Personally controlled electronic health record (eHealth record) system

eHealth record System Operator

Audit report
Information Privacy Principles audit
Section 27(1)(h) Privacy Act 1988

Audit undertaken: July 2013
Draft report issued: December 2013
Final report issued: August 2014
Content

Part 1 — Introduction ........................................................................................................................................... 1
Background ..................................................................................................................................................... 1

Part 2 — Description of audit ........................................................................................................................... 3
Purpose and objective ..................................................................................................................................... 3
Scope ............................................................................................................................................................ 3
Information obtained during the audit ............................................................................................................. 4
Timing and location ......................................................................................................................................... 5
Opinion ............................................................................................................................................................ 5
Reporting ........................................................................................................................................................ 6

Part 3 — Audit issues IPP 1 ............................................................................................................................... 7
Lawfulness of the purpose of collection and necessity of collection ............................................................... 7
Fairness and lawfulness of the means of collection ........................................................................................ 10

Part 4 — Audit issues IPP 2 ............................................................................................................................. 15
Substance of notifications ............................................................................................................................... 15
Training material .......................................................................................................................................... 20
Timing of notice .............................................................................................................................................. 21
Manner of notification .................................................................................................................................. 22

Part 5 — Audit issues IPP 3 ............................................................................................................................. 25
Relevance, currency and completeness .......................................................................................................... 25
Intrude on personal affairs ............................................................................................................................ 27

Part 6 — Recommendations and auditee response to recommendations ...................................................... 28
Appendix A — Overview of eHealth record registration processes ............................................................ 31
Appendix B — summary of IPP 2 notices by registration channel ............................................................... 36
Part 1 — Introduction

Background

1.1 The personally controlled electronic health record system (eHealth record system) commenced operation on 1 July 2012. The system was established and is specifically regulated under the *Personally Controlled Electronic Health Records Act 2012* (Cth) (PCEHR Act), the *PCEHR Rules 2012* (Cth) (PCEHR Rules) and the *Personally Controlled Electronic Health Records Regulation 2012* (Cth). The *PCEHR (Assisted Registration Rules) 2012* (Cth) (Assisted Registration Rules) create additional rules for healthcare provider organisations that conduct ‘assisted registration’.

1.2 The eHealth record System Operator (System Operator), currently the Secretary of the Department of Health (Health), is responsible for the operation of the system. The Secretary’s role is set out under s 15 of the PCEHR Act and is broadly to establish and run the eHealth record program within legislative constraints; develop policy and legislation; register consumers and other participants in the system; and manage uptake, complaints, systemic issues, performance reporting, system integrity and strategic direction. The System Operator has delegated her functions and powers under the PCEHR Act to departmental staff, under an Instrument of Delegation.

1.3 Under delegation by the System Operator and an eHealth Business Partnership funding agreement, the Department of Human Services (DHS) manages contact with consumers on behalf of the System Operator.

1.4 DHS provides the contact centre capabilities and supporting infrastructure for consumer registrations via the phone, in-person, in-writing and online channels, and for enquiries and complaints. DHS also provides access to Medicare and Department of Veterans Affairs (DVA) data, including this information in the eHealth records of consumers with their consent.

1.5 The Office of the Australian Information Commissioner (OAIC) regulates the handling of personal information under the eHealth record system by individuals, Australian Government agencies, private sector organisations and some state and territory agencies (in particular circumstances). The OAIC’s functions include investigating privacy complaints from individuals, conducting investigations on the Commissioner’s own initiative, taking enforcement action where appropriate, providing advice and guidance material for eHealth record system participants, conducting audits/assessments, and receiving data breach notifications.

1.6 Under a Memorandum of Understanding with Health, the OAIC committed to undertaking up to two privacy audits of the System Operator during the period from 29 November 2012 to 30 June 2014. This report relates to the OAIC’s first audit of the System Operator.

1.7 The OAIC audited the System Operator’s policies and procedures relating to the collection of personal information during the eHealth record consumer registration
process. At the time of the audit, registrations were the area where the most activity and personal information handling was taking place in the eHealth record system. The registration process is the consumer’s first engagement with the system and is central to the notification and consent process.
Part 2 — Description of audit

Purpose and objective

2.1 The purpose of this audit was to assess whether the System Operator’s policies and procedures provide a documentary framework to allow it to maintain personal information in accordance with its obligations under Information Privacy Principles (IPPs) 1 to 3.

2.2 The three main audit objectives were to determine whether the System Operator’s policies and procedures were consistent with:

- IPP 1 requirements (manner and purpose of collection of personal information) for the collection of personal information during the registration processes
- IPP 2 requirements (collection of personal information from the individual concerned) for notice provided to consumers during the registration processes about the collection of their personal information, and the form and content of those notices
- IPP 3 requirements (solicitation of personal information, including from third parties) for the collection of personal information during the registration processes.

2.3 The audit was conducted pursuant to s 27(1)(h) of the Privacy Act 1988 (Cth) (Privacy Act), which states that a function of the Australian Information Commissioner (Commissioner) is to ‘...conduct audits of records of personal information maintained by agencies for the purpose of ascertaining whether the records are maintained according to the Information Privacy Principles.’

Scope

2.4 There are five different ways a consumer can register for an eHealth record:

- online at www.ehealth.gov.au, via a consumer portal using a my.gov.au¹ account
- by phone (1800 723 471)
- in-person, by visiting a DHS service centre offering Medicare services
- in writing, by completing an application form (available at www.ehealth.gov.au)
- through an ‘assisted registration’ process, where an authorised employee of a registered healthcare provider organisation assists a consumer to register.

A detailed description of the auditors’ understanding of each registration process is contained in Appendix A to this report.

¹ The documentation provided during the audit refers to www.australia.gov.au and australia.gov.au accounts. The auditors understand that the australia.gov.au account has been replaced with myGov accounts accessed at https://my.gov.au and so have referred to myGov accounts in this report.
2.5 The auditors considered:

- the System Operator’s policies and procedures at the time of the audit for the collection of personal information during consumer registrations conducted:
  - online
  - by phone
  - in-writing
  - in-person at a DHS service centre offering Medicare services.
- the System Operator’s processes for collecting personal information obtained using the assisted registration procedure, and the material produced by the System Operator to guide and regulate healthcare provider organisations’ collection of personal information via assisted registration.

2.6 The audit was confined to a review of the documentation received by the auditors from the System Operator. The auditors did not examine:

- how the documented policies and procedures had been implemented
- the registration processes for a consumer’s authorised representatives and nominated representatives.

2.7 The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) (Privacy Amendment Act) introduced significant changes to the Privacy Act on 12 March 2014. The Privacy Amendment Act includes a set of 13 new Australian Privacy Principles (APPs) which will regulate the handling of personal information by both Australian Government agencies and organisations. The APPs will replace the existing IPPs and National Privacy Principles (NPPs). As the APPs had not commenced when this audit was conducted, the System Operator was assessed against the IPPs. However, the auditors were mindful of the APPs when making recommendations, and have included some relevant comments.

