week Transition Period may not give individuals sufficient opportunity to set their privacy controls before the PCEHR becomes available to healthcare providers (in particular if the window falls over the Christmas and New Year period, when many people are on holidays or otherwise busy).
- (d) Automatic Registrants will not be able to set document level access controls during the Transition Period as there will not be any clinical data in the shell PCEHRs.
- (e) The Department advises that there will be no diminution of the existing range of privacy control settings and notification settings, or to the existing default settings. One additional notification option will be added, which will allow individuals to choose to be notified by email or SMS each time their PCEHR is accessed.
- (f) The Department also advises that it intends to improve the usability of the privacy control settings so that individuals may better understand and exercise their various choices about content, access controls and notifications. We consider this to be a privacy positive action, as not only will it assist individuals in making informed choices about their privacy, but also assist them to take their own steps to protect their data and minimise risks to data security for the purposes of APP 11.
- (g) Privacy control settings are complicated matters to communicate at the best of times, let alone to a largely uninterested audience. A submission to the PCEHR Review makes this point well:

*Consumers are generally only interested in their health record when they are ill. Trying to get consumers to be interested in one's medical record when the majority of consumers are in reasonably good health (or ignoring bouts of ill health) is an uphill battle.*⁵³

- (h) Indeed, the statistics on individual access to date seems to bear this out. Of the approximately 2 million PCEHRs registered as at 31 March 2015, only 758,109 have been linked to a myGov account.⁵⁴ This suggests that almost two-thirds of existing PCEHR consumers have never accessed their records online.
- (i) The proposed default privacy control settings mean that the individual who does not act to gain access to their PCEHR and adjust their privacy control settings will receive no notifications, retrospective Medicare data will begin to populate their PCEHR as soon as a healthcare provider either views or uploads to it, and all clinical documents in the PCEHR will be available to all their healthcare providers.

⁵³ Western Sydney Medicare Local, *Submission to the PCEHR Review*, 21 November, 2013, p.4.

⁵⁴ Information provided to us by the Department by email dated 13 May 2015.

- (j) When the default position is to allow all current and past clinical information to be shared with all current and past healthcare providers, there is a risk that individuals do not understand that this means, for example:
 - (i) that their physiotherapist, optometrist and dentist can see from their PBS records that they have been prescribed antidepressants;
 - (ii) that their boyfriend, who works in the hospital where they were once treated for a broken arm, can see that they have recently terminated a pregnancy in a different hospital; or
 - (iii) that their home address may be included in a clinical document, accessible by a person who wishes them harm.
- (k) Each of these scenarios can be prevented by the individual, but only if they know that the risk exists in the first place, and that they can adjust their privacy control settings to manage that risk. The core problem raised by an Opt-Out Model is that the individual may not know either of these things before their information is shared.
- (l) There is a spectrum of privacy harms which could potentially arise when an individual's health information is exposed to third parties, beyond their reasonable expectations. This spectrum has tangible or 'material' harms at one end (such as physical harm or threats of violence, stalking and harassment, identity theft, financial loss and psychological damage), intangible or 'moral' harms in the middle (such as reputational damage, 'creepy inferences', humiliation, embarrassment or anxiety, loss of autonomy, discrimination and social exclusion), and abstract or 'social' harms at the other end (such as the loss of trust and social cohesion posed by a 'surveillance society').⁵⁵
- (m) In terms of potential privacy controls to mitigate against this risk, one option we considered, but rejected, was to recommend altering the default settings, to more tightly limit access to the records of individuals who did not opt-out, and who have never accessed their record in order to adjust their privacy control settings. It would for example be possible to prevent the retrospective Medicare-provided data (PBS, MBS etc.) from populating the record unless the individual actively consented otherwise; or to mark all clinical documents as 'Restricted' by default, meaning no other healthcare provider could access them until the individual changed either the document's settings, or the healthcare provider's access level.
- (n) However, we appreciate that doing so would likely undermine the very premise upon which the Opt-Out Model is being proposed in the first place. That is, the 'tipping point' for the PCEHR system delivering value to both individuals and clinicians will not be reached until clinicians believe that for the vast majority of their patients,⁵⁶ they will find not only that a PCEHR exists, but that from 'day one' it will already have at least some meaningful content, such as the two years' worth of retrospective Medicare-provided data (PBS etc.), and that they can start adding further content to it immediately.

⁵⁵ This spectrum of privacy harms is drawn from work by the former UK Information Commissioner, as well as the [Future of Privacy Forum's](http://www.futureofprivacy.org) paper, "Benefit-Risk Analysis for Big Data Projects", September 2014, available at www.futureofprivacy.org

⁵⁶ The Department's assumption is that the vast majority of individuals will not opt out, and that the vast majority will not deviate from the default privacy control settings. Experience to date certainly suggests that only a very small number of PCEHR consumers have ever adjusted their privacy control settings.

- (o) We also considered, but rejected, an option to recommend altering the default settings, to require notifications to individuals. Until an individual 'touches' their record in some way, the only contact details the PCEHR system has for that individual comes from their Medicare record. Medicare does not necessarily have an up-to-date email address or mobile phone number for each individual, and if it did, it would not have been collected for the purpose of notifying them about PCEHR matters. The risk of communications going to the wrong person – which could itself reveal sensitive information about the individual⁵⁷ – is too great to recommend such an option.
- (p) The only practical solutions to this risk therefore involve extensive communications and education campaigns, and assistance for particularly vulnerable individuals, as Deloitte has noted:

Many stakeholders raised concerns about how those who aren't computer literate, literate in English or not well connected into society will be made aware of the PCEHR and will be encouraged to participate. Particular groups mentioned included the aged and frail, migrants and refugees, individuals with cognitive impairment and those in lower socio-economic groups. Individuals in these groups may not be frequent users of electronic communications and may not easily be able to access online information or services; hence consideration needs to be given to how these groups will be communicated to and engaged and how their participation in something like the PCEHR will be supported.⁵⁸

- (q) We suggest that the explanations given to individuals about the various privacy controls need to be clear, including explanations about the adjustable privacy control settings and what else the individual can do to manage their privacy concerns. Topics which should be included in individual-oriented communications should at least include:
- (i) what types of healthcare providers can access your PCEHR (e.g. medical and administration staff at GPs, hospitals, specialists, allied health providers such as dentists, optometrists and physiotherapists);
 - (ii) the circumstances in which healthcare providers can access your PCEHR (e.g. whether this includes in the context of conducting a medical assessment on behalf of an employer or insurance company);
 - (iii) how a healthcare provider can access your PCEHR (i.e. what details a healthcare provider needs to know in order to find your PCEHR);
 - (iv) how you can control the content of your PCEHR (i.e. choices in relation to Medicare-provided data like PBS, MBS etc.; and choices in relation to uploading individual clinical documents) – including the default position if you do not adjust your privacy control settings;
 - (v) how you can control access to the content in your PCEHR (i.e. choices such as setting a RAC, or restricting access in relation to particular clinical documents) – including the default position if you do not adjust your privacy control settings;
 - (vi) how you can look at the audit log to monitor who has looked at your PCEHR;

⁵⁷ For example, a notification that the consumer's PCEHR has just been accessed by a drug and alcohol rehabilitation service could, if sent to a shared email address, reveal health information about the consumer to a family member.

⁵⁸ Draft Deloitte report, p.8.

- (vii) how you can control notifications to yourself when something happens with your PCEHR – including the default position if you do not adjust your privacy control settings;
 - (viii) what to do if you have a particular concern about someone else pretending to be you in order to see your PCEHR (limit the public availability of important keys to your identity – e.g. do not publish your date of birth on social media)
 - (ix) what to do if you have a particular concern about exposure of your home address (i.e. ask healthcare providers to not include your home address in clinical documents to be uploaded to the PCEHR);
 - (x) what to do if you have a particular concern that a healthcare provider might be tempted to inappropriately access your PCEHR, for example because you are a public figure, or you have an ex-partner who works in the health sector (e.g. adjust your PCEHR privacy control settings to set a RAC, or block access by that particular healthcare provider);
 - (xi) what to do if you have a particular concern about your historical data (e.g. go to Medicare Online to see what your PBS / MBS historical data reveals about you, and then choose your privacy control settings);
 - (xii) where to go for more information (e.g. link to the Australian Privacy Commissioner's fact sheet on protecting privacy in your PCEHR); and
 - (xiii) where to go if you have a privacy complaint (including the Privacy Commissioner).
- (r) Methods of explanation could potentially include online tutorials and video clips, and mock-ups of different healthcare provider 'views' of data, to illustrate the various access control settings.
- (s) The communication strategy also needs to incorporate methods of communicating the information outlined above to audiences facing existing barriers to receiving, accessing or understanding mainstream communications.

Recommendation 20

That the Department consider allowing longer than a six week Transition Period for individuals to adjust their privacy control settings.

Recommendation 21

Information about setting privacy controls, including the way in which it is presented should be easy for individuals to understand. Privacy controls should also be as easy as possible to implement.

Recommendation 22

That the Department engage individuals in re-designing the labelling, layout and explanation of the various privacy control settings, so as to ensure that communications are clear, neutral and explicit.

Recommendation 23

That the Department ensure that clear, neutral and explicit information is available to the individual, including at the Online Opt-Out Service, to explain built-in privacy features of the system, how things will work under the default settings, and how the individual can adjust their privacy control settings and take other steps to address various privacy concerns they might have.

Recommendation 24

That the Department provide or fund specialist assistance to help vulnerable and disadvantaged individuals (such as individuals from a non-English speaking background, the illiterate, homeless, and adults with limited or no capacity) to understand and utilise their privacy control settings.

6.5 Pseudonymous PCEHR registration

- (a) APP 2 requires agencies to give individuals the option of interacting with the agency anonymously or by using a pseudonym, unless it would be impracticable to do so, or in circumstances where dealing with an identified individual is required or authorised by law.
- (b) The PCEHR system currently allows an individual to register for a PCEHR based on a pseudonymous identity, so long as the individual is a holder of a pseudonymous IHI.⁵⁹
- (c) The Department advises that it currently has a process enabling individuals to register for a PCEHR on a pseudonymous basis and that a process will be developed to allow opt-out by holders of pseudonymous IHIs (as the Online Opt-Out Service will not be able to be used in this situation). The privacy impacts will need to be assessed once that process is determined.

⁵⁹ See [Application to request a pseudonym Individual Healthcare Identifier record](http://www.humanservices.gov.au/spw/customer/forms/resources/4484-1303en.pdf), available at: <http://www.humanservices.gov.au/spw/customer/forms/resources/4484-1303en.pdf>.

Chapter 7 Automatic registration of new Medicare enrolments and IHI registrants

7.1 Overview of automatic registration of new Medicare enrolments and IHI registrants

- (a) At the end of the Opt-Out Period, the following individuals will be automatically registered for a PCEHR unless they opt-out:
 - (i) individuals who enrol for Medicare (which primarily include newborn babies and immigrants); and
 - (ii) other individuals who are not eligible for Medicare but apply for (and obtain) a verified IHI.
- (b) An individual may indicate that they wish to opt-out of PCEHR registration in:
 - (i) the Medicare enrolment application, which will be either:
 - (A) *for newborns, the Newborn Child Declaration*: When a baby is born, the parent/guardian of the newborn (typically the newborn's mother) will be provided with, and will complete, the relevant form. This form currently allows the parent/guardian to apply for a range of benefits, and it is proposed that, after the start of the Opt-Out Period, this form will also give the parent/guardian the choice of opting out the newborn from automatic PCEHR registration;⁶⁰
 - (B) *for new residents, the Medicare Enrolment Application Form (Form 3101)*⁶¹: Certain Australian visa holders⁶², Australian citizens returning to live in Australia, and New Zealand citizens living in Australia can enrol for Medicare by completing Form 3101. It is proposed that, after the start of the Opt-Out Period, this form will give individuals registering for Medicare the choice to opt-out of automatic PCEHR registration.
 - (ii) the *Healthcare Identifiers Service - Application to Create, Verify or Merge an Individual Healthcare Identifier Form (Form 2888)*:⁶³ Some individuals who are eligible for Medicare enrolment may choose not to enrol in Medicare. Other individuals, such as temporary visa holders, may be ineligible for Medicare. These people may still apply to register with the HI Service by completing Form 2888. This form will now give these individuals the choice to opt-out of PCEHR registration.
 - (iii) a process to be developed to ensure that people for whom DVA obtains an IHI have the opportunity to opt-out of PCEHR registration.

⁶⁰ We understand that individuals enrolling a newborn in Medicare using the new pre-birth registration process and DHA smartphone app will still complete the same form (at least as it relates to PCEHR information). The difference is that the form is submitted using the app rather than in hard copy to Medicare.

⁶¹ [Medicare Enrolment Application Form](http://www.humanservices.gov.au/customer/forms/3101) (also referred to as Form 3101), available at <http://www.humanservices.gov.au/customer/forms/3101>.

⁶² Migrants living in Australia, persons applying for permanent residency and living in Australia, visitors to Australia, and permanent resident visa holders who were previously enrolled in Medicare that are returning to living in Australia.

⁶³ [Healthcare Identifiers Service - Application to create, verify or merge an Individual Healthcare Identifier form](http://www.humanservices.gov.au/customer/forms/2888) available at <http://www.humanservices.gov.au/customer/forms/2888>.

- (c) If an individual does not indicate in the relevant form that they wish to opt-out, then they will be registered for a PCEHR, subject to System Operator discretion to not register any particular individual.
- (d) The information flows relating to the opt-out process and automatic registration of new Medicare enrolments and IHI registrants are described in detail in Schedule 3.
- (e) We note that:
 - (i) the existing Medicare enrolment and IHI application processes are out of scope for the purposes of this PIA, and this PIA only assesses the privacy risks arising in relation to the proposed change to those application processes arising from the Opt-Out Model;
 - (ii) this chapter assesses the privacy risks relating to the automatic PCEHR registration of individuals once they have been registered with Medicare or obtain a verified IHI from the HI Service Operator, and involve the same information flows for all categories of 'new PCEHR registrants'; and
 - (iii) the System Operator (NIO) will not:
 - (A) undertake its own verification process to check the identity of an individual or the relationship between an individual and purported authorised representative, but will rather rely on the checks that will be undertaken by Medicare or the HI Service Operator (as relevant); or
 - (B) 'link' dependants who are registered for a PCEHR to the authorised representative. If the authorised representative wishes to control the dependant's PCEHR, they must gain access via the existing channels.

7.2 Making the opt-out decision

7.2.1 Communication

- (a) As discussed elsewhere in this report, a key privacy right under Australian privacy law is for individuals to be made aware of what personal information is going to be collected about them, for what purposes. This is usually done by way of what is typically known as a 'privacy notice'.
- (b) Communication with individuals is important from an APP 5 compliance perspective, which will require that individuals are informed about:
 - (i) the identity and contact details of the collecting entity;
 - (ii) the purpose for which their information is collected;
 - (iii) whether the entity is authorised or required to collect the information by law;
 - (iv) information about the usual disclosures the entity makes;
 - (v) whether the entity is likely to disclose their information to an overseas recipient; and
 - (vi) the fact the entity's privacy policy contains information about other privacy matters, such as accessing and seeking the correction of personal information and making a complaint in relation to the handling of personal information.
- (c) Clear communications will also be important in terms of meeting community expectations. In an Opt-Out Model, individuals require information to enable them to make informed

decisions about whether or not to opt-out, and how they can adjust their privacy control settings. We refer to **Recommendation 11**.

7.2.2 Newborn Child Declaration

- (a) The Newborn Child Declaration currently provides, under the heading 'Important Information' (at page 3):

If you have applied to register your newborn child for an eHealth record, information in this form will be collected by the eHealth Record System Operator (the Secretary of the Department of Health) to verify your identity, create a record for your child and manage the eHealth record system. To verify your identity, the information in this form is compared to information held by the Department of Human Services for Medicare purposes.

To create an eHealth record for your child, information about you and your child, including health information, will be collected from registered healthcare providers, government programs such as Medicare or you. Healthcare providers, representatives nominated by you, government agencies operating the eHealth record system and private firms providing services to support operation of the system may collect, use and disclose your child's information disclosed to provide healthcare and operate the eHealth record system.

You can set up online access at www.ehealth.gov.au to view and manage information in your child's record.

In specific situations information relating to your child can be collected or shared without consent, for example if there is a serious threat to your child's safety or if authorised by a court. The Personally Controlled Electronic Health Records Act 2012 and the Healthcare Identifiers Act 2010 authorise use of information in this way. A detailed privacy statement is available at the Privacy and security tab at www.ehealth.gov.au

For information about privacy in the eHealth record system or other eHealth enquiries call 1800 723 471. For more information about how your and your child's information is handled in the eHealth record system, you can read the full Privacy statement by visiting www.ehealth.gov.au

- (b) This information does not clearly specify what information provided in the Newborn Child Declaration is given to the System Operator, or how the System Operator will obtain it (i.e. that it will be collected by Medicare, disclosed to the HI Service Operator, which will then disclose it to the System Operator).
- (c) We understand that this is a result of the practical limitations associated with including PCEHR specific information in an already long and complex form. Any risk associated with a parent/guardian not being fully informed about how their child's health information will be handled in the PCEHR system after registration could be mitigated by ensuring that the letter sent to the parent/guardian confirming their child's registration includes an information sheet containing all relevant information which was not able to be communicated via the Newborn Child Declaration.

Recommendation 25

That the information to be included in the Newborn Child Declaration must at the very least make clear that unless they opt-out the newborn, the newborn will be registered for a PCEHR (i.e. a PCEHR will be created for them).

Recommendation 26

That further information be included in the Newborn Child Declaration, or if this is not possible provided as an information sheet to parents/guardians as soon as practicable after the parent/guardian receives the Newborn Child Declaration, which advises the parent/guardian in plain language:

- the information that will be collected by the HI Service Operator and the System Operator, and how it will be collected;
- what the default privacy control settings in the PCEHR allow;
- how the parent/guardian can adjust the newborn's PCEHR privacy settings;
- who to contact if the parent/guardian has an enquiry; and
- who to contact, including the Privacy Commissioner, if the parent/guardian has a privacy complaint.

7.2.3 Forms 2888 and 3101

- (a) Forms 3101 and 2888 are forms currently used by Medicare and the HI Service Operator to enable individuals to apply for enrolment in Medicare and registration in the HI Service (respectively), and currently contain no information about the PCEHR System or the opt-out process.
- (b) In order to comply with APP 5 the Medicare Enrolment Form will need to be updated to address the matters in APP 5.2.

Recommendation 27

That the following information be provided as part of Forms 2888 and 3101, or by way of an information sheet attached to or provided with those forms:

- an explanation that, unless the individual decides to opt-out, they will be registered for a PCEHR;
- the information that will be collected by the System Operator, and how it will be collected;
- what the default privacy control settings in the PCEHR allow;
- how they can opt-out or adjust their privacy control settings if they wish;
- who to contact if they have an enquiry; and
- who to contact, including the Privacy Commissioner, if they have a privacy complaint.