**Information obtained during the audit**

2.8 The auditors obtained numerous documents from the System Operator during the audit. The auditors received documents in the following categories:

- general context of the eHealth record system, including:
  - delegation instruments
  - documents outlining the nature of arrangements between Health and DHS
  - a privacy impact assessment conducted before the eHealth record system commenced
  - details of some privacy complaints and feedback received by the System Operator in relation to registration processes to assist the targeting of our document review
- registration process documentation, including:
o policies and procedures in relation to each registration process conducted by the System Operator
o documents and guidance material developed by the System Operator in relation to the assisted registration process

• the System Operator’s staff resources, including:
  o policies and procedures available to staff
  o internal training material for staff

• consumer information, including:
  o forms used to collect personal information during the registration process
  o screen shots from the online registration process
  o notices and instructions provided to consumers in each registration process
  o the System Operator’s privacy statement.

Timing and location

2.9 The auditors conducted the fieldwork component of the audit (document review) from 3 to 5 July 2013 at the OAIC’s Sydney office.

Opinion

2.10 The auditors are of the opinion that the System Operator’s policies and procedures generally provide a documentary framework to allow it to maintain personal information in accordance with its IPP 1 to 3 obligations in relation to online registration, phone registration, in-writing registration and in-person registration at DHS service centres.

2.11 However, the auditors are of the opinion that the System Operator’s policies and procedures in relation to assisted registration, particularly non point-of-care assisted registration, do not provide a sufficient documentary framework to support it in maintaining personal information in accordance with its IPP 1 to 3 obligations.

2.12 The OAIC may provide recommendations in relation to issues it identifies during its audit. A recommendation is a suggested course of action or a control measure that, if put in place by the agency, will (in the opinion of the OAIC) minimise the risks identified around how personal information is handled against the requirements of IPP 1 to 3.

2.13 The auditors identified a number of privacy risks and have made 13 recommendations. A large number of the risks and recommendations relate to assisted registration policies and procedures (six recommendations: 2–5, 11 and 13).

2.14 Although a lower privacy risk, the recommendations also show a theme of inconsistent documentation and collection of information across the different registration channels (seven recommendations: 1, 6-10 and 12).
2.15 The OAIC will consider with the System Operator the possibility of conducting a follow up audit of the implementation of the recommendations in this audit by the System Operator.

**Reporting**

2.16 To the extent possible, the OAIC publishes final audit reports in full or in an abridged version on its website [www.oaic.gov.au](http://www.oaic.gov.au). It is sometimes inappropriate to publish all or part of a report of because of statutory secrecy provisions or for reasons of privacy, confidentiality or privilege.
Part 3 — Audit issues IPP 1

3.1 The full text of the IPPs is available at www.oaic.gov.au.

IPP 1 issues — Manner and purpose of collection of personal information:

IPP 1.1 provides that personal information shall not be collected unless the collection is for a lawful purpose directly related to the collector’s functions or activities, and necessary for or directly related to that purpose.

IPP 1.2 provides that personal information must not be collected by unlawful or unfair means.

Lawfulness of the purpose of collection and necessity of collection

Observations — lawfulness

3.2 The auditors reviewed the System Operator’s functions and activities in relation to consumer registration outlined under the PCEHR Act and its legal authority to collect personal information under that Act.

3.3 As part of the auditors’ review of the System Operator’s functions and activities, the auditors examined the Business Partnership Agreement between the Secretaries of Health and DHS. This Agreement set out the broad objectives of the eHealth program, obligations of both parties, and the business arrangements between Health and DHS.

3.4 The auditors also viewed the System Operator’s Instrument of Delegation, delegating the System Operator’s functions and powers under the PCEHR Act and PCEHR Rules to Health staff and to the Chief Executive of Medicare, DHS.

3.5 Under s 39 of the PCEHR Act, a consumer may apply to the System Operator to register for an eHealth record, using an approved form and supplying the required documents. Section 40 of the Act requires the consumer to provide the System Operator with their:

- full name
- date of birth
- individual healthcare identifier
- Medicare card number or DVA file number
- sex. ²

2 Section 40 of the Act allows other required information to be prescribed by the regulations; however, no further categories of information have been prescribed at this time.
3.6 Section 41 of the Act requires the System Operator to register eligible consumers on application if the System Operator is satisfied that the consumer’s identity has been appropriately verified.

**Observations — necessity**

3.7 The auditors reviewed all forms and written procedures used to guide the collection of personal information through each registration channel. This included:

- paper forms for in-writing registration and assisted registration
- screen shots of the online registration process
- procedural documents and training materials identifying the information collected through the phone, in-person and assisted registration channels.

3.8 The auditors observed that the fields in the paper forms and online screens, and the DHS call centre and in-person collection processes solicited specific personal information. The fields had been appropriately designed in such a way that would prevent the System Operator from collecting additional unnecessary information.

3.9 The auditors also saw that the in-person collection processes and Assisted Registration: A guide for healthcare provider organisations, January 2013 (Guide) required the System Operator’s staff and healthcare providers conducting assisted registration respectively, to simply sight identity documents, rather than collecting copies. This would appropriately help prevent the collection of unnecessary identity information.

**Privacy issues — general**

3.10 The auditors found no privacy issues in terms of the lawfulness of the collection of personal information by the System Operator.

3.11 Overall, it appeared that the majority of information collected through each of the registration processes was necessary for the System Operator to perform its functions and activities.

3.12 However, the auditors did note some inconsistency in the information collected through each of the registration processes.

**Privacy issues — Inconsistency in information collected for identity verification purposes**

3.13 There was some variation in the information collected for identity verification purposes in each of the processes. For example:

- consumers who registered online, by telephone and in-person needed to provide their full residential address, whereas the in-writing and assisted registration application forms did not request this, instead requiring the consumer’s email address and contact phone numbers (although in the case of the assisted registration form, providing this information was optional)
• the in-writing application form gave the consumer the option of providing their Medicare number, DVA number or individual healthcare identifier. The assisted registration, telephone and in-person processes gave the option of providing their Medicare or DVA number. The online process only gave the option of providing their Medicare number. Section 40 of the PCEHR Act allows the consumer to provide any of these identifiers and, we understand, any of these identifiers will be accepted if offered although this is not clear to the consumer.

• the in-writing, call centre, and in-person processes required the consumer to give their full name, whereas the online and assisted registration forms asked for their first name and surname only. Section 40 of the PCEHR Act requires the consumer to provide their ‘full name’

• the in-writing, phone and in-person and assisted registration processes required the consumer’s sex, whereas the online process did not. This information is required under s 40 of the PCEHR Act.