7.2.4 Where DVA enables IHI to be issued

- (a) The Department is investigating the process used by DVA when it provides information to enable IHIs to be issued for individuals covered by its schemes, and how the opportunity for the individual to opt-out of PCEHR registration can be incorporated into that process.
- (b) At this stage, it appears the process will involve the following:
 - (i) The individual provides DVA with information on whether the individual wants to opt-out of PCEHR registration. The Department will identify the category of individuals who will need to be given the choice to opt-out (i.e. individuals who are not registered with Medicare), and develop a process to give these individuals an opportunity to opt-out. This PIA assumes that, if an individual decides to opt-

out, the individual will provide the PCEHR opt-out information to DVA as part of DVA's existing process of interaction with the individual.

- (ii) If the individual opts-out, DVA provides Medicare with the PCEHR opt-out information along with the information required to register the individual with Medicare as entitled to receive DVA benefits (first name, last name, date of birth, address, sex and DVA number).
- (iii) If the individual opts-out, Medicare provides the HI Service Operator with the PCEHR opt-out information along with the information required by the HI Service Operator to identify the individual.

Recommendation 28

That the Department develop a process to ensure that individuals who will be issued an IHI as part of the DVA process have the opportunity to opt-out of PCEHR registration, and that the following information be provided to those individuals as part of that process (by inclusion in relevant forms or by way of an information sheet attached to or provided with those forms):

- an explanation that, unless the individual decides to opt-out, they will be registered for a PCEHR;
- the information that will be collected by DVA, Medicare, the HI Service Operator and the System Operator, and how it will be collected;
- what the default privacy control settings in the PCEHR allow;
- how they can opt-out or adjust their privacy control settings if they wish;
- who to contact if they have an enquiry; and
- who to contact, including the Privacy Commissioner, if they have a privacy complaint.

7.3 Submitting the forms

Medicare enrolment

- (a) For individuals applying for enrolment in Medicare, Medicare collects the PCEHR opt-out information in the Newborn Child Declaration / Form 3010 about the individual and any dependants and discloses it to the HI Service Operator.
- (b) The collection of personal information about the individual and relevant dependants (by Medicare and the HI Service Operator) will be permitted under:
 - (i) APP 3.1, as the collection is reasonably necessary to implement the individual's decision to opt-out themselves and/or their dependants;
 - (ii) in relation to collection of dependants' information by Medicare, APP 3.6(b), as it would be unreasonable and impracticable to collect the information directly from the dependants having regard to the fact that the dependants are children; and
 - (iii) in relation to collection by the HI Service Operator, APP 3.6 because:
 - (A) it is not practicable to obtain the information from the individual as this would require the individual to interact with the HI Service Operator as well as completing the relevant forms. By completing the relevant form the individual has expressed their wishes to opt-out of automatic registration and requiring further steps to implement this direction would make the opt-out system more difficult for individuals to use; and

- (B) provided that the forms are amended as recommended or information sheets are provided with the forms to describe the relevant collections, the individual completing the form can be taken to have consented to the collection of information by the HI Service Operator.
- (c) The disclosure of personal information about the individual (and any dependants) to the HI Service Operator will be in accordance with APP 6.1 on the basis that:
 - (i) one of the primary purposes for which the personal information will have been collected is to implement the individual's opt-out choice (which may include a choice to opt-out one or more of the individual's dependants); and
 - (ii) the disclosure of that information to the HI Service Operator is for the purpose of identifying the individual and dependants for which an opt-out decision has been made.

HI Service registration

- (d) For individuals applying for registration in the HI Service, the HI Service Operator collects the PCEHR opt-out information in the form about the individual.
- (e) The collection of personal information about the individual will be permitted under APP 3.1, as the collection is reasonably necessary to implement the individual's decision to opt-out.

DVA process

- (f) The process where DVA enables an IHI to be issued for an individual is under development but may be expected to include:
 - (i) DVA collecting personal information from the individual (including PCEHR opt-out information);
 - (ii) DVA disclosing to Medicare, and Medicare collecting, the PCEHR opt-out information (along with other information as part of the existing process); and
 - (iii) Medicare disclosing to the HI Service Operator, and the HI Service Operator collecting, the PCEHR opt-out information (along with other information).
- (g) The collection of personal information about the individual (by DVA, Medicare and the HI Service Operator) will be permitted under:
 - (i) APP 3.1, as the collection is reasonably necessary to implement the individual's decision to opt-out; and
 - (ii) APP 3.6 because:
 - (A) it is not practicable to obtain the information from the individual as this would require the individual to interact with Medicare and the HI Service Operator as well as with DVA. By providing the information to DVA the individual has expressed their wishes to opt-out of automatic registration and requiring further steps to implement this direction would make the opt-out system more difficult for individuals to use; and
 - (B) provided that information is provided with the relevant form to describe the relevant collections, the individual completing the form can be taken to have consented to the collection of information by Medicare and the HI Service Operator.

- (h) The disclosure of personal information about the individual to Medicare and the HI Service Operator will be in accordance with APP 6.1 on the basis that:
 - (i) one of the primary purposes for which the personal information will have been collected is to implement the individual's opt-out choice; and
 - (ii) the disclosure of that information is for the purpose of identifying the individual who has chosen to opt-out.

7.4 Implementing the opt-out decision

- (a) If an individual (including a dependant) has (or, for individuals who are dependants, their authorised representative has) indicated in the relevant form that they wish to opt-out:
 - (i) the HI Service Operator will disclose to the System Operator (DHS):
 - (A) the fact that the individual wishes to opt-out of automatic PCEHR registration; and
 - (B) the individual's IHI, IHI record status, IHI status, first name, last name, sex, address (except for individuals under 18 years) and date of birth;
 - (ii) the System Operator (DHS) will collect the personal information about the individual and any dependants from the HI Service Operator, and record the individual as having 'opted-out'.
- (b) We assume that the HI Service Operator will only disclose the amount of information that is reasonably required by the System Operator (DHS) to implement the opt-out choice, and ensure that the individual and/or any dependants are not automatically registered for a PCEHR. On that basis, we consider that the disclosure by the HI Service Operator:
 - (i) of the fact of the opt-out decision will be in accordance with APP 6.1 because the primary purpose for which Medicare (for Medicare enrolment applications) or the HI Service Operator (for HI Service registration applications) or DVA (for DVA IHI applications) collected the opt-out decision was to opt the individual out of automatic PCEHR registration; and
 - (ii) personal information about the individual who opted out (including the individual's IHI), to the extent it is reasonably required to identify the individual who opted-out, will also be for the primary purpose in accordance with APP 6.1.
- (c) In relation to the System Operator (DHS), we consider that the collection of personal information from the HI Service Operator will be in accordance with APP 3.1 because the collection is reasonably necessary to implement the individual's decision to opt-out themselves or their dependant(s) from automatic PCEHR registration.
- (d) In our view, the collection by the System Operator (DHS) from the HI Service Operator, a third party, the collection will also need to be in accordance with APP 3.6 because:
 - (i) an individual is unlikely to know his/her own IHI, IHI record status and IHI status and this information is available from the HI Service Operator;
 - (ii) it is not practicable to obtain other personal information from the individual as this would require the individual to interact with the System Operator (DHS) as well as completing the relevant forms. By completing the relevant form the individual has expressed their wishes to opt-out of automatic registration and requiring further steps to implement this direction would make the opt-out system more difficult for individuals to use; and

- (iii) provided that the forms are amended as recommended or information sheets are provided with the forms to describe the relevant collections, the individual completing the form can be taken to have consented to the collection of personal information from the HI Service Operator.

7.5 Automatic registration of new persons

- (a) If an individual has (or, for individuals who are dependants, their authorised representative has) not indicated in the relevant form that they wish to opt-out:
 - (i) the HI Service Operator will disclose to the System Operator (NIO) the individual's first name, last name, sex, date of birth, address (except for individuals under 18 years), IHI, IHI record status (verified) and IHI status (active); and
 - (ii) the System Operator (NIO) will:
 - (A) collect the personal information about the individual(s) from the HI Service Operator;
 - (B) use the personal information collected about the individual, as well as existing information held in the PCEHR system, to check whether the individual has an existing PCEHR registration;
 - (C) if the individual does not have a PCEHR registration, uses the individual's information collected from the HI Service Operator to:
 - (I) register the individual for a PCEHR; and
 - (II) set the default privacy control settings for the individual.
- (b) The information disclosed by the HI Service Operator to the System Operator (full name, address, date of birth, IHI and sex) is the information that is required to register an individual for a PCEHR.⁶⁴ Subject to the relevant form making it clear that one of the primary purposes of collection is to implement the individual's decision whether to opt-out, this disclosure will be for the primary purpose for which it was collected in accordance with APP 6.1.
- (c) The collection by the System Operator (DHS) will be in accordance with APP 3.1 because the information collected is required to register the individual for a PCEHR.
- (d) In our view the collection by the System Operator (DHS) from the HI Service Operator complies with APP 3.6 because:
 - (i) an individual is unlikely to know his/her own IHI, IHI record status and IHI status and this information is available from the HI Service Operator;
 - (ii) it is not practicable to obtain other personal information from the individual as this would undermine the automatic registration process; and
 - (iii) provided that the forms are amended as recommended or information sheets are provided with the forms to describe the relevant collections, the individual completing the form can be taken to have consented to the collection of personal information from the HI Service Operator.

⁶⁴ Address is used to let the individual know what address the System Operator will use for PCEHR purposes, and for statistical/reporting purposes.

- (e) The use of the information by the System Operator will be in accordance with APP 6.1 on the basis that it is for the primary purpose for which it was collected (which is to register the individual for a PCEHR).
- (f) We also note that we consider the proposed information flows involved in implementing an individual's decision not to opt-out to be a privacy positive because it leverages other concurrent processes, such as the identity verification conducted by Medicare or the HI Service Operator, which minimises unnecessary data handling by the System Operator.

7.6 Privacy controls

7.6.1 Setting privacy controls

- (a) Under the proposed Opt-Out Model, once the System Operator has registered a 'new person' for a PCEHR, the following default access and content control settings will be applied to the individual's PCEHR:
 - (i) there will be no RAC applied to restrict healthcare provider access to the individual's PCEHR; and
 - (ii) the Medicare repository information setting will request the inclusion of all MBS, DVA, PBS, RPBS, ACIR and AODR records into the individual's PCEHR as such records are created.
- (b) This is consistent with the current Newborn Child Declaration registration process which, unlike the other registration channels, does not allow the authorised representative to specify their preferences in relation to the upload of MBS, DVA, PBS, RPBS, AODR and ACIR information about the newborn.

7.6.2 No transition period to set privacy controls

- (a) Unlike the automatic registration of individuals who do not opt-out during the Opt-Out Period (i.e. the Automatic Registrants), there will be no 'transition period' during which access to the new person's PCEHR will be suspended and the authorised representative can set their preferred access and content control settings.
- (b) We have considered the possibility of allowing a 'transition period' for new persons (or their parents/guardians or authorised representatives) to adjust their privacy controls, but rejected that idea because new persons (i.e. individuals registering for Medicare (or an IHI) for the first time):
 - (i) will not have any historical Medicare data (which might otherwise raise particular privacy concerns); and
 - (ii) have had to proactively apply for Medicare (or an IHI), at which point they are filling in a form with the opt-out choice, so the risk faced by Automatic Registrants in relation to never having received the opt-out communications does not apply.

Chapter 8 Content and access to records

8.1 PCEHR content

8.1.1 Medicare data flow

- (a) When either an individual or a healthcare provider accesses the individual's PCEHR for the first time, this will set off a 'trigger' to upload two years of retrospective MBS, DVA, PBS, RPBS, ACIR and AODR data.⁶⁵
- (b) Although the flow of Medicare-related data into an individual's PCEHR is an existing process, this currently occurs on a consent-basis.
- (c) The move to an Opt-Out Model means that unless an individual accesses their PCEHR and adjusts their privacy control settings, the default position is that retrospective Medicare data will begin to populate the individual's PCEHR when a healthcare provider views or uploads documents to the PCEHR for the first time. We note that:
 - (i) It is proposed that the inclusion of MBS, DVA, PBS, RPBS, ACIR and AODR data in all newly created PCEHRs will be given legislative authority.
 - (ii) Individuals will be able to exercise their privacy rights by:
 - (A) opting out before the PCEHR is created;
 - (B) cancelling their PCEHR registration;
 - (C) setting privacy controls to restrict access by healthcare providers to Medicare-related data;
 - (D) opting out of the automatic Medicare data flow during the Transition Period (or at any time afterwards); and
 - (E) monitoring activity in relation to the PCEHR using the audit log or, if they choose to receive notifications, via messages alerting them that someone has viewed or used their PCEHR.
 - (iii) Similar to current arrangements, the Chief Executive Medicare will be able to exercise a discretion and not upload Medicare data. For example, in relation to individuals between the ages of 14 and 18 who have not taken control of their PCEHR, MBS and PBS details will not be accessible through their PCEHR, in line with existing Medicare policy to keep this information private from parents or others without the express consent of the young person. This is a privacy positive feature.
- (d) As discussed in section 6.4.2 of this report, although an individual can limit exposure of their data to third parties by adjusting their privacy control settings, the risk is that the individual does not understand how to set privacy controls, or the implications of not setting privacy controls (i.e. who will be able to see their Medicare data and other information). In this regard, clear and extensive communications will be important to assist individuals to understand and set their privacy controls, and what else they can do to manage their privacy concerns.

⁶⁵ In the case of the healthcare provider, the type of 'access' could be either a user viewing the PCEHR, or a system uploading a clinical document to it, such as a hospital discharge summary.

- (e) Suggested topics that should be addressed in communications with individuals are set out in paragraph 6.4.2(q). We also refer to **Recommendations 21, 22 and 23**.

8.1.2 Clinical records

- (a) We are instructed that there will be no change to the way healthcare provider individuals can upload clinical information to an individual's PCEHR under the Opt-Out Model, except that the authorisation will be provided for by legislation rather than the individual's standing consent.

8.1.3 Conclusions in relation to clinical content

- (a) The potential scope of content of a PCEHR will not change with the shift to an Opt-Out Model. However individuals may not expect that historical Medicare-provided data will be used to pre-populate their PCEHR if they do not opt-out or adjust their privacy control settings to prevent it.
- (b) The privacy risks are therefore primarily related to whether or not individuals understand what content will be included under the default privacy control settings, and how they can adjust those settings to suit their preferences (see the discussion at section 6.4 above); and whether or not individuals are able to easily access their PCEHR in order to adjust those settings (see further below).

8.2 Individual access to PCEHR

8.2.1 Access

- (a) An individual will be able to access their PCEHR (including setting privacy controls during and after the Transition Period) through myGov.
- (b) APP 12 requires the System Operator, as the entity which holds personal information about an individual, to give the individual access to that information on request.
- (c) The APP Guidelines⁶⁶ note that, in order to avoid the risk of unauthorised disclosure to a third party, the identity of the person seeking access to 'their' personal information must be verified in some way. The precise steps required will depend on the circumstances, including *'whether the individual is already known to or readily identifiable by the APP entity, the sensitivity of the personal information and the possible adverse consequences for the individual of unauthorised disclosure'*.
- (d) There is a balance to be achieved between making the identity verification process flexible enough to not frustrate individuals, but also robust enough to achieve its objective, and avoid the risk of unlawfully disclosing personal information to a third party.
- (e) In the current Opt-In Model, individuals who want to register online for a PCEHR will be taken to the myGov website to login to their myGov account (or create a myGov account if they do not have one). The individual then completes the PCEHR registration steps and once successful, their PCEHR will automatically link to the myGov account through which the registration occurred. Individuals can subsequently change the myGov account to which a PCEHR is linked. Subsequent access to the individual's PCEHR is through the myGov login.
- (f) Individuals who register another way, such as through the assisted registration channel, can still only use the online channel to access their record. Online access is the only way in which an individual can adjust all their privacy control settings, although we understand

⁶⁶ Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines*, paragraphs 12.15 – 12.17, at <http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/>, accessed 24 April 2015.

that some controls, such as setting a RAC, can in theory be done via telephone or face to face (DHS shopfront) channels.

- (g) The proposed change to an Opt-Out Model means that a PCEHR may exist for the individual before they have established their myGov credential to access it.
- (h) Concerns have been raised with the current online 'proof of record ownership' process, which was described in the PCEHR Review Report as 'clunky and over complicated'.⁶⁷

8.2.2 Privacy risks relating to usability

- (a) There is therefore a risk that, in the absence of improvements in usability of the process by which individuals can access and 'take control' of their PCEHR, many individuals will be frustrated in their attempts to manage their privacy risks.
- (b) In the context of moving the PCEHR to an Opt-Out Model, enabling easier individual access becomes critical because under the current design proposal, privacy control settings can only be controlled once the individual has succeeded in gaining access to their record. If an individual has not opted out, but then faces obstacles in accessing their PCEHR, the default privacy control settings will apply and all their health information will be shared across all treating healthcare providers.
- (c) Unfortunately it is not clear to us whether the reported difficulties for users are caused by overly-rigorous identity verification business rules, confusing website layout or presentation, confusing terminology or explanations about the underlying business rules, myGov system issues, or PCEHR system issues.
- (d) We understand that the Department is separately conducting a review of the 'usability' of the current registration method, as well as the way in which the various privacy control settings including access controls are explained and presented to individuals.
- (e) We suggest that making access to their own PCEHR as easy as possible for individuals – so long as the risk of inadvertent disclosure to the wrong individual is not raised as a result – would be a privacy positive.
- (f) In discussions with the Department, the possibility was raised that some privacy control settings could be adjusted in advance of the PCEHR shell record being created. This could potentially be done through the proposed Online Opt-Out Service, which – because it will not involve any presentation of health information or other personal information back to the individual – can allow a lower standard of identity verification than full access to the record requires.
- (g) While some privacy control settings cannot be adjusted in advance of a shell record's creation (such as settings related to a specific clinical document), others could be set in advance, such as:
 - (i) choices about which notifications to receive (e.g. when the 'emergency' override has been applied, when the record is first accessed by a healthcare provider, or every time the record is accessed by a healthcare provider);
 - (ii) choice about how to receive notifications (e.g. nominate an email address, or a mobile number for SMS messages);
 - (iii) choices about content to be included from Medicare (PBS etc.) and how much of it (none / from now on / two years history plus from now on); and
 - (iv) setting a RAC.

⁶⁷ PCEHR Review Report p.55.

- (h) We support such a concept, which would deliver a strong ‘privacy positive’ improvement over the existing system.
- (i) We have made various recommendations below to enable an improved individual access experience, which will assist the Department ensure its compliance with APP 12. We suggest that improving the accessibility of the PCEHR and thus the individual’s ability to adjust privacy control settings will also, in turn, assist the Department to meet its requirements in relation to Data Security, detailed below.

Recommendation 29

That the Online Opt-Out Service design include the ability for the individual to consider and adjust privacy control settings in relation to notifications, Medicare-provided content and setting a RAC, in advance of the creation of their shell record.

Recommendation 30

If **Recommendation 29** is accepted, that the Online Opt-Out Service design also include the ability for the individual to supply an email address, so that the System Operator can send the individual a message once the record is ‘live’, with a reminder about how to log in to myGov to access their record or further adjust their privacy control settings. (See also **Recommendation 8**.)

Recommendation 31

That the Department continue work to improve the accessibility and usability of online access and controls for individuals, while ensuring that any changes to identity verification to improve usability do not increase the risk of inadvertent disclosure to a third party.

- (j) The PCEHR Review Report noted a practical difficulty with the process by which individuals sign up for a myGov account:

*Multiple users with the same email address cannot register for a mygov.au account preventing them from accessing their record.*⁶⁸
- (k) The design of the myGov registration process assumes that the individual has a unique email address. This is not necessarily true of all people, in particular family members who may have a shared email account. Some individuals will not have any email address, but may still wish to establish online access to their PCEHR.
- (l) Individuals who do not have a unique email address therefore face a barrier to accessing their PCEHR and adjusting their privacy control settings. This will exacerbate any privacy risks those individuals face in relation to the sharing of their health information.
- (m) We suggest that a more sustainable and scalable solution is required of the myGov registration business rules. We also refer to **Recommendation 29**, which suggests allowing some privacy control settings to be adjusted via the Online Opt-Out Service.

Recommendation 32

That the Department give further consideration in the future to having a standalone PCEHR individual access portal separate to myGov.

⁶⁸ PCEHR Review Report, p.57.

Recommendation 33

That prior to the implementation of the Opt-Out Model, the Department consult with DHS as the myGov operator to provide a registration solution scalable to almost 24 million individuals, which does not operate on the assumption that the individual can supply a unique email address.

8.2.3 Other privacy risks

- (a) There is a related risk in the use of myGov as the only channel through which individuals can access their PCEHR and adjust all their privacy control settings.
- (b) As discussed above, the use of myGov may pose barriers for some individuals, which may in turn increase the risk of inappropriate sharing of health information faced by those individuals.
- (c) However there is also the potential for public concern to be raised about any proposal to push the vast majority of the populace into using only one channel to access their PCEHR. This could be interpreted (whether accurately or not) as a strategy to push millions of Australians into having a new, government-issued unique identifier: a myGov username.
- (d) Regardless of the accuracy of the claim, some members of the public could be concerned about the extent to which greater uptake of the myGov system could lead to centralised government communications, data linkage between client agencies, and the like. For the PCEHR system, there is therefore a risk that the political discussion of the opt-out proposal becomes side-tracked by debate and privacy concerns (whether valid or not) about the myGov channel.
- (e) We suggest that the establishment of an alternative, stand-alone individual access portal for the PCEHR would eliminate these concerns, as well as addressing the compliance risks identified elsewhere in this report in relation to the Data Security and Access privacy principles. **Recommendation 32** above therefore addresses this risk.

8.3 Data quality

- (a) Poor data quality from source data can lead to errors within the PCEHR system, including clinical information being attributed to the wrong person, or incorrect clinical information being attributed to the correct person. This can in turn lead to errors in clinical decision-making, with negative health outcomes for the individual, and/or privacy breaches which lead to harms to the individual such as discrimination or embarrassment.
- (b) APP 10 requires the System Operator to 'take such steps (if any) as are reasonable in the circumstances' to ensure that the personal information collected, used and disclosed by the system is accurate, up-to-date and complete, and relevant for the purpose of its use or disclosure.
- (c) The Privacy Commissioner has advised that 'more rigorous steps may be required' if the information is 'sensitive information' such as health information, and/or if there are 'possible adverse consequences for an individual if the quality of personal information is not ensured'.⁶⁹ We suggest that each of these criteria are reflected in the PCEHR system.

⁶⁹ Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines*, paragraph 10.6, at <http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/>, accessed 24 April 2015.

- (d) The APP Guidelines note that taking reasonable steps to only handle 'high quality' personal information will build 'community trust and confidence'.⁷⁰ The reverse is equally true: a loss of faith in the accuracy of data could dramatically impact on public trust in, and the reputation of, the PCEHR system. This in turn could affect participation rates by individuals and clinicians, both of which are required for the system as a whole to deliver value.
- (e) Some stakeholders have raised concerns about the quality and utility of data from the various source systems upon which the PCEHR system relies, including the HI Service and Medicare's feeds of data about PBS, RPBS, MBS, DVA, ACIR and AODR records.
- (f) A submission to the PCEHR Review from e-health IT consultant and influential blogger Dr David More stated:

*We have seen many errors in the data uploaded to the PCEHR already from Medicare Australia data sources - which includes some in my PCEHR record. Data quality in health information is presently not ideal in many health systems and needs to be improved before much use is made of the information for management and research.*⁷¹

- (g) A report on PCEHR progress prepared on behalf of the Consumers e-Health Alliance also raises concerns about data quality, in relation to the ability of the HI Service to safely and accurately identify individuals, based on sources including the HI Service's own annual report.⁷²
- (h) A submission to the PCEHR Review from Western Sydney Medicare Local also raised the issue of accuracy of data from clinical systems:

*Many GP records need curation (cleansing) prior to uploading to the PCEHR – this curating records probably takes biggest time component in sending a SHS to the PCEHR. The question is how to get GPs to go through their records and bring them all up to the same level.*⁷³

- (i) While these are all existing risks in relation to the PCEHR system, the repercussions will manifoldly increase with the introduction of an Opt-Out Model, when the system will be dealing with almost 24 million (mostly passive) individuals, rather than the 2 million individuals now.
- (j) It is beyond the scope of this PIA to assess the quality and integrity of the various sources of data to be utilised by the PCEHR system. However we have recommended ways in which data quality risks should be assessed and then managed prior to implementation of the Opt-Out Model.
- (k) Although managing data quality risks should not be left to individuals themselves, enabling individuals' access to their PCEHR nonetheless provides an important point at which data accuracy can be checked, and then any errors appropriately notified and remedied.⁷⁴ **Recommendations 29, 30, 31 and 32** in this report, which suggest ways in

⁷⁰ Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines*, paragraph 10.3, at <http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/>, accessed 24 April 2015.

⁷¹ PCEHR Enquiry Submission from Dr David G More, November 2013.

⁷² See Karen Dearne, "An analysis of Commonwealth Government annual reports covering e-health and PCEHR activities in 2013-14: A Review of Progress", prepared for the Consumers e-Health Alliance, December 2014.

⁷³ Western Sydney Medicare Local, *Submission to the PCEHR Review*, 21 November, 2013, p.5.

⁷⁴ For example, if an individual requests a healthcare provider organisation to correct personal information contained in their PCEHR and is not satisfied with the outcome, the individual could raise the issue with the System Operator. Under section 73B of the PCEHR Act, the System Operator could request the healthcare

which to improve individuals' ability to access their PCEHR, will therefore also assist with compliance with the Data Quality principle.

Recommendation 34

That the Department include links on any 'Opt-Out' websites relating to the transition to an Opt-Out Model to existing clinical safety audits, as well as reports outlining the steps taken by the Department to address any recommendations arising from those audits, prior to implementing the Opt-Out Model.

Recommendation 35

That the Department commission and publish an updated review of the data quality risks posed by the use of IHIs and Medicare provided data, in the context of almost 24 million individuals, and implement any remediating strategies, prior to implementing the Opt-Out Model.

Recommendation 36

That the Department conduct a pilot of the Opt-Out Model, including the automatic registration of individuals, the creation of shell records, and testing the accuracy of automated data flows from Medicare, to ensure any data accuracy issues are identified and addressed, prior to implementing the Opt-Out Model.

8.4 Data security

8.4.1 Introduction

- (a) APP 11 requires entities which hold personal information to 'take such steps as are reasonable in the circumstances to protect the information ... from misuse, interference and loss; and ... from unauthorised access, modification or disclosure'.
- (b) The likelihood and level of security risk to PCEHR system data security will increase under an Opt-Out Model due to the large number of individuals, as well as the richness of the volume of information. In particular, the registration of almost all Australians will increase the 'honeypot' value of the PCEHR system.
- (c) Some of the likely risk scenarios we consider will arise under an Opt-Out Model are discussed below.

8.4.2 Unauthorised users

- (a) The first scenario involves one person impersonating another in order to gain access to someone's PCEHR. The motivation in this case might be to create a nuisance for, or to gain leverage in a dispute with, a family member or ex-partner; or to gain valuable information on a stranger such as a public figure.
- (b) The question is whether or not the proposed identity verification requirements for an individual to access 'their' PCEHR will be sufficient to mitigate against this risk from an imposter, without unduly creating barriers for the genuine individual.
- (c) The second scenario involves organised criminals and other types of external hackers, circumventing controls in order to access multiple individuals' records.

provider organisation to correct the record and, if they refuse to do so, direct the healthcare provider organisation to attach a note prepared by the individual to the individual's record.

- (d) These are both existing risks for the PCEHR under the Opt-In Model. However, for the reasons set out above, we suggest that the likelihood of these risks occurring will increase under an Opt-Out Model.
- (e) There has already been criticism of the myGov website, with media articles pointing out flaws in its information security which 'hackers could have potentially leveraged to hijack myGov accounts', including accessing PCEHR records linked to myGov accounts.⁷⁵
- (f) As with data quality, a loss of faith in the security of personal information in PCEHRs could dramatically impact on public trust in, and the reputation of, the PCEHR system. This in turn could affect participation rates by individuals and clinicians, both of which are required for the system as a whole to deliver value. It is therefore critical for the Department to ensure that the PCEHR system is held to the highest possible standards for information security.
- (g) It is out of scope for this PIA to review the adequacy of either existing or proposed information security controls, including the proposed identity verification requirements for individual access. However we suggest that a comprehensive review be undertaken.
- (h) In relation to this risk, we also refer to **Recommendation 32** which suggests establishing a standalone individual access portal for the PCEHR system.

Recommendation 37

That the Department commission an information security Threat & Risk Assessment in relation to the PCEHR system, including the security of the myGov individual access channel, and the adequacy of the identity verification process for individuals to access their PCEHR, prior to implementing the Opt-Out Model.

8.4.3 Inappropriate access to PCEHR by healthcare provider or other authorised user

- (a) People with legitimate access to a database can sometimes feel tempted to look up the records of people they know personally, or public figures. They might be motivated by curiosity, or by a plan to use any personal information they find out for some personal benefit – such as for leverage in a dispute with that person, or by selling the information to an interested third party.
- (b) Current privacy controls on the PCEHR system mean that unless the individual is already a patient of that healthcare provider organisation, an authorised user is unlikely to be able to find out all the details about a stranger (such as a celebrity or other public figure) they would need in order to gain access to their PCEHR.
- (c) However authorised users may already know enough details about family members, friends or acquaintances to enable access to their PCEHR.
- (d) This is an existing risk with the PCEHR system, managed in a variety of ways. However this risk will be multiplied with the switch to an Opt-Out Model as close to 24 million individuals may be expected to have PCEHRs.
- (e) The following existing privacy controls on authorised users are expected to continue under an Opt-Out Model:
 - (i) in order to access an individual's PCEHR, a healthcare provider or other authorised user first needs to know (or be able to find out) the individual's IHI; or

⁷⁵ See Ben Grubb, "[Revealed: serious flaws in myGov site exposed millions of Australians' private information](http://www.smh.com.au/it-pro/security-it/revealed-serious-flaws-in-mygov-site-exposed-millions-of-australians-private-information-20140515-zrczw.html)", 15 May 2014, at <http://www.smh.com.au/it-pro/security-it/revealed-serious-flaws-in-mygov-site-exposed-millions-of-australians-private-information-20140515-zrczw.html>, accessed 12 December 2014.

a set of details such as their family name, given name, date of birth, sex, and either their Medicare number *or* Medicare-recorded address;

- (ii) the individual's home address is not exposed in the PCEHR itself, although it may be included in the contents of clinical documents;
 - (iii) there is an audit log, visible to the individual themselves, of all instances of access to their record by authorised users;
 - (iv) the individual can utilise a range of privacy control settings to control what content can populate their PCEHR, who can access that content, and whether the individual wants to receive notifications when certain things happen; and
 - (v) there is a program to monitor access to individuals' records, including heightened monitoring of access to people of particular interest, and unusual patterns of access by authorised users.
- (f) We do not suggest that any further privacy controls could be built into the PCEHR system, in terms of preventing inappropriate access to PCEHRs by healthcare providers, without affecting legitimate access by healthcare providers.

8.4.4 Evidence of identity

- (a) Some individuals who wish to use the online or phone channels to opt-out themselves or a dependant may not have a primary EOI document, while others may have their primary EOI document legitimately issued in a different name to their Medicare card. In particular, women may commonly have a maiden surname for one document and a married surname for another. When scaled up to almost 24 million individuals, this identity verification model may pose a barrier for hundreds of thousands of individuals.
- (b) The proposed solution where an individual, who wishes to opt-out but who cannot provide a primary EOI document in the same name as their Medicare card is to require the individual to attend a Medicare shopfront. This may pose a barrier for some individuals, as well as potential cost implications for DHS (e.g. increased staff resourcing requirements).
- (c) However, there is a balance to be achieved between making the identity verification process flexible enough not to frustrate individuals, but also robust enough to achieve its objective while minimising privacy impacts.
- (d) We note that the current mechanism by which individuals register online for a PCEHR does not involve the use of a primary EOI document. Instead, the individual is asked to provide various identity details as per their Medicare records (first name, surname, date of birth and address, and Medicare card number), as well as additional details from their Medicare history, which effectively act as 'shared secrets': information such as the surname or postcode of the last GP seen for which a Medicare rebate was claimed, the date of that visit, or the bank account used for receiving rebates.
- (e) Further, the proposed method by which individuals in the Opt-Out Model will be able to verify their identity in order to access their PCEHR online also involves the same combination of Medicare-only information.
- (f) It is the combination of details which are available on the face of the Medicare card, with other information that would be very difficult for an unauthorised third party to know about the individual, which provides a level of assurance about the individual's identity that the Department has accepted as sufficient to allow an individual to register for or access 'their' PCEHR, and thus see the clinical information stored within.

- (g) The identity verification test currently used for registration therefore offers a model for online identity verification of individuals for whom a primary EOI document, in the precise same name as their Medicare account, is not available. We therefore suggest that this should be offered as an alternative for those individuals who would otherwise face a barrier to accessing the Online Opt-Out Service.

Recommendation 38

As part of the design development in relation to the online and telephone channels, the Department should consider alternative pathways for an individual to verify their identity where they do not have a primary EOI document at all, or only have an EOI document in a different name to their Medicare card. For example, the Online Opt-Out Service and telephone channel could be designed to also allow the Medicare-information only method of verifying the individual's identity.

Recommendation 39

That the Department provide or fund specialist assistance to help vulnerable and disadvantaged individuals (such as individuals from a non-English speaking background, the illiterate, homeless, and adults with limited or no capacity) to access one of the channels to exercise their opt-out choice.

8.4.5 Access by other third parties

- (a) Once almost 24 million individuals have a PCEHR, the System Operator will be holding a very large and content-rich dataset, which may be of interest to non-malicious third parties such as insurers, courts, law enforcement agencies, freedom of information applicants, employers and researchers. Stakeholder consultations in relation to this proposal also elicited some concerns about third party access, by or on behalf of insurers and employers in particular:

There was significant discussion in the consultation session about the potential for a consumer's record to be accessed by organisations not directly involved in the delivery of care, or persons other than the relevant clinician within the provider organisation. Many consumers were particularly concerned about the potential for organisations such as their employer or their private health insurance provider being able to access their record and use the information in the record to the detriment of the consumer. While it was acknowledged that the PCEHR legislation restricts access to only registered care providers, consumers were concerned about the potential for these types of organisations access to their information via intermediaries such as medical assessor utilised by their employer or health insurer to conduct a health assessment of the consumer.⁷⁶

- (b) The existing legislative framework limits the ability for third party access to PCEHRs in a number of ways, including the following:
- (i) **Restrictions on disclosure to courts and tribunals:** Section 69 of the PCEHR Act provides that participants in the PCEHR system and individuals cannot be required to disclose health information included in an individual's PCEHR to a court or tribunal except for disclosure by the System Operator:

⁷⁶ Draft Deloitte report p.13.

- (A) to a court or tribunal in proceedings relating to the PCEHR Act, unauthorised access to information through the PCEHR system or the provision of indemnity cover to a healthcare provider; or
 - (B) to a coroner.
- (ii) **Prohibitions in relation to collection, use and disclosure:** Civil penalties apply to unauthorised collection, use and disclosure of health information included in a consumer's PCEHR from the PCEHR system (section 59 of the PCEHR Act). Authorisations are limited.

Insurance companies

- (c) There are some risk scenarios where an insurance company could indirectly obtain access to information held in an individual's PCEHR.
- (d) The first scenario is where an individual has commenced proceedings against a healthcare provider for negligence. The exception in section 69 of the PCEHR Act for disclosure in proceedings relating to the provision of indemnity cover to a healthcare provider could result in PCEHR information being disclosed in proceedings (including PCEHR information not previously available to the healthcare provider). Further, there is an authorisation permitting participants in the PCEHR system to collect, use and disclose PCEHR information for purposes relating to the provision of indemnity cover for a healthcare provider (section 68 of the PCEHR Act). This authorisation is not expressly subject to compliance with access controls (although they may apply in practice).
- (e) There is also the potential for information to be obtained from the PCEHR system as authorised, but then further disclosed for other purposes. For example:
 - (i) participants in the PCEHR system may collect, use and disclose PCEHR information with the individual's consent (section 66 of the PCEHR Act); and
 - (ii) participants in the PCEHR system may collect, use and disclose PCEHR information for the purposes of providing healthcare to the registered individual (in accordance with access controls) (section 61 of the PCEHR Act). For example, this could include a registered healthcare provider organisation assessing an individual's health for an employer or an insurer.
- (f) The effect of section 71(4) of the PCEHR Act is that information may be obtained from the PCEHR system, stored elsewhere and then collected, used and disclosed from that other source without restriction under the PCEHR Act. However, the collection, use and disclosure of the information will continue to be subject to other existing laws of the Commonwealth, states or territories, including the Privacy Act and health records legislation. It will also continue to be subject to any professional obligations that apply – e.g. to treating healthcare providers.
- (g) There is also the potential for other laws to authorise collection, use and disclosure of PCEHR information by participants in the PCEHR system (section 65 of the PCEHR Act).
- (h) The drafting instructions propose that the definition of 'healthcare' is amended so that it does not include activities performed for reasons other than care or treatment of an individual, and in particular does not include certain activities connected with insurance covering the individual. This change would limit the ability of participants in the PCEHR system to collect, use and disclose PCEHR information for the purposes of healthcare in reliance on section 61. However, it would not affect the potential for PCEHR information obtained for an authorised purpose being used and disclosed for other purposes.

- (i) Another risk scenario that arises is where an individual has made a claim for an injury and is referred to a healthcare provider for a medical assessment. Unless the individual has set their privacy controls to restrict third party access, it is possible that a medical assessor could access information contained in the individual's PCEHR that they do not want disclosed. Consequently this could result in privacy complaints. Therefore ensuring that the communication strategy with individuals provides clear information about setting privacy controls – including the implications of not setting privacy controls in this type of scenario – will be important to mitigate this risk. We refer to our discussion in section 6.4 and **Recommendations 21, 22 and 23**.