• there were also differences in the proof of identity documents required under the different registration processes.

3.14 The auditors acknowledge that some differences may be warranted due to the different nature of each registration process, particularly in relation to the proof of identity documents that may be needed. The auditors also appreciate that there may need to be some flexibility in identity verification processes, to enable the System Operator to perform its registration functions and activities effectively.

3.15 However, the auditors consider there is a risk that some of this variation may be unwarranted because the information is inconsistent with, or additional to, what is required to be collected under the PCEHR Act. For example, where the consumer is not required to provide identity information under the PCEHR Act, such as a residential address, and that information is collected inconsistently across the different registration methods, there is the risk that collecting that information is not necessary or directly related to the relevant purpose, as required under IPP 1.1.

Privacy issues — Inconsistency in information collected for non-identity verification purposes

3.16 There were some inconsistencies in the other information the System Operator collected for non-identity verification purposes. For example:

• some of the processes (such as online registrations) asked the consumer to voluntarily supply their Indigenous status, some did not (such as in-writing registrations), and some specifically instructed DHS staff not to record this (streamlined in-person registrations)

• some of the processes (such as phone registrations) asked the consumer to provide an emergency contact; others (such as in-writing registrations) did not give this option.

---

3 Training module MCA00682B p11.
• some of the processes (such as in-writing registrations) asked the consumer whether they had previously been registered; others (such as online registrations) did not.

3.17 It was not evident from the System Operator’s privacy notices, policies or procedures why there were these differences in the information collected for non-identity verification purposes. Where personal information is collected inconsistently, this raises a question as to whether additional personal information collected via some channels and not others are necessary collections. Unless there is a sound basis for this, there is the risk that collecting that information is not necessary or directly related to the relevant purpose, as required under IPP 1.1.

3.18 These matters give rise to a similar risk that the information collected is not relevant to that purpose or that the information collected is not complete, as required under IPP 3 (see part 5).

Recommendation 1 — Review information collected

3.19 It is recommended that the System Operator review the types of information collected through each of the registration processes (particularly examining inconsistent collections), to ensure that it is satisfied that each item of personal information collected is necessary for, or directly related to, its registration functions and activities, as required under IPP 1.1.

Fairness and lawfulness of the means of collection

Observations

3.20 The eHealth record system is voluntary\(^4\) and consumers must opt-in by registering. This approach requires consumers to provide consent before enrolling in the system.

3.21 The System Operator allows consumers to apply to register for an eHealth record under a pseudonym. The auditors noted that making pseudonym records available was good privacy practice and consistent with future obligations for Australian Government agencies under APP 2. From March 2014, APP 2 will require the System Operator to give individuals the option of not identifying themselves or of using a pseudonym where this is lawful and practicable.

3.22 The System Operator has given consumers the option to register with the assistance of a registered healthcare provider organisation. The Guide says that this process was developed so that patients can register for an eHealth record with support and guidance from those healthcare provider organisations involved in their care and whose guidance they trust.

3.23 The Guide states (pp3–4) that ‘…the benefits of an eHealth record will be most significant for patients who need to share information with different providers or who have complex conditions. This might include those with chronic conditions, mothers

\(^4\) Section 3 of the PCEHR Act.
and newborns, Aboriginal and Torres Strait Islander peoples, people with a disability, and older Australians.’

3.24 The OAIC’s Plain English Guidelines to Information Privacy Principles 1-3 provide in relation to IPP 1.2, that unfairness can include misleading the person into giving the information or putting the person under too much pressure to provide the information. The requirements under the Privacy Act, together with the PCEHR legislative framework which requires a consumer to consent to information being uploaded into the eHealth record system in order to be registered, are important controls that safeguard against collection of personal information by unfair means.

3.25 The auditors considered the collection processes in relation to online registration, phone registration, in-writing registration and in-person registration at a DHS service centre contain sufficient controls by virtue of the process and within the documentary framework to ensure that the means of collecting personal information through these processes would generally be fair.

3.26 However the auditors consider that further enhancements could be made to strengthen the policies and procedures used for assisted registration to mitigate against any risk of unfair collection in the assisted registration context. This is described below.

**Privacy issues — policies and procedures for assisted registrations**

3.27 The auditors distinguished between:

- assisted registrations conducted by healthcare providers for their own patients at the point-of-care

- assisted registrations conducted by healthcare provider organisations (whether or not contracted by the System Operator) for members of the general public at non point-of-care locations or when the organisation is not caring for that patient.

3.28 The Guide is a well-crafted document prepared by the System Operator. It sets out the policies and procedures point-of-care healthcare providers must develop when conducting assisted registrations. The Guide does not provide any guidance regarding fairness of collection or the extra care that may need to be taken when registering vulnerable people to ensure adequate notice and consent.

3.29 The auditors consider that providing this guidance is an important control measure to help ensure that information is collected fairly. This is particularly the case where the assisted registration process may be used to assist more vulnerable members of the community to obtain an eHealth record. By not doing so, Health is leaving itself open to a risk that the HPOs will not consider this issue fully when conducting assisted registrations.

---


6 Assisted registrations are described under Assisted registration in Appendix A.
3.30 The Guide provides for assisted registration to occur in hospital emergency departments. As individuals and their associates may be especially vulnerable when accessing emergency health services, a clear statement in the Guide that the training to be provided to employees should include training on providing notice and obtaining informed consent in those circumstances, would help to mitigate against the risk that such registration is considered to be unfair or unreasonably intrusive.

3.31 In general the System Operator could improve the Guide by dedicating a section to explaining the need for the means of collection to be fair. The section could provide examples of behaviour that allows for a fair means of collection and outline behaviours that would make the means of collection unfair. For example, providing people with insufficient time to consider and fill out forms or misleading consumers as to the purpose of registration are examples of behaviour that could be included to indicate how personal information may be collected by unfair means. An example of behaviour that unreasonably intrudes on the personal affairs of consumers would assist in relation to IPP 3, which is discussed later.

3.32 In addition, the Guide does not mention that the healthcare provider is obliged under the Assisted Registration Rules\(^7\) to inform the consumer of alternative registration methods. For example there is no reference to this in the registration process flowcharts. The assisted registration application form and assisted registration ‘Essential Information’ brochure do appropriately inform the consumer of alternative registration methods.

3.33 The Guide could advise healthcare providers that they should also verbally inform the consumer of this (particularly given that they may complete the form on behalf of consumers who have limited English skills or a disability and may not be able to read about the alternative registration options).

**Recommendation 2 — Guidance on fairness**

3.34 It is recommended that the System Operator amend the Guide to state that all collections should be conducted in a fair manner. To assist in this, the Guide could:

- provide guidance regarding the extra care that may need to be taken when registering vulnerable people, to ensure that information is collected fairly
- include examples of behaviours that unreasonably intrude on the personal affairs of an individual.

**Recommendation 3 — Alternative registration methods**

3.35 It is recommended that the System Operator amend the Guide to inform healthcare provider organisations that they are obliged under the Assisted Registration Rules to inform the consumer of alternative registration methods. This could be mentioned, for example, in the registration process flowcharts.

---

\(^7\) PCEHR (Assisted Registration) Rules 2012.
Privacy issues — policies and procedures for non point-of-care assisted registrations — s 95B and related matters

3.36 The System Operator has subcontracted at least one third party healthcare provider organisation (the third party subcontractor) to administer registrations via the assisted registration process.  

3.37 The System Operator has also engaged Medicare Locals to support the adoption of the eHealth record system. Medicare Locals have been facilitating assisted registrations.

3.38 Section 95B of the Privacy Act requires agencies entering into Commonwealth contracts to take contractual measures to ensure the contracted service provider does not do an act, or engage in a practice, that would breach an IPP if it were done or engaged in by the agency. Section 95B also requires agencies to take contractual measures to ensure that such an act or practice is not authorised by a subcontract.

3.39 The auditors were not provided with copies of any subcontracts or other agreements documenting the nature of the arrangements (including service standards and accountability) between the System Operator and third parties collecting personal information on its behalf via assisted registration. Therefore, the auditors were unable to assess the System Operator’s compliance with its s 95B obligations and what steps, if any, the System Operator had taken to ensure the personal information it collected from the third party subcontractor had been collected in compliance with the IPPs.

Recommendation 4 — Review subcontract and any other agreements

3.40 It is recommended that the System Operator consider whether it is necessary to review and revise its subcontract with any third party subcontractor providing assisted registration, and any other agreements documenting the nature of the arrangements (including service standards and accountability), to ensure that these comply with s 95B of the Privacy Act.

Privacy issues — policies and procedures for non point-of-care assisted registrations — the System Operator’s processes and procedures

3.41 The Guide is designed for use in point-of-care assisted registrations. The auditors also received a document Assisted Registration: Business as Usual, which outlined the System Operator’s policies regarding assisted registration as of 23 April 2012, and similarly only related to point-of-care assisted registrations.

3.42 At the time these documents were prepared, it appears that the System Operator had intended that assisted registrations would only be conducted predominantly by point-of-care healthcare providers under a ‘known customer’ model.

3.43 Whilst it has been used for non point-of-care registrations, the Guide does not include any consideration of the particular circumstances and privacy risks that may arise from non point-of-care assisted registrations. Given that the consumers are unlikely to be known to third party non point-of-care providers, the manner in which a person is

---

8 Non point-of-care registrations are described under Assisted registration in Appendix A.
best able to consider and receive information and make informed decisions may be unknown. This may call for further oversight measures and additional guidance to mitigate against any additional risks that non point-of-care assisted registration may raise.

3.44 Summaries of consumer feedback provided to the auditors contain allegations of potentially ‘unfair’ behaviours being exhibited at some non point-of-care assisted registrations. We acknowledge that this feedback is untested and the number of summaries provided is small compared to the overall number of registrations conducted in the same period.

3.45 However, the feedback highlights areas of possible risk where personal information is collected by healthcare providers providing non point-of-care assisted registrations.

3.46 The System Operator advised\(^9\) that non point-of-care assisted registrations had been conducted in a broad range of settings across Australia. These included DHS service centres, medical centres, aged care settings, hospitals, Aboriginal Medical Services, and healthcare conferences and events.

3.47 The auditors consider that additional guidance is warranted to ensure that consumers who are particularly vulnerable, such as some consumers attending aged care settings, hospitals and Aboriginal Medical Services, are provided with all necessary information, understand the voluntary nature of registration and are able to provide informed consent to the registration. This is a similar issue to Recommendation 2.

3.48 There may be a greater risk that such persons do not have capacity and, as the Guide states, healthcare providers cannot offer assisted registration to any adult who does not have capacity or who is acting on behalf of an adult in their care. Such consumers may be suitable candidates for registration by an authorised representative, rather than by the third party subcontractor.

3.49 The System Operator may wish to put in place additional controls to help ensure that non point-of-care assisted registrations staff are effectively trained to collect information by fair means.

**Recommendation 5 — Amend the Guide for non point-of-care locations**

3.50 It is recommended that the System Operator amend the Guide to specifically address non point of care assisted registration settings or, if it considers it necessary, create a new guide for non point-of-care registrations.

---

\(^9\) Response to information request by the OAIC dated 19 April 2013.
Part 4 — Audit issues IPP 2

IPP 2 issues — Solicitation of personal information from individual concerned:

IPP 2 provides that, where a collector solicits and collects personal information directly from an individual, it must take such steps (if any) as are reasonable in the circumstances to inform the individual of the purpose of collection, any legal authorisation or requirement for the collection, and any person, body or agency to which it usually discloses that information. IPP 2 requires the collector to notify the individual of these matters before the information is collected or, if that is not practicable, as soon as practicable afterwards.

Substance of notifications

Observations

4.1 The System Operator collects personal information directly from the individual concerned in all registration channels except assisted registration. In assisted registration, personal information is initially collected from the consumer by a registered healthcare provider organisation, from which the System Operator collects the personal information.

4.2 Different privacy notices are provided to the consumer depending on the registration channel chosen. The auditors understand that the following notices are provided:

- **Online**: consumer is required to read the on-screen ‘Essential Information’ (online Essential Information).

- **In-writing**: the ‘Application to register for a Personally Controlled Electronic Health Record’ form contains a privacy notice (application form privacy notice), and requires applicants to declare they have read the ‘eHealth Registration Booklet’ (Registration Booklet) which is either provided with the form, or otherwise available online.

- **Phone**: If the consumer has not read certain sections of the Registration Booklet, the System Operator staff member reads out documents entitled ‘Essential information for eHealth record applicants’ (Essential Information) and ‘Your privacy in the eHealth record system’ (Your Privacy).

- **In-person**: If the consumer has not read certain sections of the Registration Booklet, the System Operator’s staff give the consumer handouts of the Essential Information and Your Privacy documents.\(^\text{10}\) For streamlined in-person registration, the consumer will also see the application form privacy notice.

- **Assisted registration**: the relevant healthcare provider organisation provides the consumer with the ‘Essential information about assisted registration for a PCEHR’ document (AR Essential Information). In signing the assisted registration application form, the consumer declares they have read this document.

---

\(^{10}\) The auditors understand these handouts are the same documents read out during phone registrations.
4.3 The auditors reviewed each of these privacy notices. A summary of these notices and the channels to which they relate are set out in Appendix B — ‘IPP 2 notices by registration channel’.