Research

- (j) Section 15(ma) of the PCEHR Act authorises the System Operator to *'prepare and provide de-identified data for research or public health purposes'*.
- (k) We understand that as yet, no research requests have been received by the Department. However this situation can be expected to change with a shift to an Opt-Out Model. A protocol for managing and responding to research requests has not yet been developed.
- (l) In relation to de-identification, the APP Guidelines state:

*De-identification may not altogether remove the risk that an individual can be re-identified. There may, for example, be a possibility that another dataset or other information could be matched with the de-identified information.*⁷⁷
- (m) The Victorian Privacy Commissioner has advised agencies in Victoria to be mindful of the ease with which data from different sources can be matched – in particular, using public sources of information such as online search engines, public registers, and telephone directories – when assessing whether or not a person's identity may be ascertainable from the information, when matched against other sources.⁷⁸
- (n) The NSW Privacy Commissioner has likewise warned that privacy risks may arise *'in the publication of non-identifying statistical data, which may nevertheless be aggregated with other data to effectively re-identify some individuals'*.⁷⁹
- (o) The re-identification risks posed by ready access to large datasets has been evidenced a number of times. For example:
 - (i) A 2000 study by a PhD student at Carnegie Mellon University obtained publicly available health insurance information on Massachusetts state workers that was stripped of names, addresses, social security numbers and other 'identifying' information. The student then purchased state voter rolls for the city of Cambridge, including the name, ZIP code, address, sex and birth date of every registrant. The insurance data showed that there were six people in Cambridge born on the same day as the governor: half were men. The voter data allowed the student to pinpoint the state's governor as the only one of those residing in a particular ZIP code in Cambridge. The corresponding health-insurance data included the governor's medical diagnoses and prescriptions.⁸⁰

⁷⁷ Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines*, paragraph B.61, at <http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/>, accessed 24 April 2015.

⁷⁸ Privacy Victoria, *Guidelines to Victoria's Information Privacy Principles*, Edition 02, September 2006, p.11.

⁷⁹ Privacy NSW, *Privacy Contact Officer Newsletter*, June 2002.

⁸⁰ See ['Computational Disclosure Control: A Primer on Data Privacy Protection'](http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/sweeney-thesis-draft.pdf) available at <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/sweeney-thesis-draft.pdf>

- (ii) In 2006, search engine provider AOL released 'anonymous' web search records for 658,000 users. *New York Times* journalists linked search terms to identify users and contact them.⁸¹
- (iii) In 2014, an 'anonymised' dataset of 173 million taxi trips taken during 2013 in New York City was re-identified within only two hours to the individual driver, using other publicly available data.⁸² Identification of passengers took a little longer, but was also possible.⁸³
- (p) Coded information, such as names converted by an algorithm into a Statistical Linkage Key, will remain potentially re-identifiable to the person or body with the means to link the code back to other identifying details. Coded information may therefore still be 'personal information' protected by the PCEHR Act and Privacy Act.
- (q) The UK Information Commissioner's Office recommends techniques such as:
 - (i) removing variables (e.g. drop ethnicity);
 - (ii) recoding (e.g. change DOB to age bands such as '35-44 yr old');
 - (iii) suppression (replace value with 'missing' or 'null');
 - (iv) micro-aggregation (e.g. group in fours, so ages 31, 33, 33 and 34 each become 32.75);
 - (v) data-swapping (e.g. swap salaries for two people within the same postcode, so the aggregate not affected); and
 - (vi) adding 'noise'.⁸⁴
- (r) The Australian Privacy Commissioner suggests similar techniques, and recommends choosing the best technique, following a risk assessment, 'to ensure that personal information is protected and that a de-identified information asset will still be useful for its intended purpose'.⁸⁵
- (s) With a near total population database, and advances in computing power and 'big data' analytics, re-identification of de-identified data is becoming easier. Therefore the release of 'de-identified' datasets is posing higher levels of privacy risk.
- (t) We suggest that the Australian Privacy Commissioner's Guidelines, and the UK Anonymisation Code of Practice, offer useful resources for the Department when contemplating how to exercise its functions under section 15(ma) of the PCEHR Act.

⁸¹ "Forget Facebook privacy, your digital life is being monitored", Aditya Chakraborty, 26 May 2010, SMH – available at <http://www.smh.com.au/opinion/society-and-culture/forget-facebook-privacy-your-digital-life-is-being-monitored-20100525-wavc.html#poll>

⁸² See 'On Taxis and Rainbows: Lessons from NYC's improperly anonymized taxi logs' available at <https://medium.com/@vijayp/of-taxis-and-rainbows-f6bc289679a1>

⁸³ For an explanation of how differential privacy ('adding noise') would have resolved the NYC taxi trip dataset problems, see <http://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/>

⁸⁴ Information Commissioner's Office (UK), *Anonymisation Code of Practice*, 2012, available at http://ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation, accessed 16 December 2014. Also, for an explanation of how differential privacy ('adding noise') would have resolved the NYC taxi trip dataset problems, see <http://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/>, accessed 16 December 2014.

⁸⁵ Office of the Australian Information Commissioner, "Privacy business resource 4: De-identification of data and information", available at <http://www.oaic.gov.au/privacy/privacy-resources/privacy-business-resources/privacy-business-resource-4-de-identification-of-data-and-information>, accessed 16 December 2014.

Recommendation 40

That the Department develop a De-identification Protocol, in consultation with the Australian Privacy Commissioner and taking into account the risk of re-identification from de-identified datasets, prior to implementation of the Opt-Out Model.

8.5 Privacy complaints, penalties and redress for harm

8.5.1 Overview

- (a) The move to an Opt-Out Model will likely lead to a material increase in privacy complaints about the PCEHR system, as the number of individuals affected grows from 2 million to more than 23 million – and more over time.
- (b) The most challenging type of complaint will be the allegation that *'I never even knew I had a PCEHR, and now X scenario has happened, and I have suffered Y harm as a result'*.
- (c) We have made recommendations about the need to ensure that every effort is made to communicate directly with all Medicare card holders about the shift to an Opt-Out Model to reduce this risk.
- (d) Nonetheless, we suspect that many individuals will slip through the communications cracks, and they may not discover for years that they even have a PCEHR that is accessible to potentially thousands of healthcare providers. Some of those individuals will suffer harm as a result of the sharing of their health information without their knowledge. This residual risk will need to be accepted, and managed accordingly, by the Department.
- (e) Ensuring there are criminal penalties set at an appropriate level to discourage misuse by individuals will be one important component of effective governance of the PCEHR system. Another will be civil penalties to encourage healthcare provider organisations, and other participants in the PCEHR system, to take seriously their privacy responsibilities, including obligations to maintain the security and integrity of data.
- (f) A robust complaints-handling process will be important, including the ability to provide compensation to affected individuals without the individual needing to escalate their complaint to the Privacy Commissioner. The Privacy Commissioner will need to be adequately resourced to handle such complaints.
- (g) Nonetheless, it is likely that gaps in the criminal and civil enforcement models will remain. The Australian Law Reform Commission has recently identified some of those gaps, and recommended enactment of a statutory cause of action for serious invasions of privacy. We suggest that a similar model could be adopted and applied to the PCEHR system, as a final safety net to compensate any individual who suffers harm due to an intentional or reckless invasion of privacy in relation to their PCEHR. (See our discussion in section 8.5.9.)

8.5.2 Types of privacy harms

- (a) The following framework can be used for considering privacy harms:⁸⁶
 - (i) **Tangible damage:** This type of harm is normally physical or economic. It includes bodily harm, loss of liberty or freedom of movement, damage to earning power and other significant damage to economic interests (e.g. arising from identity theft).

⁸⁶ [Centre for Information Policy Leadership](http://www.informationpolicycentre.com/), Hunton & Williams LLP, *Risk-based Approach to Privacy: Improving Effectiveness in Practice*, 2014, available at <http://www.informationpolicycentre.com/>, accessed 23 April 2015

- (ii) **Intangible distress:** This type of harm includes: detriment arising from monitoring or exposure of identity, characteristics, activity, associations or opinions; chilling effect on freedom of speech, association, etc.; reputational harm; personal, family, workplace or social fear, embarrassment, apprehension or anxiety; unacceptable intrusion into private life; and discrimination or stigmatisation.
 - (iii) **Societal harm:** This type of harm can arise from business activity or where personal information is used by governmental bodies. It includes damage to democratic institutions and loss of social trust.
- (b) Within this framework, there is the potential for (at least) the following types of harm as a result of invasion of privacy in relation to an individual's PCEHR:
- (i) Tangible damage (primarily in relation to the individual):
 - (A) identity theft;
 - (B) financial loss (although no financial details are stored in the PCEHR system, financial loss could arise indirectly, e.g. in an employment or insurance context); and
 - (C) threat to physical safety (e.g. release of address details);
 - (ii) Intangible distress (primarily in relation to the individual):
 - (A) humiliation, damage to reputation or relationships; and
 - (B) discrimination; and
 - (iii) Societal:
 - (A) reputational damage in relation to the System Operator and government; and
 - (B) loss of confidence in the PCEHR System, leading to decreased participation by individuals (so that the health and other benefits of the PCEHR System are not achieved).
 - (iv) An invasion of privacy may be considered to give rise to societal harm, such as loss of confidence, even where there is no tangible damage or intangible distress to an individual.
- (c) The risks giving rise to potential privacy harms we suggest should be subject to clear, uniform and enforceable obligations – including enforceable remedies for a victim who suffers tangible or intangible harm – include:
- (i) an authorised user searching for or viewing a PCEHR when they do not have a legitimate reason for doing so (e.g. 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 their viewing it is for a purpose that is not legitimate (e.g. the individual is in the care of a colleague, but the user is not actually involved in treating the individual, and the user is looking at their colleague's computer);
 - (iii) an authorised user viewing a PCEHR legitimately, but then misusing or disclosing the individual's data in some unauthorised way (e.g. the individual is in the user's care, but the user discloses clinical information about the individual to the media,

or uses the individual's home address from a clinical document to pursue a personal dispute);

- (iv) poor data quality practices (e.g. 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 (e.g. a healthcare provider being negligent in the way they allow their staff to share log-ins, or a DHS shop-front having a computer screen viewable in a public waiting area).

8.5.3 Criminal penalties

- (a) The PCEHR Act does not contain any criminal offence provisions.
- (b) A criminal offence provision would have the following advantages:
 - (i) Assigning criminal sanctions would emphasise to individuals considering whether or how to participate in the PCEHR system how seriously privacy protection is taken in relation to the PCEHR system.
 - (ii) Criminal sanctions would emphasise the importance of privacy obligations to healthcare providers and other users of the PCEHR system, acting as a deterrent against deliberate misuse.
 - (iii) Criminal sanctions could cover those scenarios where no other avenue is available. For example, where existing provisions do not cover all scenarios which could involve unauthorised viewing, collection, use and/or disclosure of information in an individual's PCEHR (see for example the issues raised in paragraphs 8.5.4(c) and 8.5.5(a) below). Further, a criminal offence could provide an effective sanction against an employee where the organisation cannot be held accountable (e.g. an organisation can seek to avoid responsibility for a breach of a civil penalty or other privacy breach by arguing that it occurred due to a rogue employee operating contrary to the organisation's policies).
 - (iv) Availability of criminal sanctions in addition to civil penalties allows for a more graduated range of enforcement options.
- (c) There are criminal offence provisions in the HI Act. For example, section 26 of the HI Act is a criminal offence provision in relation to the unauthorised use or disclosure of healthcare identifiers, carrying a maximum penalty of two years' imprisonment. 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.
- (d) However we suggest that not all potential privacy harms involving a PCEHR would necessarily involve misuse of the individual's IHI. Relying on the HI Act alone would cover the first scenario listed above (at paragraph 8.5.2(c)(i)), because to get to that point the authorised user would first have to obtain and then misuse the individual's IHI. However we believe the misuse provisions of the HI Act would not cover the other four scenarios outlined above (at paragraphs 8.5.2(c)(ii)-8.5.2(c)(v)).
- (e) There are also criminal offence provisions found in other general criminal statutes, such as 'accessing restricted data', which is an offence under section 478.1 of the *Criminal Code* (Cth) and section 308H of the *Crimes Act 1900* (NSW) with a maximum penalty of two years' imprisonment. We have not assessed whether every State and Territory has an equivalent offence provision.

- (f) There are also criminal offence provisions found in some privacy laws, such as sections 68 and 69 of the *Health Records & Information Privacy Act 2002* (NSW), which likewise sets a maximum penalty of two years' imprisonment, and which includes an offence of soliciting an unlawful disclosure. However these offences would only apply to some participants in the PCEHR system (in this case, only NSW public sector officials).
- (g) The existing civil penalty provisions do not cover all of the above privacy harm risk scenarios, and therefore by themselves do not provide sufficient deterrence against misuse.
- (h) We suggest that a review be conducted to ensure that there is a regime which provides a criminal offence provision, with a penalty of imprisonment (which would presumably not be any less than the penalty under section 26 of the HI Act), that effectively covers all possible participants in the PCEHR system, and which covers all potential criminal misuse or unauthorised disclosure of information in or from an individual's PCEHR, including their health information, personal information and identifying information, and including secondary disclosure or soliciting a misuse or disclosure.

Recommendation 41

That the Department review whether existing criminal offence provisions in other statutes already effectively cover all the scenarios which could involve unauthorised viewing, collection, use and/or disclosure of an individual's PCEHR, or information drawn from their PCEHR, and whether such provisions set sufficiently serious maximum penalties to act as a deterrent. If existing provisions elsewhere are sufficient, we suggest inserting a note in the PCEHR Act, referring to those other provisions. Otherwise, we suggest adding criminal offence provisions to the PCEHR Act, related to the unlawful viewing, collection, use, disclosure, secondary disclosure or soliciting a misuse or disclosure of health information, personal information or identifying information in or from an individual's PCEHR, with a maximum penalty including both penalty units and a two year term of imprisonment.

8.5.4 Civil penalties

- (a) The PCEHR Act sets out a range of circumstances in which 'health information' may be collected, used or disclosed by participants in the PCEHR system: see sections 61 to 70.
- (b) An act of collection, use or disclosure of 'health information' other than as authorised under sections 61 to 70 is unauthorised, and attracts a civil penalty under sections 59 and 60 of the PCEHR Act.
- (c) This civil penalty regime only relates to 'health information'. It does not apply specifically to 'identifying information', which can include an individual's name, date of birth, address and Medicare number,⁸⁷ although to the extent that this information is collected in the course of providing healthcare, such information might also be captured by the definition of 'health information'.⁸⁸ For example, if an individual's home address is included in a clinical document such as a hospital discharge summary, home address may constitute 'health information' protected by these civil penalty provisions. However this will not always be the case for all identifying information. Likewise there will be other personal information included in an individual's PCEHR which is neither 'health information' nor 'identifying information', such as information about their nominated representatives or authorised representative, which is not collected in the context of providing healthcare, but in the context of managing the PCEHR.

⁸⁷ See definition of 'identifying information' in section 9 of the PCEHR Act.

⁸⁸ See definition in section 5 of the PCEHR Act.

- (d) The existing civil offence provisions do not cover other scenarios such as negligent or reckless data security and data quality practices in relation to PCEHRs which could impact on the security or integrity of an individual's information.
- (e) The existing civil offence provisions do not cover all of the above privacy harm risk scenarios (see section 8.5.2), and therefore alone do not provide sufficient deterrence against privacy risks arising.
- (f) The civil penalty is set at 120 penalty units for an individual, which is currently worth \$20,400. Bodies corporate can be subject to a maximum of 5 times the specified penalty (i.e. up to \$102,000).⁸⁹ Civil penalties are payable to the Commonwealth. The existing civil penalty regime therefore does not provide any redress for an affected individual.

8.5.5 Interferences with privacy

- (a) The APPs cover a range of information-handling obligations, including not only collection, use and disclosure, but also data security and data quality. An alleged breach of the APPs is a matter which triggers the Australian Privacy Commissioner's powers to investigate and conciliate complaints under the Privacy Act. However not all participants in the PCEHR system are regulated by the APPs. For example, State government healthcare providers such as public hospitals are not covered by the APPs.
- (b) Separately, a breach of Part 4 or 5 of the PCEHR Act constitutes an 'interference with privacy'.⁹⁰ An 'interference with privacy' is a matter which also triggers the Australian Privacy Commissioner's powers to investigate and conciliate complaints under the Privacy Act.
- (c) In this sense, a 'breach of the PCEHR Act' could be either:
 - (i) unauthorised collection, use or disclosure which would breach sections 59 or 60 of the PCEHR Act, as discussed above in relation to civil penalties (or breach of other sections of the PCEHR Act, such as sections 75 in relation to data breach notification and section 77 in relation to taking records outside Australia); or
 - (ii) conduct which would breach the PCEHR Rules (see section 78 of the PCEHR Act).
- (d) The PCEHR Rules include a requirement on healthcare provider organisations to have a policy regarding data security matters such as physical and information security, staff training, and management of access controls for staff within their organisation.
- (e) However a breach of the PCEHR Rules will only be regarded as an 'interference with privacy', such as to trigger the Privacy Commissioner's powers, if it is by a registered repository operator or registered portal operator. Healthcare provider organisations and individuals are not included in the scope of section 78.
- (f) Data quality obligations are currently governed by the participation agreement (which healthcare provider organisations are required to enter by the *PCEHR (Participation Agreements) Rules 2012*). A breach of the participation agreement alone would not currently amount to a breach of the PCEHR Act, and so would not become an interference with privacy on this basis (although it may separately amount to an interference with privacy under the general Privacy Act provisions, for those healthcare providers regulated as 'entities' under the Privacy Act). We understand that it is proposed that the data quality obligations be moved into the PCEHR Rules.

⁸⁹ PCEHR Act, section 70.

⁹⁰ PCEHR Act, section 73.

- (g) In any case, whether a matter generates a complaint about a breach of the APPs or an 'interference with privacy', enforcement will depend on the Privacy Commissioner's ability to investigate and conciliate complaints in a timely manner.

Recommendation 42

That the Department include, in the amending legislation, an expansion of the civil penalty provision at section 78 of the PCEHR Act to cover all participants covered by the PCEHR Rules.

8.5.6 Resourcing the complaints handling function

- (a) The enforcement of both the APPs and the general 'interference with privacy' provisions of the PCEHR Act depend on the Australian Privacy Commissioner having sufficient resources to carry out expeditious investigations.
- (b) The number of privacy complaints handled by the Office is already rising significantly.⁹¹ We suggest that delays in the resolution of complaints can be expected in 2014-15 and beyond, without significant additional resourcing.⁹²
- (c) Public trust in the PCEHR system, and in particular in the proposed shift to an Opt-Out Model, may depend in part upon the government as a whole being able to demonstrate its commitment to a robust privacy governance framework. This will include resourcing of a proactive complaints-handling unit within the Department (though, we suggest, independent of the System Operator), as well as resourcing of the key regulator, the Australian Privacy Commissioner.

Recommendation 43

That the Department ensure the governance of the PCEHR system is adequately resourced, including establishing a complaints-handling unit independent of the PCEHR System Operator, with the ability to offer compensation to harmed individuals, report suspected criminal instances of misuse to the police, and report to the Privacy Commissioner and others on both individual and systemic issues.

Recommendation 44

That additional resourcing be provided to the Privacy Commissioner to manage PCEHR-related complaints, investigations and advisory functions, modelled on the expected increase in individuals with a PCEHR under an Opt-Out Model.

8.5.7 Obligations to minimise harm arising from a breach

- (a) Mandatory breach notification is intended both to act as a deterrent (by encouraging robust data security practices to avoid breaches occurring) and as a harm-minimisation

⁹¹ [In 2013–14, the OAIC received 4239 privacy complaints](http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201314/chapter-seven-privacy-compliance), an increase of 183.3% over the 1496 received in 2012–13. See <http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201314/chapter-seven-privacy-compliance>

⁹² [In 2013–14, complaints were closed in an average of 2.8 months. However in 2013-14, only 2617 privacy complaints were closed, while 4,239 new ones were opened](http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201314/chapter-seven-privacy-compliance). We suggest that delays can therefore be expected in 2014-15, without significant additional resourcing. See <http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201314/chapter-seven-privacy-compliance>, accessed 18 December 2014.

strategy (by enabling affected individuals to take further steps to protect themselves from harm).

- (b) Section 75 of the PCEHR Act requires certain participants in the PCEHR system to notify affected individuals and/or the Privacy Commissioner of any identified instances of an 'unauthorised collection, use or disclosure of health information' from a PCEHR.
- (c) This provision only applies to the System Operator, a registered repository operator or a registered portal operator. It does not currently cover healthcare provider organisations.
- (d) This provision also only applies to 'health information'.
- (e) We suggest that the scope of this provision should be expanded to *all* relevant authorised users of *any* types of personal information from PCEHRs.

Recommendation 45

That the Department include, in the amending legislation, an expansion of the data breach notification requirements in section 75 of the PCEHR Act to cover all participants (i.e. all authorised users of the PCEHR system), and also to cover all 'identifying information' and other types of 'personal information' not already encompassed by the term 'health information'.

8.5.8 Gaps in the enforcement regime

- (a) As noted above, there are various gaps and weaknesses in the current enforcement regime, including:
 - (i) criminal offence provisions do not exist in the PCEHR Act;
 - (ii) neither criminal nor civil penalties offer redress to the victim of a privacy breach;
 - (iii) compensation for the victim of a privacy breach depends on the scope of the Privacy Commissioner's powers, and adequate resourcing of the Privacy Commissioner's Office;
 - (iv) the 'interference with privacy' provisions do not apply to all participants in the PCEHR system;
 - (v) the 'interference with privacy' provisions do not apply to all types of conduct which could lead to harm; and
 - (vi) the APPs (or the State/Territory equivalents) do not apply to all participants in the PCEHR system.
- (b) Even when privacy principles such as the APPs might apply, interpretation of privacy laws to date has exposed other weaknesses.
- (c) 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 'collection' or 'use' of the information by the user, such as to trigger their privacy obligations (noting that, for the purposes of the PCEHR Act at least, 'use' is defined to include 'view').⁹³

⁹³ *Director General, Department of Education and Training v MT* (GD) [2005] NSWADTAP 77; and *JD v Department of Health* (GD) [2005] NSWADTAP 44.

- (d) Case law also suggests that a respondent organisation can avoid responsibility for providing a civil remedy to the victim of a privacy breach if the user responsible for the breach can be characterised as having been on a 'personal frolic'.⁹⁴ That is, organisation responsibility may be reduced and, even where the individual user may be liable instead, an individual is less likely to be able to pay any significant monetary remedy.
- (e) 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.

8.5.9 Statutory cause of action to address gaps

- (a) Even if all of the above recommendations are accepted and adopted, there will likely remain weaknesses in the criminal and civil enforcement models.
- (b) Criminal offence and civil penalty provisions, even if enacted, could provide a deterrent effect, but can provide no redress for a victim who has suffered harm as a result of the crime. To obtain redress for a suffered harm, the victim requires a compensation model.
- (c) One compensation model is by way of a complaint to the Privacy Commissioner.
- (d) Some acts cannot be the subject of a complaint to the Privacy Commissioner, such as inadequate data security by healthcare provider organisations not regulated by the APPs (such as State/Territory public hospitals, not all of which have equivalent privacy laws to the APPs), or misconduct by individuals rather than regulated 'entities'.
- (e) Obtaining redress for those acts which *can* be complained about to the Privacy Commissioner depends on the resourcing of the Privacy Commissioner's Office.
- (f) In recognition of some of these gaps and weaknesses in current privacy laws and their enforcement, the Australian Law Reform Commission has recently recommended enactment of a statutory cause of action for serious invasions of privacy.⁹⁵ This would give individuals the right to pursue a remedy without having to rely on the Privacy Commissioner taking action.
- (g) We suggest that a similar model could be adopted and applied to the PCEHR system, as a final 'safety net' to cover only the most serious of cases, which would allow an individual to privately commence proceedings against a respondent for compensation – but only if the individual has suffered harm due to an intentional or reckless handling of private information in relation to their PCEHR.
- (h) The type of scenario to be included would be 'revenge disclosure', such as a healthcare provider accessing his ex-girlfriend's PCEHR, and disclosing mental health information about her on social media, which could result in her loss of employment, and thus significant financial harm as well as personal distress and potentially risks to her mental well-being. Neither civil nor criminal penalties against the individual healthcare provider, even if available and successful, can compensate the individual for the serious harm suffered.
- (i) The inclusion of this type of final safety net could be an important consideration for the public when considering the proposed shift to an Opt-Out Model, as they weigh up the relative risks and benefits to themselves as health consumers.

⁹⁴ See for example *Director General, Department of Education and Training v MT* [2006] NSWCA 270.

⁹⁵ See Australian Law Reform Commission, *Report 123: Serious Invasions of Privacy in the Digital Era*, available at <http://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123>, accessed 18 December 2014.

- (j) We suggest that the drafting of such a cause of action ensure that its scope includes:
 - (i) intentional and unauthorised browsing, viewing, collection, use, disclosure or secondary disclosure of personal information, health information or identifying information in or from a PCEHR; or
 - (ii) a reckless failure to take reasonable steps to ensure the quality or security of that information.

Recommendation 46

That the Department include, in the amending legislation, a statutory cause of action modelled on the Australian Law Reform Commission's recommendations in ALRC Report 123, such that an individual who has suffered due to an intentional or reckless handling of private information in relation to their PCEHR (such as an intentional and unauthorised browsing, viewing, collection, use, disclosure or secondary disclosure of their personal information, health information or identifying information in or from a PCEHR, or a reckless failure to take reasonable steps to ensure the quality or security of that information), can sue the responsible party for compensation.

Chapter 9 Conclusions

9.1 The Privacy Positives

9.1.1 Important proposed privacy controls will remain

There are a number of privacy controls already built into the PCEHR system. Importantly, the following features will remain:

- (a) the individual can utilise a range of privacy control settings to control what content can populate their PCEHR, who can access that content, and whether the individual wants to receive notifications when certain things happen;
- (b) healthcare providers cannot 'trawl' through the system to find records relating to people who are not their patients; to find an individual's PCEHR, the authorised user needs to already know the individual's IHI, or the following details about the individual:
 - (i) Medicare card number, Individual Reference Number (IRN – the person's position number on the card), family name, given name, date of birth and sex; or
 - (ii) Medicare card number, IRN, family name, date of birth and sex (this type of search can only be used if the individual has only one name); or
 - (iii) Medicare card number, family name, given name, date of birth and sex; or
 - (iv) DVA file number, family name, given name, date of birth and sex; or
 - (v) DVA file number, family name, date of birth and sex (this type of search can only be used if the individual has only one name); or
 - (vi) family name, given name, date of birth, sex and Medicare-recorded address;
- (c) the individual's home address is not displayed to the healthcare provider from the PCEHR shell record;
- (d) there is an audit log, visible to the individual themselves, of all instances of access to their record by authorised users;
- (e) for individuals between the ages of 14 and 18 who have not taken control of their PCEHR, MBS and PBS details will not be accessible through their PCEHR, in line with existing Medicare policy to keep this information private from parents or others without the express consent of the young person;
- (f) the individual can cancel their PCEHR at any time, and re-instate it again at any time; and
- (g) there is a program to monitor access to individuals' records, including heightened monitoring of access to people of particular interest, and unusual patterns of access by authorised users.

9.1.2 Proposed new privacy positives

There are a number of additional privacy controls proposed as part of the shift to an Opt-Out Model:

- (a) the individual can opt-out of being registered;
- (b) confirmation of a successful 'opt-out' will be sent to the individual using their Medicare address;
- (c) the 'shell record' will not include any clinical content;

- (d) there will be a transition period, before any healthcare providers can access PCEHRs of automatic registrants, during which individuals can access their 'shell record' and adjust their privacy control settings;
- (e) clinical content will only start 'flowing' into the PCEHR the first time either the individual accesses the record, or a healthcare provider views or uploads to the record;
- (f) the Department plans to improve the usability of the existing privacy control settings, so that individuals may better understand and exercise their various choices about content, access controls and notifications; and
- (g) an additional privacy setting will be introduced, to allow individuals to choose if they would like an automated notification, such as an email or SMS, *every* time their PCEHR is accessed.

9.2 Privacy risks and recommendations

- (a) We have found that a number of the identified privacy risks relating to the Opt-Out model can be addressed through various migration strategies relating to the amendments to the PCEHR and HI Acts, communications, transparency and system design. However, whether this assessment remains true depends on:
 - (i) the final form of the legislation in relation to authorising collections, uses and disclosures;
 - (ii) the final IT system design; and
 - (iii) other decisions that need to be made by the Department at an operational level.
- (b) Our recommendations are set out in full below.

Recommendation 1

That, in order to ensure transparency and assist public debate about the privacy risks and benefits of implementing the Opt-Out Model, the Department publish:

- (a) the Deloitte *Report on the public consultation into the Review of the PCEHR* (once finalised);
- (b) this PIA report; and
- (c) an exposure draft Bill.

Recommendation 2

That prior to introducing the legislation, the Department conduct further consultation on this proposal with groups representing those most likely to be concerned about the privacy of their health information and other personal information, including both individuals and practitioners in the family violence, mental health and sexual health fields.

Recommendation 3

That a letter, addressed to the named individual, is sent to every Medicare card holder, about the change to an Opt-Out Model. The letter should explain:

- that unless they opt out by X date, they will be registered for a PCEHR (i.e. a PCEHR will be created for them);
- what the default privacy control settings allow;
- how they can opt out or adjust their privacy control settings if they wish;
- who to contact if they have an enquiry; and
- who to contact, including the Privacy Commissioner, if they have a privacy complaint.

Recommendation 4

That the Department investigate how other forms of direct communications could also be utilised, without leading to additional collections of personal information, for example by sending an email to the 6 million existing myGov account holders.

Recommendation 5

That the Department ensure its communication strategy includes measures to reach vulnerable and disadvantaged individuals who may not receive or understand a letter, such as individuals from a non-English speaking background, Indigenous people, the illiterate, homeless, and adults with limited or no capacity.

Recommendation 6

That the Department ensure its communication strategy includes measures to reach other people who may not receive a named letter, such as leaflets at Australian Immigration counters or other government shopfronts during the Opt-Out and Transition Periods, to target returning travellers and other individuals.

Recommendation 7

That the system design include, for any individuals who were automatically registered (and who have not already taken action to set their own privacy controls), a communication direct to the individual, which is triggered the first time their PCEHR is accessed by a healthcare provider.⁹⁶ The communication should explain that their PCEHR is now 'live', what the default privacy settings allow, how they can adjust their privacy control settings if they wish, who to contact if they have an enquiry, and who to contact (including the Privacy Commissioner), if they have a privacy complaint. The communication could be sent by email or SMS if the individual has previously provided such details (see also **Recommendation 30**), or otherwise by mail to the Medicare-provided address.

⁹⁶ The conditions for triggering this communication should be the same as the conditions which will trigger the 'flow' of Medicare-provided data to begin – i.e. either a healthcare provider views the PCEHR, or a system uploads a clinical document to it, such as a hospital discharge summary.

Recommendation 8

That the Department consider whether it is technically feasible and appropriate for the PCEHR system to be designed to allow medical software providers' systems to generate a pop-up message the first time an individual's PCEHR is viewed by a healthcare provider, which the healthcare provider could then print out for the individual who is present with them.

Recommendation 9

The PCEHR Privacy Statement on the eHealth website should be reviewed and updated to ensure that it addresses the relevant entities that will be handling personal information and in what capacity (i.e. System Operator, HI Service Operator and NIO), and the purposes for which information will be collected, used and disclosed by those entities.

Recommendation 10

That the Online Opt-Out Service include a clear summary about how the opt-out process works and the implications of opting out (or not opting out), as well as information about the ability to set privacy controls.

Recommendation 11

That the Department develop an appropriate collection notice to include in the Online Opt-Out Service which explains how a person's personal information will be handled (collected, used and disclosed) by and between various entities (i.e. the System Operator, HI Service Operator, NIO, Medicare and Document Verification Service (DVS)) during the opt-out process and automatic registration process. The collection notice should also address the use and disclosure of existing information held by the System Operator, the HI Service Operator and Medicare for the purpose of implementing an individual's decision to opt-out or cancel a PCEHR (including identity verification processes), and to automatically register relevant individuals for a PCEHR.

Recommendation 12

That the drafting instructions for the proposed amendments to the HI Act ensure that section 22A of the HI Act is amended so that the scope of the provision allows the HI Service Operator to use identifying information and healthcare identifiers of individuals for the purpose of implementing an individual's choice to opt-out.

Recommendation 13

Subject to consideration of any secondary implications of changing the definition of 'identifying information' in section 7 of the HI Act, that the drafting instructions for the proposed HI Act amendments ensure that the definition of 'identifying information' is amended to include IHI record status and IHI status.

Recommendation 14

That the drafting instructions for the proposed HI Act amendments ensure that section 22A of the HI Act is amended so that the scope of the provision allows the HI Service Operator to disclose identifying information and healthcare identifiers of individuals for the purpose of implementing an individual's choice to opt-out.

Recommendation 15

That the Online Opt-Out Service design limit the number of times that a user of the Online Opt-Out Service may attempt to verify their identity.

Recommendation 16

That the drafting instructions for the proposed amendments to the PCEHR Act ensure that section 58 is amended so that the scope of the provision:

- allows Medicare to use and disclose identifying information for the purposes of implementing the individual's choice to opt-out their dependants; and
- allows for purposes of uses and disclosures beyond identity verification.

Recommendation 17

That the Department, in conjunction with DHS, develop a scripted message for telephone and face to face opt-out channels which identifies the specific information handling arrangements that arise during the opt-out process.

Recommendation 18

That the Department develop, or update existing, written materials (brochures, booklets etc.) to provide information about the opt-out process and the handling of personal information in that context.

Recommendation 19

Further to Recommendation 16, that the proposed amendment to section 58 of the PCEHR Act allows the System Operator/NIO to use identifying information for the purposes of identifying Automatic Registrants and implementing automatic registration.

Recommendation 20

That the Department consider allowing longer than a six week Transition Period for individuals to adjust their privacy control settings.

Recommendation 21

Information about setting privacy controls, including the way in which it is presented should be easy for individuals to understand. Privacy controls should also be as easy as possible to implement.

Recommendation 22

That the Department engage individuals in re-designing the labelling, layout and explanation of the various privacy control settings, so as to ensure that communications are clear, neutral and explicit.

Recommendation 23

That the Department ensure that clear, neutral and explicit information is available to the individual, including at the Online Opt-Out Service, to explain built-in privacy features of the system, how things will work under the default settings, and how the individual can adjust their privacy control settings and take other steps to address various privacy concerns they might have.

Recommendation 24

That the Department provide or fund specialist assistance to help vulnerable and disadvantaged individuals (such as individuals from a non-English speaking background, the illiterate, homeless, and adults with limited or no capacity) to understand and utilise their privacy control settings.

Recommendation 25

That the information to be included in the Newborn Child Declaration must at the very least make clear that unless they opt-out the newborn, the newborn will be registered for a PCEHR (i.e. a PCEHR will be created for them).

Recommendation 26

That further information be included in the Newborn Child Declaration, or if this is not possible provided as an information sheet to parents/guardians as soon as practicable after the parent/guardian receives the Newborn Child Declaration, which advises the parent/guardian in plain language:

- the information that will be collected by the HI Service Operator and the System Operator, and how it will be collected;
- what the default privacy control settings in the PCEHR allow;
- how the parent/guardian can adjust the newborn's PCEHR privacy settings;
- who to contact if the parent/guardian has an enquiry; and
- who to contact, including the Privacy Commissioner, if the parent/guardian has a privacy complaint.

Recommendation 27

That the following information be provided as part of Forms 2888 and 3101, or by way of an information sheet attached to or provided with those forms:

- an explanation that, unless the individual decides to opt-out, they will be registered for a PCEHR;
- the information that will be collected by the System Operator, and how it will be collected;
- what the default privacy control settings in the PCEHR allow;
- how they can opt-out or adjust their privacy control settings if they wish;
- who to contact if they have an enquiry; and
- who to contact, including the Privacy Commissioner, if they have a privacy complaint.

Recommendation 28

That the Department develop a process to ensure that individuals who will be issued an IHI as part of the DVA process have the opportunity to opt-out of PCEHR registration, and that the following information be provided to those individuals as part of that process (by inclusion in relevant forms or by way of an information sheet attached to or provided with those forms):

- an explanation that, unless the individual decides to opt-out, they will be registered for a PCEHR;
- the information that will be collected by DVA, Medicare, the HI Service Operator and the System Operator, and how it will be collected;
- what the default privacy control settings in the PCEHR allow;
- how they can opt-out or adjust their privacy control settings if they wish;
- who to contact if they have an enquiry; and
- who to contact, including the Privacy Commissioner, if they have a privacy complaint.

Recommendation 29

That the Online Opt-Out Service design include the ability for the individual to consider and adjust privacy control settings in relation to notifications, Medicare-provided content and setting a RAC, in advance of the creation of their shell record.

Recommendation 30

If Recommendation 29 is accepted, that the Online Opt-Out Service design also include the ability for the individual to supply an email address, so that the System Operator can send the individual a message once the record is 'live', with a reminder about how to log in to myGov to access their record or further adjust their privacy control settings. (See also

Recommendation 8.)

Recommendation 31

That the Department continue work to improve the accessibility and usability of online access and controls for individuals, while ensuring that any changes to identity verification to improve usability do not increase the risk of inadvertent disclosure to a third party.

Recommendation 32

That the Department give further consideration in the future to having a standalone PCEHR individual access portal separate to myGov.

Recommendation 33

That prior to the implementation of the Opt-Out Model, the Department consult with DHS as the myGov operator to provide a registration solution scalable to almost 24 million individuals, which does not operate on the assumption that the individual can supply a unique email address.

Recommendation 34

That the Department include links on any 'Opt-Out' websites relating to the transition to an Opt-Out Model to existing clinical safety audits, as well as reports outlining the steps taken by the Department to address any recommendations arising from those audits, prior to implementing the Opt-Out Model.

Recommendation 35

That the Department commission and publish an updated review of the data quality risks posed by the use of IHI and Medicare provided data, in the context of almost 24 million individuals, and implement any remediating strategies, prior to implementing the Opt-Out Model.

Recommendation 36

That the Department conduct a pilot of the Opt-Out Model, including the automatic registration of individuals, the creation of shell records, and testing the accuracy of automated data flows from Medicare, to ensure any data accuracy issues are identified and addressed, prior to implementing the Opt-Out Model.