4.4 For assisted registrations, as the System Operator does not collect personal information directly from the individual, the requirements of IPP 2 do not strictly apply to the System Operator in this context. However, given that:

- personal information is being collected from individuals for the purposes of a system for which the System Operator is responsible
- the System Operator itself developed the framework in which the assisted registration information is collected, and
- the System Operator has developed the AR Essential Information document and requires registered healthcare provider organisations to distribute it to consumers,

the auditors consider that, as a matter of best practice, the System Operator should ensure that the AR Essential Information complies with relevant privacy requirements. Further, from March 2014, APP 5 will require the System Operator to ensure the individual is aware of specified matters, even where collection is not directly from the individual.

4.5 NPP 1.3 (rather than IPP 2) applies to many notifications in the assisted registration context given the fact that the direct collection will frequently be conducted by private sector organisations. NPP 1.3 requires notification of additional items to IPP 2, including the identity of the collecting organisation and how to contact it, the fact the individual can gain access to the information, and the main consequences of not providing the information. The auditors have also addressed these requirements in the discussion below.

4.6 This audit considers compliance with IPP 2. The auditors note that APP 5 will replace IPP 2 from 12 March 2014, which will introduce a number of changes, including that:

- APP 5 will apply to any situation where an APP entity collects personal information about an individual (not just where an entity collects directly from the individual)
- the matters for notification will be expanded to include matters such as the identity and contact details of the APP entity, and that the APP privacy policy of the entity contains information about accessing and correcting information and making a privacy complaint.

In implementing the IPP 2 recommendations contained in this audit report, the auditors encourage the System Operator to also prepare for the introduction of the new requirements in APP 5.
Privacy issues — inconsistency between privacy notices

4.7 There was considerable variation in the content of IPP 2 notices provided to consumers through the different registration channels. Given the different delivery modes for the notice, some variation may be appropriate – a notice being read out to a consumer over the phone is likely to be briefer than an online notice which a consumer can read in their own time. However, each notice must comply with IPP 2.

4.8 The reason for the nature of other variations was less apparent. For example it is unclear why:

- applicants through the in-person channel are only provided with the Your Privacy and Essential Information handouts, while applicants through the assisted registration channel (which is also a face-to-face interaction) receive the detailed AR Essential Information document. The applicants through these two channels are getting very different levels of notification
- reading the Registration Booklet is not a precondition to applying through all registration channels (as it is for applying through the in-writing channel). This is particularly so when the privacy notices in the phone and in-person channels are less comprehensive
- some privacy notices specifically refer readers to the Registration Booklet for more information, while the online Essential Information, Your Privacy document and AR Essential Information do not reference the booklet.

4.9 Consumers must receive consistent notification of IPP 2 matters irrespective of the registration channel they use. Consumers are providing their personal information for the same purpose, and their information (collected through the registration process and subsequently based on consent they provide during registration) will be subject to the same usual disclosures, irrespective of the registration channel used.

4.10 As well as being required by IPP 2, appropriate notification is important to ensuring consumers understand why their information is being collected and how it will be used and disclosed. Where consumers are not sufficiently informed, the risk of privacy complaints increases. The auditors noted from the assisted registration consumer comments and feedback reviewed that the most common issue raised was around inadequate notification. This is indicative of the importance of notification in minimising consumer complaints and dissatisfaction.

4.11 The Registration Booklet is a useful source of information for consumers about the privacy aspects of the system, the system more broadly (which will help consumers understand the privacy notices) and the next steps. The auditors suggest that each privacy notice should include a specific reference to the Registration Booklet.

Recommendation 6 — Consistent notification

4.12 The auditors recommend that the System Operator review and revise each IPP 2 privacy notice used in conjunction with eHealth record registration (particularly
considering consistency between each notice) so that consumers are receiving consistent IPP 2 notification through all channels.

**Privacy issues — specific requirements of IPP 2 — purpose of collection**

4.13 IPP 2(c) requires the System Operator to notify consumers of the purpose for which information is collected. Each privacy notice addressed this requirement to some extent. The broad purposes for collecting personal information during the registration process are identified in the IPP 2 notice documents as relating to identity verification, deciding whether the individual can be registered for an eHealth record, managing the consumer’s eHealth record, and managing the eHealth record system more broadly.

4.14 However, not all privacy notices identified all of these purposes. For example:

- the application form privacy notice does not reference the purposes of identity verification or managing the eHealth record system
- the AR Essential Information does not reference the identity verification purpose
- the Your Privacy notice does not refer to the purpose of managing the consumer’s particular eHealth record.

4.15 During the registration process, the System Operator is collecting consent from consumers to the System Operator’s future collection of:

- health records uploaded by the consumer’s healthcare providers, and
- Medicare records from DHS.

4.16 Each notice does identify that once registered, health information will be collected by the System Operator when it is uploaded by a healthcare provider. However, given that the System Operator is seeking consent to these future collections (and requiring it in the case of health records), each privacy notice should also identify the purpose of those future collections to ensure a consumer is able to provide informed consent.

**Recommendation 7 — Identify each purpose of collection**

4.17 Each privacy notice should identify the purposes for which the personal information is being collected. The purpose of future collections should also be more clearly stated in each privacy notice.

**Privacy issues — specific requirements of IPP 2 — legislative authority**

4.18 IPP 2(d) requires the System Operator to notify consumers of any legislative authorisations for the collection of personal information. The majority of IPP 2 notices identify the legislative authorisation as coming from the PCEHR Act and the *Healthcare Identifiers Act 2010* (HI Act). However, neither the AR Essential Information document nor the Registration Booklet clearly states the legislative authority for the collection of the consumer’s personal information by the System Operator and these notices should be amended to include this information.
Recommendation 8 — Identify the source of legislative authorisation

4.19 The source of legislative authority should be included on all notices.

Privacy issues — compliance with specific requirements of IPP 2 — ‘usual disclosures’

4.20 The majority of IPP 2 notices also identify that there are some circumstances where the PCEHR Act authorises the collection of health information without consent, which is most likely to arise in the case of an emergency. However, the application form privacy notice does not include this information.

4.21 Most IPP 2 notices identify some usual disclosures of personal information as required by IPP 2(e). However, these documents note only a limited class of usual disclosures (for example, the application form privacy notice). These classes are not consistent across the notices.

4.22 This does not provide consumers with a clear understanding of to whom their personal information is usually disclosed as required by IPP 2(e).

4.23 The auditors also compared the usual disclosures mentioned in the privacy notices with the information on disclosures in the full privacy statement. There are a number of disclosures included in the full privacy statement which do not appear in all of the privacy notices, such as disclosures to the System Operator’s contracted private sector firms, and disclosures to the OAIC, state and territory regulators and healthcare provider organisations to deal with a question or issue raised by the consumer with the System Operator.