Recommendation 37

That the Department commission an information security Threat & Risk Assessment in relation to the PCEHR system, including the security of the myGov individual access channel, and the adequacy of the identity verification process for individuals to access their PCEHR, prior to implementing the Opt-Out Model.

Recommendation 38

As part of the design development in relation to the online and telephone channels, the Department should consider alternative pathways for an individual to verify their identity where they do not have a primary EOI document at all, or only have an EOI document in a different name to their Medicare card. For example, the Online Opt-Out Service and telephone channel could be designed to also allow the Medicare-information only method of verifying the individual's identity.

Recommendation 39

That the Department provide or fund specialist assistance to help vulnerable and disadvantaged individuals (such as individuals from a non-English speaking background, the illiterate, homeless, and adults with limited or no capacity) to access one of the channels to exercise their opt-out choice.

Recommendation 40

That the Department develop a De-identification Protocol, in consultation with the Australian Privacy Commissioner and taking into account the risk of re-identification from de-identified datasets, prior to implementation of the Opt-Out Model.

Recommendation 41

That the Department review whether existing criminal offence provisions in other statutes already effectively cover all the scenarios which could involve unauthorised viewing, collection, use and/or disclosure of an individual's PCEHR, or information drawn from their PCEHR, and whether such provisions set sufficiently serious maximum penalties to act as a deterrent. If existing provisions elsewhere are sufficient, we suggest inserting a note in the PCEHR Act, referring to those other provisions. Otherwise, we suggest adding criminal offence provisions to the PCEHR Act, related to the unlawful viewing, collection, use, disclosure, secondary disclosure or soliciting a misuse or disclosure of health information, personal information or identifying information in or from an individual's PCEHR, with a maximum penalty including both penalty units and a two year term of imprisonment.

Recommendation 42

That the Department include, in the amending legislation, an expansion of the civil penalty provision at section 78 of the PCEHR Act to cover all participants covered by the PCEHR Rules.

Recommendation 43

That the Department ensure the governance of the PCEHR system is adequately resourced, including establishing a complaints-handling unit independent of the PCEHR System Operator, with the ability to offer compensation to harmed individuals, report suspected criminal instances of misuse to the police, and report to the Privacy Commissioner and others on both individual and systemic issues.

Recommendation 44

That additional resourcing be provided to the Privacy Commissioner to manage PCEHR-related complaints, investigations and advisory functions, modelled on the expected increase in individuals with a PCEHR under an Opt-Out Model.

Recommendation 45

That the Department include, in the amending legislation, an expansion of the data breach notification requirements in section 75 of the PCEHR Act to cover all participants (i.e. all authorised users of the PCEHR system), and also to cover all 'identifying information' and other types of 'personal information' not already encompassed by the term 'health information'.

Recommendation 46

That the Department include, in the amending legislation, a statutory cause of action modelled on the Australian Law Reform Commission's recommendations in ALRC Report 123, such that an individual who has suffered due to an intentional or reckless handling of private information in relation to their PCEHR (such as an intentional and unauthorised browsing, viewing, collection, use, disclosure or secondary disclosure of their personal information, health information or identifying information in or from a PCEHR, or a reckless failure to take reasonable steps to ensure the quality or security of that information), can sue the responsible party for compensation.

Schedule 1 – Detailed information flows: Online Opt-Out Service

Step	Description	Information Flow
0.1	Accessing the Online Opt-Out Service	
0.1	<p>The individual accesses the Online Opt-Out Service, and selects the option to opt-out of receiving a PCEHR. Information about PCEHRs, the PCEHR system and the opt-out process (content to be developed) will be made available to individuals on the eHealth website.</p> <p>The Online Opt-Out Service will be hosted by DHS as delegate of the System Operator (System Operator (DHS)).</p> <p>Information collected and stored by the System Operator (DHS) will be stored in the DHS system.</p> <p>The opt-out process, and cancellation process, commences when the individual enters their identifying information into the Online Opt-Out Service in Step 1.</p>	N/A
1-4	Verification of individual's identity (Enhanced Bronze Level Assurance)	
1	<p>The individual enters the following information in the Online Opt-Out Service (via secure online channel):</p> <ul style="list-style-type: none"> • first name, last name, sex, date of birth, and Medicare card number or DVA card number; and • the unique reference number of the individual's driver licence, passport or Immicard (an 'EOI Credential') that can be verified through the Document Verification Service (DVS) and the EOI credential type. <p>We have assumed that this information will be collected by the System Operator (DHS) and not simply passed on to the HI Service Operator and DVS.</p>	System Operator (DHS) collects personal information about the individual.

Step	Description	Information Flow
2a	<p>System Operator (DHS):</p> <ul style="list-style-type: none"> • provides the individual's first name, last name, sex, date of birth and Medicare/DVA card number to the HI Service Operator; and • requests the HI Service Operator to perform an 'IHI Lookup' and: <ul style="list-style-type: none"> ○ check the information about the individual matches the information in the HI system; and ○ if there is a match, provide the individual's IHI number, IHI record status, and IHI status. <p>The Department has advised that the above information is the minimum data set required for the HI Service Operator to identify the relevant IHI.</p>	<p>System Operator (DHS) discloses personal information about the individual to the HI Service Operator.</p> <p>HI Service Operator collects the personal information about the individual from the System Operator (DHS).</p>
2b	<p>The HI Service Operator checks whether there is an existing IHI record which matches the personal details provided in Step 2a, and sends the IHI Lookup outcome to the System Operator (DHS).</p> <ul style="list-style-type: none"> • If there is not an exact match, the HI Service Operator sends an error message to the System Operator (DHS). • If there is an exact match, the HI Service Operator sends to the System Operator (DHS) the individual's: <ul style="list-style-type: none"> ○ IHI number; ○ IHI record status; and ○ IHI status. 	<p>The HI Service Operator:</p> <ul style="list-style-type: none"> • uses the personal information collected in Step 2a, as well as existing personal information held by the HI Service Operator, to locate the individual's IHI record; and • discloses personal information (including IHIs) to the System Operator (DHS). <p>System Operator (DHS) collects personal information (including IHIs) from the HI Service Operator.</p>
3a	<p>System Operator (DHS) requests DVS to perform a DVS check by providing:</p> <ul style="list-style-type: none"> • the individual's first name, last name, date of birth and (where the EOI Credential is an Australian passport) sex; and • the EOI Credential type and unique reference number. 	<p>System Operator (DHS) discloses personal information about the individual to the Attorney-General's Department (as the DVS operator).</p>

Step	Description	Information Flow
3b	DVS checks whether there EOI Credential is a 'real' document (e.g. that it has a record of a driver licence, passport, etc., issued to a person matching the details provided in Step 3a), and sends a 'Yes' or 'No' response to the System Operator (DHS).	<p>The DVS checking process conducted by the Attorney-General's Department is out of scope.</p> <p>System Operator (DHS) collects personal information (i.e. the fact the individual's identity has been verified) about the individual from the Attorney-General's Department (as the DVS operator).</p>
4	<p>If an error message is received from the HI Service Operator in Step 2b, or a 'No' response is received from DVS in Step 3b, the Online Opt-Out Service will display a message to the individual:</p> <ul style="list-style-type: none"> advising that their identity was not verified, and recommending that they contact the eHealth helpline for assistance; and showing a Transaction Reference Number (TRN). 	N/A
5a-5e	<p>Verification of child dependants (if applicable)</p> <p><i>(Skip Steps 5a to 5e and go to Step 6 if the individual is under 14 years.)</i></p>	
5a	The Online Opt-Out Service will allow the individual to specify (by entering first name and last name of) any dependants on the same Medicare card who they would like to include in the opt-out / record cancellation request.	System Operator (DHS) collects personal information about the dependants from the individual.
5b	<p>The System Operator (DHS) sends a request to Medicare for information relating to dependants listed on the individual's (hereafter, also the 'Authorised Representative') Medicare card.</p> <p>In making this request, the System Operator (DHS) sends to Medicare the purported Authorised Representative's first name, last name, sex, date of birth and Medicare/DVA card number (collected in Step 1) and names of dependants collected in Step 5a.</p>	<p>System Operator (DHS) discloses personal information about dependants collected in Step 5a and the individual collected in Step 1 to Medicare.</p> <p>Medicare collects the information provided by the System Operator (DHS).</p>
5c	Medicare uses the individual's information to search the Medicare system	Medicare:

Step	Description	Information Flow
	<p>and locate the dependants who:</p> <ul style="list-style-type: none"> are listed on the same Medicare card as the individual; are under 18 years old; are at least 14 years younger than the individual; and match the information (first name, last name) entered by the individual at Step 5a. <p>Medicare provides to System Operator (DHS) the first name and last name, sex and date of birth for each dependant that matches (or an error message where there is a mismatch, allowing the individual to correct and resubmit or remove the dependant in Step 5a).</p>	<ul style="list-style-type: none"> uses the information provided by the System Operator (DHS), as well as existing information held in the Medicare system, to locate the dependants of the individual; and discloses personal information about the individual's dependants to the System Operator (DHS). <p>System Operator (DHS) collects personal information about dependants (first name, last name, sex, date of birth and Medicare/DVA card number) from Medicare.</p>
5d	<p>System Operator (DHS):</p> <ul style="list-style-type: none"> provides the first name, last name, sex, date of birth and Medicare/DVA card number of each of the dependants identified by Medicare in Step 5c to the HI Service Operator; and requests the HI Service Operator to perform an 'IHI Lookup' for each of the dependants. 	<p>System Operator (DHS) discloses personal information about dependants to the HI Service Operator.</p>
5e	<p>The HI Service Operator checks whether there is an existing IHI record which matches the personal details provided in Step 5d, and sends the IHI Lookup outcome to System Operator (DHS).</p> <ul style="list-style-type: none"> If there is not an exact match, the HI Service Operator sends an error message to the System Operator (DHS). If there is an exact match, the HI Service Operator sends to the System Operator (DHS) the relevant dependants': <ul style="list-style-type: none"> IHI number; IHI record status; and IHI status. 	<p>HI Service Operator:</p> <ul style="list-style-type: none"> collects personal information in Step 5d from the System Operator (DHS); uses the information collected from the System Operator (DHS), as well as existing information held by the HI Service Operator, to locate the IHI record for the relevant dependant(s); and discloses personal information (including IHIs) to the System Operator (DHS). <p>System Operator (DHS) collects personal information (including IHIs) from the HI Service Operator.</p>

Step	Description	Information Flow
6	PCEHR registration check	
6	<p>System Operator (DHS) provides the first name, last name, sex, date of birth, Medicare card number/DVA card number, IHI number, IHI record status and IHI status of the individual/Authorised Representative, and each of the dependants identified in Step 5, to the System Operator (NIO).</p> <p>System Operator (NIO) checks whether the individual/Authorised Representative, and each of the dependants identified in Step 5, is registered for a PCEHR and, if so, whether they have taken control of their PCEHR.</p> <p>After checking the PCEHR system, the System Operator (NIO) advises the System Operator (DHS) whether or not the individual/dependants has/have an existing PCEHR. Dependants who have an existing PCEHR and have taken control of their record will be included in the list provided to the System Operator (DHS).</p>	<p>System Operator (DHS and NIO) '<u>use</u>' personal information about the individual/Authorised Representatives and dependants in relation to the following:</p> <ul style="list-style-type: none"> • System Operator (DHS) provides personal information to the System Operator (NIO); • System Operator (NIO) uses the personal information received from the System Operator (DHS), as well as existing information held in the PCEHR system, to check whether the individual or dependant(s) have an existing PCEHR (and, if so, whether the dependant has taken control of their PCEHR); • System Operator (NIO) provides the results of the check (i.e. whether there is an existing PCEHR for the individual/dependant and possibly whether the dependant has taken control of their record) to the System Operator (DHS).
7-9a	Opt out / cancellation decision	
7	<p>System Operator (DHS) displays to the individual (via the Online Opt-Out Service) the first and last name of individuals (i.e. the individual and the dependants identified in Step 6) that can be opted out of automatic PCEHR registration, and whether or not that individual has an existing PCEHR. (Note: Information about dependants who have an existing PCEHR and have taken control of that PCEHR will be displayed to the individual/Authorised Representative, however the Authorised Representative will not be able to opt-out or cancel for the minor.)</p>	System Operator (DHS) discloses personal information about dependants to the individual.
8a	<p>The individual/Authorised Representative:</p> <ul style="list-style-type: none"> • selects the individuals they wish to opt-out of automatic PCEHR registration (hereafter, the 'Opt-Out Individuals') / cancel the existing PCEHR registration for (hereafter, the 'Cancellation Individuals'); and 	System Operator (DHS) collects personal information about the individual/Authorised Representative and selected dependants from the individual/Authorised Representative.

Step	Description	Information Flow
	<ul style="list-style-type: none"> for each dependant the Authorised Representative selects, provides a declaration of parental responsibility in relation to each of the selected dependant(s). <p>This information is submitted through the Online Opt-Out Service to the System Operator (DHS).</p>	
8b	<p>System Operator (DHS) stores the first name, last name, sex, date of birth, Medicare card number/DVA card number, IHI number, IHI record status and IHI status of the individual of each Opt-Out Individual in the DHS/Online Opt-Out Service System.</p> <p>(Note: This list will be used to ensure these Opt-Out Individuals are not automatically registered for a PCEHR during the automatic registration process. The list will be provided by the System Operator (DHS) to the System Operator (NIO) as part of the bulk automatic registration process – see information flow in Schedule 2.)</p>	System Operator (DHS) collects and uses personal information about the Opt-Out Individuals.
9a	System Operator (DHS) via the Online Opt-Out Service screen notifies the individual that the opt-out/cancellation process was successful, which comprises the time, date and TRN of the opt-out transaction (but not the name or any other personal information of any of the Opt-Out Individuals).	N/A (no personal information is handled in this step.)
10a-10b	<p>Cancellation of existing PCEHR registrations (if applicable)</p> <p><i>(Skip Steps 10a and 10b if the individual/Authorised Representative did not elect to cancel the PCEHR registration for any individuals.)</i></p>	
10a	<p>System Operator (DHS):</p> <ul style="list-style-type: none"> provides each Cancellation Individual's IHI number, first name, last name, sex, and date of birth to the System Operator (NIO); and directs the System Operator (NIO) to cancel the PCEHR registration of each Cancellation Individuals. 	System Operator (DHS) 'uses' personal information about each of the Cancellation individuals by providing that information to the System Operator (NIO).

Step	Description	Information Flow
10b	The PCEHR System Operator (NIO) locates the PCEHR of each Cancellation Individual and cancels the PCEHR registration. This process (including notification letters) will follow existing processes.	<p>Out of scope – this is an existing process.</p> <p>We have assumed that, once NIO is directed to cancel an individual's record, the way a PCEHR is cancelled via the opt-out process is the same as the current online cancellation process.</p>
11-12	Notification of opt-out	
11	<p>System Operator (NIO) will:</p> <ul style="list-style-type: none"> provide to Medicare: <ul style="list-style-type: none"> the individual/Authorised Representative's IHI number, first name, last name, sex and date of birth; the IHI number, first name, last name, sex and date of birth of each Opt-Out Individual; and instruct Medicare to send an opt-out notification to the individual/Authorised Representative stating that each of the Opt-Out Individuals have been opted-out of automatic PCEHR registration. 	PCEHR System Operator (NIO) discloses personal information about the individual/Authorised Representative and each Opt-Out Individual to DHS/Medicare.
12	<p>Medicare sends a notification to the individual/Authorised Representative confirming that each Opt-Out Individual has been opted out of being automatically registered for a PCEHR, and will identify each Opt-Out Individual by their first and last name.</p> <p>Note: For the purposes of this PIA, we have assumed that notifications will be sent by mail to the individual/Authorised Representative's registered Medicare mailing address.</p>	<p>Medicare:</p> <ul style="list-style-type: none"> collects the personal information received from the System Operator (NIO) in Step 11; uses the information received from the System Operator (NIO), as well as existing information held in the Medicare system (i.e. the individual's address), to send a notification to the individual/Authorised Representative; and discloses personal information about dependants to the individual/Authorised Representative.

Schedule 2 – Detailed information flows: Automatic registration

Step	Particulars	Information Flow
1-4	Identification of Automatic Registrants	
1	<p>System Operator (NIO) requests:</p> <ul style="list-style-type: none"> the HI Service Operator provide the list of all individuals registered with the HI Service to NIO who have an active IHI status and verified IHI record status; and the System Operator (DHS) provide the list of all individuals who opted-out of being automatically registered for a PCEHR. 	N/A (No personal information is handled in this step.)
2	<p>HI Service Operator provides the IHI, IHI record status, IHI status, first name, last name, sex, address (except for individuals under 18 years) and date of birth of each individual registered in the HI Service (that has an active IHI status and verified IHI record status) to the System Operator (NIO).</p>	<p>HI Service Operator uses its database.</p> <p>HI Service Operator discloses personal information (including IHIs) about individuals to the System Operator (DHS).</p> <p>System Operator (DHS) collects personal information from the HI Service Operator.</p>
3	<p>System Operator (DHS) provides the IHI, IHI record status, IHI status, first name, last name, sex, address (except for individuals under 18 years) and date of birth of each individual that opted-out during the Opt-Out Period to System Operator (NIO).</p>	System Operator uses personal information (including IHIs).
4	<p>System Operator (NIO):</p> <ul style="list-style-type: none"> uses information obtained in Steps 2 and 3; uses the PCEHR system to identify the individuals who have an existing PCEHR or had (but have since cancelled) a PCEHR; and creates a list of the people that will be automatically registered for a PCEHR (the 'Automatic Registrants') by removing the individuals who opted out and the individuals who have/had a PCEHR from the list of all individuals registered in the HI Service with an active IHI status and 	System Operator (DHS) uses personal information (including existing data held in the PCEHR system) about individuals.

Step	Particulars	Information Flow
	verified IHI record status.	
5-6	Creation of shell PCEHR	
5	System Operator (NIO) creates a shell record for each Automatic Registrant using the HI Data Set collected from the HI Service Operator.	System Operator (NIO) uses personal information (including IHIs) about Automatic Registrants.
6	System Operator (NIO) sets the default access and content control settings for each Automatic Registrant's PCEHR, including in relation to 'standing authority' for the upload of health information and MBS and related information.	System Operator (NIO) uses and collects personal information (i.e. information about default access controls) about Automatic Registrants.
7-8	Setting access controls <i>(Skip Steps 7 and 8 if the individual does not access their PCEHR during the Transition Period.)</i>	
7	Individual may create and access their myGov account, and link their myGov account to their PCEHR.	The myGov process itself is out of scope for the purposes of this PIA. However, we will consider the impact of the myGov process on the ability of individuals to set their PCEHR access controls.
8	Individual may, during the Transition Period, access their PCEHR through myGov, and set their access and content preferences as follows: <ul style="list-style-type: none"> access preferences – if the individual wishes to limit the access by healthcare provider organisations to their PCEHR, they can set a Record Access Code (RAC) which healthcare provider organisations must input into the PCEHR system in order to view the individual's PCEHR, or a Limited Document Access Code (LDAC) to restrict access to certain documents; and content preferences – the individual's preferences for the inclusion of the individual's Medicare Benefits Schedule (MBS – future and past two years), Department of Veterans' Affairs (DVA – future and past two years), Pharmaceutical Benefits Scheme (PBS – future and past two years), Repatriation Pharmaceutical Benefits Scheme (RPBS – future and past two years), Australian Childhood Immunisation Register (ACIR – all) and Australian Organ Donor Register (AODR – all) records into 	System Operator (NIO) collects personal information (i.e. information about access controls) about Automatic Registrants. We note that there will be no changes to the existing access controls, although there will be changes to the way in which the access control options are displayed.