4.24 For example, the ‘Your Privacy’ contains some usual disclosures and includes a link to the full privacy policy. The Essential Information booklet does not include any usual disclosures, but refers readers to the Registration Booklet (but not to the full privacy policy directly). The Registration Booklet includes some usual disclosures and links to the full privacy policy.

4.25 The auditors suggest that the System Operator reconsider whether disclosures to these entities are ‘usual’ (that is, which are common practice – this may include regular arrangements to give information to those entities). Where the disclosures are ‘usual’, each privacy notice should be amended to identify these additional entities (if there are many, by type of entity) and, if the disclosure is partial, the kind of information to be provided. This may be done in the document itself or through linking to another document.

4.26 If it is known that the entity will ‘on disclose’ the information to another party, this should also be noted.

4.27 APP 5 5.2(ff), which came into force on 12 March 2014, requires consumers be provided with notice of ‘usual’ disclosures in broadly equivalent terms to IPP 2.
Recommendation 9 — Make ‘usual disclosures’ consistent

4.28 Each notice should set out usual disclosures (by class and/or by specific reference) and the System Operator should review inconsistencies across notices to ensure each notice sets out all usual disclosures directly or by links (using a layered approach).

Privacy issues — scheduled review of notices

4.29 The auditors were not provided with any documentation indicating that the System Operator has in place a policy to regularly review privacy notices to ensure they remain accurate, consistent and up-to-date. If no such policy is in place, the auditors suggest one is developed to ensure that the System Operator meets its Privacy Act notification obligations into the future.

Training material

Observations

4.30 The auditors reviewed a number of training packages provided to the System Operator’s staff conducting phone and in-person registrations. Each training package directed staff to give the consumer (or read out to the consumer over the phone) the Essential Information (linked to in the online training). The Essential Information addressed only one IPP 2 requirement. This is not problematic in itself because the auditors understand that it is generally presented along with the Your Privacy document which does address IPP 2 issues to some extent.

4.31 However, the auditors noted that the training packages only identify the Essential Information document which may lead staff to believe it is the only document they need to provide. The training packages should be updated to reflect the fact that both documents need to be provided.

4.32 The training packages appear to take staff step-by-step through the phone and in-person registration processes. The auditors observed some inconsistencies between the steps outlined in the training packages, and the steps outlined in the process documents entitled ‘Register a consumer for an eHealth record (procedure)’ and ‘Finalise consumer eHealth record registration’.

4.33 For example, the training packages advise staff to read out the ‘important information’ (explaining that the record will be available to all healthcare providers involved in their care) to the consumer before selecting ‘create record’, a step which is not contained in the written process documents.

4.34 Training materials will need to be updated from time to time to ensure that the training material and process documents align and to directly address the importance of notice under IPP 2.
Timing of notice

Observations

4.35 The IPP 2 notice is provided to consumers prior to any personal information being collected in the following registration channels:

- online registration: the first step in this process involves the consumer reading the online Essential Information and clicking a button confirming they have read it
- in-writing: the IPP 2 notice is near the beginning of the form before the fields in which consumers enter personal information.

4.36 According to the written process documents, the IPP 2 notice is provided to consumers after the collection of some personal information in the following channels:

- phone: identity verification is undertaken by the System Operator’s staff before the IPP 2 notice is provided
- in-person (both streamlined and standard): the System Operator’s staff undertake identity verification before providing the IPP 2 notice.

4.37 Consistent with the written process documents, one training module dealing with phone registration states that the consumer’s identity must be verified prior to ensuring the consumer reads the essential information. However, the registration training modules relating to in-person registration direct staff to provide the notice to the consumer to read while they are conducting identity verification.

4.38 For assisted registration, the IPP 2 notice is intended to be provided prior to, or concurrently with, the collection of personal information. The assisted registration guide indicates that Step 1 (Apply) of the registration process includes ‘Patient reads Essential Information and completes and signs the one page application form’. The Guide also goes on to note that: ‘Your organisation must provide the application form… to the consumer to complete. You must also ensure the consumer is provided with the document “Essential information about assisted registration for a personally controlled electronic health record.”’

Privacy issues

4.39 IPP 2 requires agencies to provide IPP 2 information before personal information is collected or, if that is not practicable, as soon as practicable after the information is collected.

---

11 ‘Register a consumer for an eHealth record (procedure)’; ‘Streamlined Registration (eHealth records) – Offering the service’.
12 Two documents regarding streamlined registration contained conflicting processes. The auditors have relied on the more comprehensive ‘Streamlined Registration (eHealth records) – Offering the service’ document. The document ‘Checklist – Streamlined Registration Process’ sets out a different process in terms of the order of steps, which includes providing the Essential Information as the first step.
13 Training module MCA00683a.
14 See p5.
15 See p11.
collected. An agency should only put off giving an IPP 2 notice if there are practical problems in giving the notice before collecting the information that the agency cannot overcome by any reasonable means.\(^\text{16}\)

4.40 For the online and in-writing registration channels, the System Operator complies with the IPP 2 requirement to generally notify before collecting information.

4.41 For the phone and in-person registration channels, however, the System Operator does not provide IPP 2 information until after identity verification takes place (or, according to some training modules, during the identity verification process). There may be a practical reason why this is the case, however it is not apparent to the auditors.

4.42 There is inconsistency in process documentation related to streamlined registration. The comprehensive process document ‘Streamlined Registration (eHealth records) – Offering the service’ has the IPP 2 notice being provided after identity verification, while the short ‘Checklist – Streamlined Registration Process’ document has the IPP 2 notice being provided as the first step.

**Recommendation 10 — Amend material to remove inconsistencies and ensure that IPP 2 notice is provided up front**

4.43 The auditors recommend that the System Operator:

- amends the phone and in-person registration processes (and all related documentation and training modules) to ensure that IPP 2 notification is provided to consumers before any personal information is collected (unless it is not practicable to do so)

- review the ‘Streamlined Registration (eHealth records) – Offering the service’ and ‘Checklist – Streamlined Registration Process’ documents and revise where necessary to ensure a clear, consistent and IPP 2 compliant process to avoid confusion amongst the System Operator’s staff.

**Manner of notification**

**Observations**

4.44 The AR Essential Information document is intended to be handed out to consumers who are considering registering for an eHealth record via the assisted registration channel. The auditors observed that this document consists of dense text presented in a very small font over a double-sided A4 page.

4.45 The procedures for phone registration require the System Operator’s staff to read out the Your Privacy and Essential Information documents. The procedures (both in written process documents and training modules) do not contain a prompt for the staff member to check whether the consumer has understood the notice, whether they would like any part repeated, or whether they have any questions.

\(^{16}\) See IPP 2 Guidelines – Guideline 11 on p16.
4.46 The procedures for in-person registration require the System Operator’s staff to hand to the consumer the Your Privacy and Essential Information documents. As with phone registration procedures, there is no prompt for staff to check the consumer understands the documents.