Step	Particulars	Information Flow
	the individual's PCEHR.	
9-15	Medicare data flow	
9	When either the individual or a healthcare provider accesses the individual's PCEHR for the first time, this sets off a 'trigger' to upload the two years of retrospective MBS, DVA, PBS and RPBS data to the individual's PCEHR (unless the individual opted-out of this when setting their access controls – see Step 8). (In the case of the healthcare provider, the type of 'access' could be either a user viewing the PCEHR, or a system uploading a clinical document to it, such as a hospital discharge summary.)	N/A (No personal information is handled in this step.)
10	An electronic notification is sent from the System Operator (NIO) to DHS (Chief Executive Medicare) to request that MBS/DVA/PBS/RPBS/AODR/ACIR data (' Medicare Repository Data ') be made available in the PCEHR system. The request will include the following information about the individual: <ul style="list-style-type: none"> • IHI; • whether the individual has a PCEHR identity and/or PCEHR; and • the Medicare Repository Data to be made available (which will be the preferences set by the individual in Step 8 or, if the individual set no preferences during the Transition Period, the upload of all Medicare Repository Data). 	Out of scope - This is an existing process.
11	DHS (Chief Executive Medicare) as registered repository operator identifies the Medicare record for the individual in the Medicare/DVA claims database, PBS/RPBS claims database and ACIR and AODR (the ' live system ') using the IHI.	Out of scope - This is an existing process.
12	DHS (Chief Executive Medicare) as registered repository operator copies the individual's MBS/DVA claims records, PBS/RPBS records, ACIR records and AODR records from its live system to its PCEHR repository administration system.	Out of scope - This is an existing process.

Step	Particulars	Information Flow
13	DHS (Chief Executive Medicare) as registered repository operator attaches the individual's IHI to the individual's Medicare Repository Data in its PCEHR repository administration system.	Out of scope - This is an existing process.
14	<p>DHS (Chief Executive Medicare) as registered repository operator sorts the records in its PCEHR repository administration system to match the automatic (default) uploading of Medicare Repository Data.</p> <p>DHS (Chief Executive Medicare) as registered repository operator indexes the records for individuals who have not opted out of having their retrospective Medicare data from being uploaded. A list of key fields for each record is created in the repository.</p>	Out of scope - This is an existing process.
15	DHS (Chief Executive Medicare) as registered repository operator makes the index available to the PCEHR System Operator (NIO).	Out of scope - This is an existing process.

Schedule 3 – Detailed information flow: Automatic registration of new Medicare and IHI registrants

Step	Particulars	Information Flow
A1- A3	Application to enrol in Medicare <i>(Steps A1 to A3 only applies to individuals, and their dependants (if any), who apply for enrolment in Medicare.)</i>	
A1	<p>Individuals who are enrolled for Medicare will automatically be registered for a PCEHR unless they opt-out.</p> <p><u>Newborn Child Declaration</u></p> <p>After the birth of a child (newborn), the Newborn's mother (or potentially the Newborn's father or an adoptive mother or father) will be provided with a Newborn Child Declaration, which allows the Newborn's mother to apply for, among other things, Medicare enrolment of the Newborn.</p> <p>The Newborn Child Declaration currently has a section which provides information about the PCEHR opt-in process, and will be updated to provide an option for the mother to opt-out the Newborn from being automatically registered for a PCEHR.</p> <p><u>Medicare Enrolment Form</u></p> <p>Certain Australian visa holders,⁹⁷ Australian citizens returning to live in Australia and New Zealand citizens living in Australia (hereafter referred to as 'individuals') can enrol for Medicare by completing the Medicare Enrolment Form (Form 3101).⁹⁸ The individual who makes the application may also include their dependants in the Medicare Enrolment Form. Spouses may apply at the same time</p>	N/A (This step does not involve the handling of any personal information.)

⁹⁷ Migrants living in Australia, persons applying for permanent residency and living in Australia, visitors to Australia, and permanent resident visa holders who were previously enrolled in Medicare that are returning to living in Australia.

⁹⁸ [Medicare Enrolment Application Form](http://www.humanservices.gov.au/customer/forms/3101) (also referred to as Form 3101), available at <http://www.humanservices.gov.au/customer/forms/3101>.

Step	Particulars	Information Flow
	<p>using the same form.</p> <p>The Medicare Enrolment Form will be updated to provide information about the PCEHR opt-out process, and will provide an option for an individual applying for Medicare enrolment to opt-out of being automatically registered for a PCEHR. The individual will also be able to opt-out dependants under 14 years. Any dependants over 14 years can use the same form to opt themselves out.</p>	
A2	<p>The individual completes the Newborn Child Declaration / Form 3101, and provides it to Medicare (to a Medicare officer, either via post or in-person at a DHS Service Centre or, for a Newborn Child Declaration, via a Medicare smartphone app).</p> <p>Medicare collects and uses the Newborn Child Declaration / Form 3101 to enrol the relevant individual(s) in Medicare.</p> <p>As part of the Medicare enrolment process, Medicare will:</p> <ul style="list-style-type: none"> • verify the identity of the individual and each individual to be enrolled, and verify the parent/guardian-dependant relationship between the individual and any dependants applying for Medicare enrolment; and • provide information about each individual it enrolls for Medicare to the HI Service Operator, for the HI Service Operator to allocate the individual a verified IHI. 	<p>Medicare collects and uses personal information about the individual and dependants. This PIA assumes that Medicare collects but does not use the PCEHR opt-out information in the form for its own purposes. The existing Medicare process is out of scope of this PIA. Only new aspects are considered.</p>
A3	<p>The HI Service Operator will collect information about each individual enrolled for Medicare, and allocate them a verified IHI.</p>	<p>HI Service Operator collects and uses personal information about the individual and dependants. This PIA assumes that the HI Service Operator collects but does not use the PCEHR opt-out information for its own purposes. The existing HI Service Operator process is out of scope of this PIA. Only new aspects are considered.</p>
B1-B2	<p>Application to register with HI Service</p> <p><i>(Steps B1 and B2 only applies to individuals who apply for registration in the HI Service.)</i></p>	

Step	Particulars	Information Flow
B1	<p>Individuals who are registered in the HI Service will automatically be registered for a PCEHR unless they opt out.</p> <p><u>Eligible for Medicare, but do not enrol</u></p> <p>Some people who are eligible for Medicare enrolment may choose not to enrol in Medicare. These people may apply to register with the <i>HI Service via the Healthcare Identifiers Service - Application to Create, Verify or Merge an Individual Healthcare Identifier Form (Form 2888)</i>.⁹⁹</p> <p><u>Ineligible for Medicare</u></p> <p>Individuals, such as temporary visa holders, who are ineligible for Medicare, may also apply to register with the HI Service via Form 2888.</p> <p><u>Form 2888</u></p> <p>Form 2888 will be updated to provide information about the PCEHR opt-out process, and will provide an option for the individual applying for registration in the HI Service to opt-out of being automatically registered for a PCEHR.</p>	N/A (This step does not involve the handling of any personal information.)
B2	<p>The individual completes the Form 2888, and provides it to the HI Service Operator (by post to DHS).</p> <p>The HI Service Operator collects and uses Form 2888 to register the individual in the HI Service (i.e. create a verified IHI for the individual or verify the individual's unverified IHI).</p>	HI Service Operator collects and uses personal information about the individual. This PIA assumes that the HI Service Operator collects but does not use the PCEHR opt-out information for its own purposes. The existing HI Service Operator process is out of scope of this PIA. Only new aspects are considered.
C1-C3	<p>Application to register by DVA</p> <p><i>(Step C1 to C3 only applies where DVA enables issue of an IHI for an individual).</i></p>	
C1	The individual provides DVA with information on whether the individual wants to opt-out of being automatically registered for a PCEHR.	<p>The individual discloses personal information to DVA.</p> <p>DVA may collect personal information from the individual. This PIA assumes that DVA collects but does not use the PCEHR opt-</p>

⁹⁹ [Healthcare Identifiers Service - Application to create, verify or merge an Individual Healthcare Identifier form](http://www.humanservices.gov.au/customer/forms/2888) available at <http://www.humanservices.gov.au/customer/forms/2888>.

Step	Particulars	Information Flow
	This process is under development.	out information for its own purposes.
C2	<p>DVA provides Medicare the following information about individuals entitled to receive DVA benefits:</p> <ul style="list-style-type: none"> first name, last name, date of birth, address, sex and DVA number; and if the individual has decided to opt-out, the PCEHR opt-out information. <p>Medicare collects and uses the information to enrol the individual in its DVA claims/RPBS system.</p> <p>As part of the Medicare enrolment process, Medicare will:</p> <ul style="list-style-type: none"> identify whether or not the individual is already registered with Medicare (and therefore has a verified IHI); and if not, provide information about the individual to the HI Service Operator, for the HI Service Operator to allocate the individual a verified IHI. <p>This process will be updated so that, where the individual has decided to opt-out, Medicare also provides the PCEHR opt-out information to the HI Service Operator.</p>	<p>DVA discloses personal information of the individual to Medicare.</p> <p>Medicare collects and uses personal information of the individual. This PIA assumes that Medicare collects but does not use the PCEHR opt-out information for its own purposes. The existing Medicare process is out of scope of this PIA. Only new aspects are considered.</p>
C3	The HI Service Operator will collect information including the PCEHR opt-out information about the individual, and allocate them a verified IHI.	HI Service Operator collects and uses personal information about the individual. This PIA assumes that the HI Service Operator collects but does not use the PCEHR opt-out information for its own purposes. The existing HI Service Operator process is out of scope of this PIA. Only new aspects are considered.
4	<p>Actioning individual's opt-out decisions</p> <p><i>(Step 4 only applies to the individual, the individual's dependant(s) (if any), if they decided to opt out.)</i></p>	
4	<p>If the individual decided (by selecting the opt-out option in the Newborn Child Declaration / Form 3101 / Form 2888 / DVA form) to opt-out himself/herself, or opt-out one or more of their dependants, the HI Service Operator will disclose to the System Operator (NIO):</p> <ul style="list-style-type: none"> the fact that the individual/dependant is opting-out of automatic PCEHR 	<p>The HI Service Operator discloses personal information (including an IHI) to the System Operator (DHS).</p> <p>The System Operator (DHS) collects and uses personal information (including an IHI).</p>

Step	Particulars	Information Flow
	<p>registration; and</p> <ul style="list-style-type: none"> IHI, IHI record status, IHI status, first name, last name, sex, address (except for individuals under 18 years) and date of birth for the individual/dependant. <p>The System Operator (NIO) will:</p> <ul style="list-style-type: none"> collect the personal information about the individual and/or individual's dependants (as applicable) from the HI Service Operator; and record the individual as having 'opted-out', so as not to automatically register them in the future. 	
5-7	<p>Automatic registration of individuals not opted-out</p> <p><i>(Steps 5, 6 and 7 apply to the individual, and the individual's dependant(s) (if any), if they decided not to opt out.)</i></p>	
5	<p>The HI Service Operator provides to the System Operator (NIO):</p> <ul style="list-style-type: none"> the fact that the individual did not opt out (and is to be registered for a PCEHR); and the following information about each individual to be registered: <ul style="list-style-type: none"> IHI, IHI record status (verified), IHI status (active); and first name, last name, sex, date of birth and address (except that address will not be provided for individuals under 18 years). 	<p>The HI Service Operator discloses personal information (including an IHI) to the System Operator (NIO).</p> <p>System Operator (NIO) collects personal information (including IHIs) about each individual.</p>
6	<p>System Operator (NIO) uses the individual's information to check whether the individual has an existing PCEHR registration.</p> <p>If the individual does not have a PCEHR registration, the System Operator (NIO) uses the individual's information to register to the individual for a PCEHR.</p> <p>Note: for dependants, they will be registered for a PCEHR. However, their PCEHR registration will not be linked to the registration of their authorised representative. In order to gain access to a dependant's PCEHR, the authorised representative will need to create and link their myGov account to the dependant's PCEHR registration. Alternatively, the authorised representative can use the telephone, face-to-face or</p>	<p>System Operator (NIO) uses personal information about the individual received from the HI Service Operator, as well as existing information held in the PCEHR system.</p>

Step	Particulars	Information Flow
	mail channels. The process by which a parent or guardian links themselves as an authorised representative of an dependant's PCEHR registration is an existing process and outside the scope of this PIA.	
7	System Operator (NIO) sets the default privacy control settings for the individual, which will not include a Record Access Code (RAC) and allow the upload of Medicare repository information.	System Operator (NIO) uses personal information about the individual.

Schedule 4 – Current participants in the PCEHR system

1. Individual participants

Individual participant	Role and functions
individuals	<p>A prerequisite for registration in the PCEHR System for an individual is that the individual must have been assigned a IHI by the HI Service Operator, and must have provided certain identifying information in accordance with section 40 of the PCEHR Act.</p> <p>Central to the PCEHR System is the concept of personal control. Participating individuals can exercise control over their PCEHR in the 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 organisation access; • set notification settings; • 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	<ul style="list-style-type: none"> • A person younger than 18 years of age and an adult who is incapable of making decisions for themselves can participate in the PCEHR System via an authorised representative. • Three types of authorised representative are recognised by the System Operator: <ul style="list-style-type: none"> o a person with parental responsibility of a child;¹⁰⁰ o a person with legal authority to act on behalf of a child (where the child does not have a person with parental responsibility for them)¹⁰¹ or an adult who lacks capacity;¹⁰² or o a person who, in the absence of any of the people described in (1) and (2), the System Operator is satisfied is 'otherwise an appropriate person to be the authorised representative of the individual'.¹⁰³ • Once the individual is registered for a PCEHR, and the System

¹⁰⁰ Section 6(1) of the PCEHR Act.

¹⁰¹ Section 6(2)(a) of the PCEHR Act.

¹⁰² Section 6(4)(a) of the PCEHR Act.

¹⁰³ Sections 6(2)(b) and 6(4)(b) of the PCEHR Act.

Individual participant	Role and functions
	<p>Operator is satisfied that the representative has authority to act on behalf of the individual, the authorised representative will be given the same access and controls as the individual.</p> <ul style="list-style-type: none"> • There may be more than one authorised representative for an individual. • Once an authorised representative has control over an individual's PCEHR, the individual would be unable to take personal control over their PCEHR (without first demonstrating that they had capacity¹⁰⁴). However, the authorised representative could give the individual 'read only' access to their PCEHR by making the individual a nominated representative.¹⁰⁵
nominated representatives	<ul style="list-style-type: none"> • An individual or authorised representative may nominate any other persons (such as carers and family members) to access a PCEHR. • A standard nominated representative may view the individual's PCEHR, but will not be able to manage the individual's access controls, contribute to information in an individual's PCEHR or provide consent for a healthcare provider to obtain access to the individual's PCEHR. • There are no age restrictions on nominated representatives and a minor can be a nominated representative.¹⁰⁶
full access nominated representatives	<ul style="list-style-type: none"> • An individual or authorised representative may nominate any other persons (such as carers and family members) to access and manage a PCEHR. • As well as viewing an individual's PCEHR, a full access nominated representative is able to manage certain aspects of the individual's PCEHR as if they were the individual. • There are no age restrictions on full access nominated representatives and a minor can be a nominated representative.

¹⁰⁴ Children who choose to take control over their PCEHR do not have to prove they have capacity – PCEHR Rules, rule 10.

¹⁰⁵ Con Ops, section 3.2.8 (Representatives).

¹⁰⁶ Con Ops, section 3.2.8 (Representatives).

2. Healthcare participants

Healthcare participant	Role and functions
healthcare provider organisation	<p>Healthcare provider organisations that have been allocated an HPI-O are eligible to register to participate in the PCEHR System.</p> <p>A healthcare provider organisation will have been allocated an identifier by the HI Service Operator on the basis that they are either:</p> <ul style="list-style-type: none"> • a Seed Organisation: a legal entity which provides or controls the delivery of healthcare services, which in a network of healthcare provider organisations is the principal entity in the structure; or • a Network Organisation: part of or subordinate to a Seed Organisation in a legal, business and/or administrative sense and can be used to represent different departments, sections or divisions within an organisation (e.g. departments within a hospital) or can be a separate legal entity from the Seed Organisation. <p>A network hierarchy is a connected group of healthcare provider organisations, comprising one Seed Organisation and one or more Network Organisations linked to the Seed Organisation. A network hierarchy is created and managed by the Seed Organisation in accordance with subsections 9A(3) to (7) of the HI Act.</p> <p>A healthcare provider organisation must register in the PCEHR System before its personnel can access PCEHRs in connection with the provision of healthcare to registered individuals.</p> <p>Healthcare provider organisations will access PCEHRs in accordance with the permissions attached to the organisation in its associated network hierarchy which has been assigned an 'Access Flag'. Access Flags are designed to balance reasonable consumer expectations about the sharing of health information as part of providing healthcare, and arrangements within the healthcare organisation for access to health information.¹⁰⁷</p> <p>Healthcare provider organisations will interact with the System Operator via the organisation's Responsible Officer (RO) and Organisation Maintenance Officer (OMO), who are appointed via the HI Service.</p>
healthcare provider individuals	<p>Healthcare provider individuals (i.e. clinicians, doctors, healthcare professionals) are not required to be 'registered' in the PCEHR System. However, in order to access PCEHRs via the Provider Portal, a healthcare provider individual must be registered by a registration authority as a member of a particular health profession. Healthcare provider organisations must ensure the System Operator is given information identifying individuals requesting access to PCEHRs on behalf of the healthcare provider organisation.¹⁰⁸</p>
authorised persons	<p>The PCEHR System entrusts a registered healthcare provider organisation to grant access to healthcare provider individuals and other local users who need to access the PCEHR System as part of their duties.</p>

¹⁰⁷ Rule 9 of the *PCEHR Rules 2012*.

¹⁰⁸ Section 74 of the PCEHR Act.

Healthcare participant	Role and functions
	<p>An authorised person 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 PCEHR Act, an ‘employee’ includes an individual who provides services for the entity under a contract for services or an individual whose services are made available to the entity (including services made available free of charge).</p> <p>Registered healthcare provider organisations are required to have IT systems which have user account management systems which restrict access to only those people who require access as part of their duties, uniquely identify persons using the PCEHR System and have appropriate password or other access control mechanisms for access to PCEHRs.</p>
contracted service provider	<ul style="list-style-type: none"> • A contracted service provider in the PCEHR System is an organisation that provides information technology services or health information management services in relation to the PCEHR System to a healthcare provider organisation under contract to that healthcare provider organisation. • A contracted service provider must be registered in the PCEHR System before it is able to interact with the PCEHR System on behalf of a healthcare provider organisation.
specialists	<ul style="list-style-type: none"> • The PCEHR System supports 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.