4.47 It is not clear from the documentation whether the consumer is able to retain these handouts, or whether they need to be returned after reading. The auditors noted that the ‘eHealth Streamlined Registration Process Training Information’ document refers to staff having a ‘laminated essential and privacy information’, which implies the consumer does not keep the documents.

4.48 The auditors were not provided with any documentation addressing the provision of eHealth information in accessible formats.

4.49 As noted previously, the auditors reviewed summaries of a selection of feedback received by the System Operator in relation to assisted registrations.

4.50 The majority appeared to relate to registrations conducted at non-point-of-care locations. A number related to not being given enough time to consider the information provided and whether or not to register. In addition, some alleged that notification was not provided.

*Privacy issues — dealing with potentially vulnerable people*

4.51 When collecting an individual’s personal information, IPP 2 requires an agency to take reasonable steps to ensure that the individual is generally aware of particular information.

4.52 The auditors understand that the assisted registration channel is particularly likely to be used by more vulnerable sections of the population (such as the elderly and people from non-English speaking backgrounds), for whom other registration channels might be inappropriate.

4.53 Given the likelihood of these groups using this channel, the auditors consider that depending on the circumstances, the format of the AR Essential Information may not constitute reasonable steps for ensuring that these consumers are generally aware of IPP 2 information. The notice contains dense text and a very small font. This can create difficulties, including that small type is likely to be difficult to read, and dense text might be difficult to comprehend for people with limited English skills.

4.54 While no information was provided by the System Operator about the availability of eHealth record system information in other languages and accessible formats, the auditors acknowledge that such material may exist.

4.55 As a matter of best practice, such information should be available to ensure all consumers can be informed about the eHealth record system. The availability of

---

17 The auditors note that the document *Concept of Operations: Relating to the introduction of a Personally Controlled Electronic Health Record System* foreshadowed that the System Operator would release material in various accessible formats (see section 3.2.5).
information in accessible formats is particularly important in the assisted registration context where, because of the registration assistance provided, consumers with communication challenges are more likely to register. The auditors acknowledge that DHS, in managing contact with consumers as described in paragraph 1.3 of this report, has the capability to provide translator services as required. However, this may not apply to registrations conducted by other organisations.

Recommendation 11 — Amend format for potential audience

4.56 To ensure the System Operator is taking reasonable steps to notify consumers, the auditors recommend that it reconsider the format of the AR Essential Information to ensure it is appropriate for probable users of this registration channel.

4.57 If IPP 2 information is not already available in a range of languages, the System Operator should consider whether such material should be available in written form.

Privacy issues — seek confirmation of understanding

4.58 In some circumstances, the most practical method of delivering an IPP 2 notice is orally and the auditors acknowledge this is reasonably the case for the phone registration channel. When delivering an IPP 2 notice orally, however, particular steps should ideally be taken to ensure the individual has comprehended the information.

4.59 The System Operator has implemented good privacy practice by requiring the System Operator’s staff to read out the IPP 2 notice exactly as printed. However, receiving a notice orally can affect an individual’s ability to comprehend the details of the notice.

4.60 To ensure the consumer is generally aware of the IPP 2 information, the auditors suggest that the phone registration process should also include the following best practice steps:

- after reading out the notice, the System Operator’s staff should ask the consumer whether they have understood the notice, need it repeated or have any questions
- ideally, a written IPP 2 notice should subsequently be sent to the consumer following the transaction, possibly as an insert in correspondence.\(^\text{18}\)

4.61 For in-person registration, the consumer is asked to read and comprehend the notice. This may occur a short space of time and the consumer may feel the information provided is not sufficient.

4.62 The auditors would similarly suggest that the System Operator’s staff ask consumers whether they have understood the notice, need more time to review it or have any questions. Consumers should also be able to keep the notice they are provided with for future reference.

\(^\text{18}\) These two suggestions reflect the OAIC’s IPP 2 Guidelines — see p20.
Part 5 — Audit issues IPP 3

IPP 3 issues — Solicitation of personal information generally:

IPP 3 provides that, where a collector solicits and collects personal information it must take steps (if any) that are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is collected, the information is relevant to that purpose, up-to-date and complete, and that the collection does not intrude to an unreasonable extent on the individual’s personal affairs.

Relevance, currency and completeness

Observations

5.1 As stated in ‘Part 3 – IPP 1 issues’, the auditors reviewed all forms and written procedures used to guide the collection of personal information through each registration channel.

5.2 The auditors also received a number of documents outlining the System Operator’s policies and procedures in relation to each type of registration. Much of this information related to the various identity verification procedures and the identity documents that needed to be provided for each type of registration.

5.3 The System Operator has a process of verifying the consumer’s identity against Medicare records, to ensure the consumer is a known Medicare customer. The auditors considered this a generally sound process, which appeared to help ensure the details given to the System Operator were up-to-date and complete.

5.4 Overall, the relevance of most of the information collected through each of the registration processes was generally clear.

5.5 The auditors observed that the application forms and procedures for each of the registration processes were designed in such a way that would prevent the collection of irrelevant information (see ‘Part 3 – IPP 1 issues’ above).

5.6 The System Operator has a process for consumers who cancel their registration and later decide to re-register. This process was the same as the initial registration process and appropriately requires the consumer to redo the identity verification check and re-verify their details. This process helps ensure the information collected is up-to-date and complete.

Privacy issues — inconsistency in information collected

5.7 As noted under ‘IPP 1 issues’ above, there was considerable inconsistency in the information collected through each of the registration processes. This inconsistency led the auditors to question precisely which information may be relevant for the System Operator to collect and whether there was a risk that irrelevant information may be collected.
5.8 For the same reason, the auditors were uncertain whether the information the System Operator collected through each of the registration processes was complete. If certain information was necessary for some processes, it was unclear why it was not collected through the other processes.

5.9 Based on the inconsistencies in the information collected through each of the registration processes, the auditors concluded there was a risk that the information collected may be incomplete in some circumstances and irrelevant in others.

**Recommendation 12 — Review personal information collected**

5.10 The System Operator should review the types of information collected through each registration process with a view to ensuring that each item of personal information collected is relevant to the purpose of collection and complete. The System Operator should review this as appropriate.

**Privacy issues — assisted registration — non point-of-care providers**

5.11 The auditors note that the Guide appears to assume:

- assisted registration takes place at point-of-care only
- the consumer is a known customer.

5.12 Little information is given in the Guide in relation to the other forms of identification that may be used if the known customer model cannot be used. None of the identification methods for the known customer model or which were otherwise provided as part of the audit material are clearly stated to apply to non point-of-care healthcare provider organisations offering assisted registration.