3. PCEHR System infrastructure providers/operators

PCEHR System Participant	Role and functions
System Operator	<p>The System Operator:</p> <ul style="list-style-type: none"> • is currently the Secretary of the Department of Health. • operates the PCEHR System; • supplies operational capabilities around: <ul style="list-style-type: none"> ○ the individual portal, provider portal, administration portal and the B2B gateway; ○ manages the core services and system components, such as the index service¹⁰⁹; access control mechanisms¹¹⁰; a reporting service¹¹¹; the Register¹¹²; registration of individuals and providers¹¹³; an audit service¹¹⁴; and ○ manages the National Repositories Service¹¹⁵; and ○ manages complaints in relation to the PCEHR System;¹¹⁶ • supplies the operational capabilities for the administration of the PCEHR System¹¹⁷ (e.g. service support, service delivery, infrastructure management, security management, application management, asset management and corporate services¹¹⁸); and • educates individuals and participants about the PCEHR System.¹¹⁹
HI Service Operator	<p>The HI Service Operator assigns 3 types of healthcare identifiers:</p> <ul style="list-style-type: none"> • Individual Healthcare Identifier (IHI): for individuals receiving healthcare services; • Healthcare Provider Identifier (Individual (HPI-I)): for individual healthcare providers; and • Healthcare Provider Identifier (Organisation (HPI-O)): for healthcare provider organisations such as a hospitals and clinics where healthcare is given. <p>Chief Executive Medicare is the service operator of the Healthcare Identifiers Service. This role is separate to Medicare's funding and claiming services.</p>
Department of Human Services (DHS)	<p>Access to the PCEHR System (by individuals and other participants) via the phone, face to face and mail channel is delivered by DHS customer service operators acting as delegate of the System Operator. The System Operator retains overall responsibility for all PCEHR</p>

¹⁰⁹ Section 15(a) of the PCEHR Act.

¹¹⁰ Section 15(b) of the PCEHR Act.

¹¹¹ Section 15(d) of the PCEHR Act.

¹¹² Sections 15(e) and 56 of the PCEHR Act

¹¹³ Section 15(f) of the PCEHR Act.

¹¹⁴ Section 15(g) of the PCEHR Act.

¹¹⁵ Section 15(i) of the PCEHR Act.

¹¹⁶ Section 15(j) of the PCEHR Act.

¹¹⁷ Section 15(k) of the PCEHR Act.

¹¹⁸ Con Ops, section 7.3 (System Operator).

¹¹⁹ Section 15(m) of the PCEHR Act.

PCEHR System Participant	Role and functions
	functions.
National Infrastructure Operator (NIO)	The principal information technology infrastructure for the PCEHR System is supplied and operated by Accenture on behalf of (and as a contracted service provider to) the System Operator. The System Operator retains overall responsibility for all PCEHR functions.
National Repository Service Provider	<p>The National Repositories Service stores a minimum critical set of health information about participating individuals. 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; • Discharge Summaries; • Specialist Letters; • Personal Health Summary; and • Consumer Notes.¹²⁰ <p>The National Repositories Service is managed by the System Operator.</p>
registered repository operators	<p>In addition to the National Repositories Service, the PCEHR System has the capability to connect to other repositories operated by registered repository operators. Repository operators have an obligation upon having registration cancelled (i.e. the repository shutting down) not to transfer or dispose of health records held by the repository operator for PCEHR purposes without the prior written approval of the System Operator.</p> <p>The System Operator has registered Chief Executive Medicare as a repository operator. As a registered repository operator, Chief Executive Medicare has made available to the PCEHR System Medicare and DVA claims history, PBS/RPBS history, organ donor information and childhood immunisation information.¹²¹ Individuals may choose whether or not to have this information included in their PCEHR.</p> <p>Examples of other repository operators which may be registered by the System Operator in the future include:</p> <ul style="list-style-type: none"> • Pathology service repositories holding pathology result reports; and • Regional or State/Territory operated repositories.¹²²
registered portal operators	The System Operator can register an entity to operate a portal (an electronic interface) to facilitate access to the PCEHR System. Currently, all portals for the PCEHR System (the Provider Portal,

¹²⁰ Con Ops, section 6.6.1 (National Repositories Service).

¹²¹ See section 38 of the PCEHR Act.

¹²² Con Ops, section 6.6.2 (Conformant Repositories).

PCEHR System Participant	Role and functions
	Consumer Portal and Admin Portal) are operated by the System Operator.

Schedule 5 – Sources of information

1. Publicly available information

- (a) Deloitte, *Review of the Personally Controlled Electronic Health Record* (December 2013), available at [http://health.gov.au/internet/main/publishing.nsf/Content/46FEA5D1ED0660F2CA257CE40017FF7B/\\$File/FINAL-Review-of-PCEHR-December-2013.pdf](http://health.gov.au/internet/main/publishing.nsf/Content/46FEA5D1ED0660F2CA257CE40017FF7B/$File/FINAL-Review-of-PCEHR-December-2013.pdf)
- (b) [eHealth website](http://www.ehealth.gov.au/), available at <http://www.ehealth.gov.au/>, including the eHealth Registration Booklet titled '[Connecting your healthcare: a guide to registering for an eHealth record](http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/Content/resources/$File/registration_booklet_low_res.pdf)', available at [http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/Content/resources/\\$File/registration_booklet_low_res.pdf](http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/Content/resources/$File/registration_booklet_low_res.pdf).
- (c) [Healthcare Identifiers Service - Application to create, verify or merge an Individual Healthcare Identifier form \(2888\)](http://www.humanservices.gov.au/customer/forms/2888), available at <http://www.humanservices.gov.au/customer/forms/2888>.
- (d) [Medicare enrolment application form \(3101\)](http://www.humanservices.gov.au/customer/forms/3101), available at <http://www.humanservices.gov.au/customer/forms/3101>

2. Information provided by the Department of Health

- (a) Meetings (in person or via telephone) with the Department of Health, held on 2, 3, 10, 11 and 16 December 2014, 23 April 2015 and 13 May 2015.
- (b) Comments provided by the Department:
 - (i) in relation to draft information flows, provided 10 and 18 December 2014;
 - (ii) in relation to the draft PIA report, version 1, provided 16 December 2014;
 - (iii) in relation to the draft PIA report, version 2, provided 17 April 2015;
 - (iv) in relation to the draft PIA report, version 3, provided 12 May 2015; and
 - (v) in relation to the draft PIA report, version 4, provided 19 May 2015.
- (c) Deloitte, *Department of Health Report on the public consultation into the Review of the PCEHR* (draft, 26 September 2014), and submissions received by Deloitte in relation to the preparation of the report.
- (d) Department of Health, *Online Opt-Out Portal Information Flow* (4th ed; 16 December 2014), including the Visio information flow diagram.
- (e) Department of Health, *Initial drafting instructions for amendments to the PCEHR Act and HI Act* (28 November 2014)
- (f) Department of Health, *Evidence of Identity (EOI) for the Personally Controlled Electronic Health (PCEHR) System* (19 June 2014)
- (g) Department of Health, *Public Awareness Campaign project – summary of key stages* (provided 26 November 2014)
- (h) Office of the Australian Information Commissioner, Memorandum: Discussion of potential privacy risks under an opt-out eHealth record system (21 June 2014)

- (i) Screenshots of registration process and PCEHR system, provided 1 December 2014

3. Legislation

- (a) *Healthcare Identifiers Act 2010* (Cth)
- (b) *Personally Controlled Electronic Health Records Act 2012* (Cth)
- (c) *Privacy Act 1988* (Cth)

Schedule 6 – Summary of the APPs

1. Collection of personal information

1.1 Anonymity and pseudonymity

- (a) Wherever it is lawful and practicable in the circumstances, APP 2 requires Commonwealth agencies to give individuals the option of interacting anonymously or by using a pseudonym.

1.2 Collection necessity

- (a) APP 3.1 requires Commonwealth agencies to collect personal information only where it is necessary for, or directly related to, a purpose that is directly related to a function or activity of the agency.

1.3 Collection methods – lawful, fair and not intrusive

- (a) APP 3.5 requires Commonwealth agencies to only collect personal information by lawful and fair means.

1.4 Collecting sensitive personal information

- (a) APPs 3.3 and 3.4 limit the circumstances in which Commonwealth agencies can collect sensitive information. Some of the permitted collections include where the individual has given consent, where collection is required or authorised by or under an Australian law, or (where it is unreasonable or impracticable to obtain the individual's consent) the collection is necessary to lessen or prevent a serious threat to the life, health or safety of an individual.

1.5 Direct collection

- (a) APP 3.6 requires Commonwealth agencies to collect personal information about an individual from that person unless:
 - (i) the individual consents to the agency collecting the information from a third party;
 - (ii) the agency is required or authorised by or under an Australian law to collect the information from a third party; or
 - (iii) it is unreasonable or impracticable to collect the information directly from the individual.

1.6 Collection transparency and choice (notification, options)

- (a) APP 5 requires agencies, when collecting personal information about an individual, to take such steps as are reasonable in the circumstances to ensure that the individual is aware of a number of matters, which include the following:
 - (i) the purposes for which their information is being collected;
 - (ii) whether the collection is authorised or required by law;
 - (iii) if the agency collects, or has collected, personal information from a third party, the fact that the agency so collects or has collected the information, and the circumstances of the collection; and
 - (iv) any third parties to whom it is the agency's usual practice to disclose that information.

2. Use and disclosure

2.1 Use and disclosure of personal information

- (a) APP 6 imposes limitations around the use and disclosure of personal information for a purpose other than the purpose for which the information was collected in the first place. There are also additional restrictions in relation to the use and disclosure of 'sensitive information'.

2.2 Use and disclosure of unique identifiers

- (a) APP 7 limits the collection and use of government-issued identifiers by private sector organisations. There are no limitations under the APPs in relation to the collection, use or disclosure of government-related identifiers by agencies.

2.3 Cross-border disclosures

- (a) APP 8 imposes additional restrictions in relation to the disclosure of personal information to an overseas recipient.

3. Data quality

- (a) APP 10 requires agencies to take reasonable steps (if any) to ensure that:
 - (i) the information they collect is relevant to the purpose of collection, and is up to date and complete; and
 - (ii) the information is accurate prior to using or disclosing it.

4. Data security

- (a) APP 11 requires Commonwealth agencies to take reasonable security safeguards to ensure that the information they hold is protected against loss, unauthorised access, use, modification or disclosure, and against other misuse.

5. Access and correction

- (a) APP 12 requires agencies to provide individuals with access to their own personal information, unless an exception applies (for example, the agency is required or authorised to refuse access under another Commonwealth law that provides for access to documents, such as the *Freedom of Information Act 1982* (Cth)).
- (b) APP 13 requires agencies to take reasonable steps to correct any personal information they hold to ensure it is accurate, relevant, up to date, complete and not misleading.

Schedule 7 – Glossary and acronyms

Term	Definition
2011 PIA	Minter Ellison and Salinger Privacy, Privacy Impact Assessment Report: Personally Controlled Electronic Health Records (PCEHR) (15 November 2011), available at http://ehealth.gov.au/internet/ehealth/publishing.nsf/content/pcehr-legals-pia-toc .
Access List	a list of participating healthcare provider organisations that have accessed an individual's PCEHR, excluding those organisations 'removed' by the individual. Each organisation is assigned a level of access for the PCEHR: 'general access', 'limited access' or 'revoked'.
ACIR	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.
Admin Portal	a portal to enable customer service officers working in one of the channels (e.g. Call Centre, DHS - Medicare shop front) to process registrations of individuals and authorised representatives and help individuals manage their PCEHR.
ALRC	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	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	the Australian Privacy Principles, set out in Schedule 1 of the Privacy Act.
authentication	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	has the meaning given by section 6 (Definition of authorised representative of an individual) of the PCEHR Act.
Authorised User	a person authorised by a participating healthcare provider organisation to access the PCEHR System on behalf of the organisation.
Automatic Registrant	a person who will be automatically registered for a PCEHR because they did not opt-out during the Opt-Out Period, and do not have an existing or cancelled PCEHR.
Call Centre	the DHS call centre staffed by DHS customer service operators, contactable by calling 1800 723 471.

Term	Definition
Con Ops	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).
Consumer Registration Booklet	Department of Health, Connecting your healthcare: a guide to registering for an eHealth record (Health Registration Booklet), available in-store at a DHS Service Centre, by calling the Call Centre, or online at http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/application_methods .
Contracted Service Provider (CSP)	an entity that provides: (a) information technology services relating to the PCEHR system; or (b) health information management services relating to the PCEHR system; to a healthcare provider organisation under a contract with the healthcare provider organisation.
Department	the Department of Health.
Dependant	an individual who is represented by an authorised representative in the PCEHR System because they are under 18 years of age or are not capable of making decisions for themselves.
DHS	the Department of Human Services (Commonwealth) and includes the Centrelink, Child Support and Medicare programs.
DHS Service Centre	a Department of Human Services service centre which offers Medicare services.
Discharge Summary	a record that can be used when an individual is discharged from a healthcare provider organisation. 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.
DVA	the Department of Veterans' Affairs.
DVS	the Document Verification Service operated by the Attorney-General's Department.
employee	of an entity includes, but is not limited to, the following: (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	Evidence of Identity.

Term	Definition
Event Summary	<p>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 organisation 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.</p> <p>An event summary is intended to be the 'default' record type and is used when none of the other types of record are appropriate.</p>
full access nominated representative	a nominated representative who has been granted 'Full Access' by a registered individual. Full access nominated representatives are able to view the entire PCEHR of the individual, and also manage certain aspects of the individual's PCEHR as if they were the individual.
health information	<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>
healthcare	<p>(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:</p> <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 <p>(b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.</p> <p>Note: This is the definition used in the PCEHR Act which is the same definition used in the Privacy Act for health service.</p>
healthcare provider	<p>(a) an individual healthcare provider; or</p> <p>(b) a healthcare provider organisation.</p>
healthcare provider organisation	means an entity that has conducted, conducts, or will conduct, an enterprise that provides healthcare (including healthcare provided free of charge).
HI	healthcare identifier.

Term	Definition
HI Act	<i>Healthcare Identifiers Act 2010 (Cth).</i>
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	the HI Service Operator (Chief Executive Medicare) acting through delegated officers of DHS.
HPI-I	a 16 digit unique number assigned to healthcare provider individuals, which is used to identify the individual providers who deliver healthcare in the Australian healthcare setting.
HPI-O	a 16 digit unique number assigned to healthcare provider organisations, which is used to identify the organisations who deliver care in the Australian healthcare setting.
IHI	a 16 digit unique number assigned to members of the public, which is used to identify individuals who receive care in the Australian health system. There are five types of IHI status: active, deceased, retired, expired and resolved. There are three types of IHI record status: verified, unverified and provisional. ¹²³
index service	the index service maintained by the System Operator for the purposes of the PCEHR system, as mentioned in section 15(a) (Functions of the System Operator) of the PCEHR Act.
individual	an individual who has received, receives or may receive healthcare.
LDAC (Limited Document Access Code)	a code an individual can create and provide to a healthcare provider organisation in order to grant the organisation access to 'Restricted Access' records within the individual's PCEHR.
MBS	Medicare Benefits Schedule.
Medicare	the Chief Executive Medicare acting through delegated officers of DHS performing Medicare-related functions under the National Health Act and Health Insurance Act.
National Repositories Service	the service referred to in section 15(i) of the PCEHR Act.
NEHTA	National E-Health Transition Authority.
NIO	National Infrastructure Operator.
nominated representative	of an individual means an individual who has agreed with the individual to be the individual's nominated representative for the purposes of the individual's PCEHR.
OAIC	the Office of the Australian Information Commissioner.
OMO	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.

¹²³ NEHTA, *Healthcare Identifiers Service User Guide for Practice Managers*, 2011, p. 8.

Term	Definition
Online Opt-Out Service	the online service to be used during the Opt-Out Period for individuals to be able to indicate that they do not want to be registered for a PCEHR.
Opt-Out Period	the period during which individuals can opt-out of automatic registration for a PCEHR.
participant in the PCEHR system	any of the following: (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.
PBS	an Australian Government scheme aimed at providing all Australians with affordable access to a wide range of prescription medicines.
PCEHR	a personally controlled electronic health record, being the record of information that is created and maintained by the System Operator in relation to the individual, and information that can be obtained by means of that record, including, but not limited to, the following: (a) information included in the entry in the Register that relates to the individual; (b) health information connected in the PCEHR System to the individual (including information included in a record accessible through the index service); (c) other information connected in the PCEHR system to the individual, such as information relating to auditing access to the record.
PCEHR Identity	an identity created in the PCEHR System, which consists of the individual's full name, sex, address, date of birth, IHI, IHI status and IHI record status. A PCEHR Identity is separate from a PCEHR. A person who is an authorised representative but is not themselves registered will still have a PCEHR Identity.
PCEHR Privacy Policy	the privacy policy relating to the PCEHR System, available at a DHS Service Centre, by calling the Call Centre, or online at http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/Content/ehealth_privacy .
PCEHR Review Report	the report titled Review of the Personally Controlled Electronic Health Record, dated December 2013.
Personal Health Note	a note provided as a memory aid for individuals and their representatives and are not visible to healthcare providers.

Term	Definition
Personal Health Summary	summary information that an individual wishes to share with their healthcare providers via their PCEHR. The Personal 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).
RAC (Record Access Code)	a code that an individual can create and provide to a healthcare provider organisation in order to have the organisation added to the individual's Access List.
record	includes a database, register, file or document that contains information in any form (including in electronic form).
registered healthcare provider organisation	a healthcare provider organisation that is registered under section 44 of the PCEHR Act.
registered portal operator	a person that: <ol style="list-style-type: none"> is the operator of an electronic interface that facilitates access to other parts of the PCEHR system; and is registered as a portal operator under section 49 of the PCEHR Act.
registered repository operator	a person that: <ol style="list-style-type: none"> holds, or can hold, records of information included in personally controlled electronic health records for the purposes of the PCEHR system; and is registered as a repository operator under section 49 of the PCEHR Act.
registration	the processes associated with the creation by an individual of their PCEHR. Registration includes processes covering verification of identity and evidence of entitlement (i.e. meeting the criteria for participation, such as having an IHI).
report	data extracted from one or more records from one or more PCEHRs for reporting purposes.
RPBS	Repatriation Pharmaceutical Benefits Scheme.
shared health summary	a record that is: <ol style="list-style-type: none"> prepared by the individual's nominated healthcare provider; and described by the individual's nominated healthcare provider as the individual's shared health summary.
Specialist Letter	includes a record created by a specialist. The PCEHR System supports 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 sent to the PCEHR System.
System Operator	has the meaning given by section 14 of the PCEHR Act.
System Operator (DHS)	the System Operator acting through DHS officers, who have been subdelegated by the Chief Executive Medicare.

Term	Definition
System Operator (Health)	the System Operator acting through delegated officers of the Department of Health.
System Operator (NIO)	the System Operator acting through NIO as its contracted service provider.
Transition Period	the period during which Automatic Registrants can access their PCEHR and set access controls before any healthcare provider access occurs.

About the authors

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, Hong Kong, the People's Republic of China, Mongolia, New Zealand and the United Kingdom. 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.

Minter Ellison has undertaken a range of PIAs for the Australian Government, including the Personally Controlled e-Health Record, the National Disability Insurance Scheme, the Unique Student Identifier initiative, and a number of PIAs regarding the functionality of online government services such as those offered through myGov.

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.