5.13 The auditors did not receive any identity verification policies and procedures specifically for non point-of-care provider assisted registrations as part of the audit material. As such, the auditors were unable to assess what steps the System Operator had taken to ensure the personal information used by non point-of-care providers to verify identity was relevant to purpose, up-to-date and complete.

5.14 It was unclear why the System Operator has implemented and approved identification criteria for point-of-care but has not included guidance for non point-of-care provider organisations, as the latter are performing assisted registrations for consumers with whom they have no previous relationship (with the potential for a greater risk of error). This may be the subject of training provided by non point-of-care provider organisations to staff undertaking registration activity; however, such training material has not been provided as part of the audit.

5.15 In the absence of clear identity verification procedures designed for non point-of-care providers offering assisted registration, there is a risk for the System Operator in being satisfied that the identity of the consumer has been appropriately verified through this process as required by the PCEHR Act.
Recommendation 13 — Review identity verification procedures for non point-of-care assisted registrations

5.16 It is recommended that the System Operator amend the Guide to provide clear guidance on identity verification policies and procedures designed for assisted registrations performed by non point-of-care healthcare provider organisations or provide further guidance separately.

Intrude on personal affairs

Observations

5.17 The auditors considered whether the content of the policies and procedures in relation to in-writing, online, phone, in-person and assisted registrations unreasonably intruded on the personal affairs of consumers.

5.18 The OAIC’s Plain English Guide to the Information Privacy Principles 1-3 says intrusive collection includes:

- asking questions about sensitive affairs
- collecting personal information by physically touching people
- repeatedly asking for the same personal information.

Privacy issues

5.19 The auditors’ review of the policy or procedures did not suggest a high risk of unreasonably intrusive collection given registration categories outlined in the procedures do not include categories that the auditors considered were about sensitive affairs. The one exception is indigenous status, which could be considered to be unreasonably intrusive without a clear reason for collection.

5.20 This report discusses consistency issues around the collection of indigenous status in relation to the necessity of collection. If the System Operator determines that collection is necessary, it is likely that the collection would not have unreasonably intruded on the personal affairs of consumers.

5.21 The auditors consider unfairness of collection, which is discussed under IPP 1, is a greater risk than an unreasonably intrusive collection. However, repeatedly asking for the same personal information (which is an example of unreasonably intrusive behaviour cited above) is an unlikely but possible scenario in the context of PCEHR assisted registration. Therefore, as suggested in recommendation 2, when providing examples of unfair collection, the System Operator could include an example in the Guide about repeatedly asking for the same personal information.
Part 6 — Recommendations and auditee response to recommendations

Recommendation 1 — Review information collected, para 3.19

Auditee response
6.1 The auditee accepted this recommendation and made the following comment:

The decision to vary the type of personal information collected, by channel, during a consumer registration process was taken in recognition of information about the consumer that may already be available.

Health will undertake a review of some of the information collected for non-identity verification purpose in order to ensure that we only collect what we need to collect.

Recommendation 2 — Guidance on fairness, para 3.34

Auditee response
6.2 The auditee accepted this recommendation and made the following comment:

Accepted, insofar as the recommendation relates to including guidance on collection of information. Health requests that it be noted that the Assisted Registration Guide is designed to be used consistently by all organisations providing assisted registration.

Recommendation 3 — Alternative registration methods, para 3.35

Auditee response
6.3 The auditee accepted this recommendation and made the following comment:

The eHealth Division, in consultation with the OAIC, will revise and publish (online) the Guide by September 2014.

Recommendation 4 — Review subcontract and any other agreements, para 3.40

Auditee response
6.4 The auditee accepted this recommendation and made the following comment:

Health reviewed its contractual arrangements with those organisations providing assisted registration services on its behalf, including Medicare Locals, and can confirm that these did comply with section 95B of the Privacy Act.
Recommendation 5 — Amend the Guide for non point-of-care locations, para 3.50

Auditee response
6.5 The auditee partially accepted this recommendation and made the following comment:

The Guide has been developed for use by all registered healthcare provider organisations providing assisted registration, independent of the setting in which the registration is undertaken. Future revisions to the Guide will be aimed at ensuring that there is more clarity that the Guide is for use in all settings.

Recommendation 6 — Consistent notification, para 4.12

Auditee response
6.6 The auditee accepted this recommendation and made the following comment:

Privacy notices have been reviewed and revised to be consistent and to comply with the new APP requirements. These have now been published.

Recommendation 7 — Identify each purpose of collection, para 4.17

Auditee response
6.7 The auditee accepted this recommendation and made the following comment:

Privacy notices have been updated and published.

Recommendation 8 — Identify the source of legislative authorisation, para 4.19

Auditee response
6.8 The auditee accepted this recommendation and made the following comment:

Privacy notices have been updated and published.

Recommendation 9 — Make ‘usual disclosures’ consistent, para 4.28

Auditee response
6.9 The auditee accepted this recommendation and made the following comment:

Privacy notices have been updated and published.
Recommendation 10 — Amend material to remove inconsistencies and ensure that IPP 2 notice is provided up front, para 4.43

Auditee response
6.10 The auditee accepted this recommendation and made the following comment:

Processes and associated notices have been updated.

Recommendation 11 — Amend format for potential audience, paras 4.56 and 4.57

Auditee response
6.11 The auditee accepted this recommendation and made the following comment:

The Assisted Registration Essential Information document has been reviewed and revised. Opportunities for multi-lingual material will be considered in the context of the available budget for 2014-15.

Recommendation 12 — Review personal information collected, para 5.10

Auditee response
6.12 The auditee accepted this recommendation and made the following comment:

Collections have been reviewed. A policy for the regular review of privacy statements has been implemented.

Recommendation 13 — Review identity verification procedures for non point-of-care assisted registrations, para 5.16

Auditee response
6.13 The auditee partially accepted this recommendation and made the following comment:

The Guide provides general guidance on undertaking assisted registration to healthcare provider organisations, independent of the setting in which the registration is undertaken.

The Guide will be amended to ensure that there is clarity that it is for use in all settings.

Healthcare provider organisations providing assisted registrations are required to address, in their policy required under Rule 9(d) of the PCEHR (Assisted Registration) Rules 2012, the process and criteria for consumer identification they will use, consistent within their organisation.
Appendix A — Overview of eHealth record registration processes

There are five ways a consumer can register for an eHealth record. Below is an overview of the auditors’ understanding of each registration process as at the date of this audit.

Online registration

The general process for registering online is as follows:

- A ‘prepare to register screen’ outlines the online registration steps and the information a consumer will need in order to complete the registration.
- After clicking ‘continue’, ‘Essential information’ text is displayed.
- After indicating they have read the essential information, the consumer is directed to the [https://my.gov.au](https://my.gov.au) account portal to create a myGov account.
- The consumer’s identity is then verified. This involves entering personal information such as Medicare card and address details, and answering questions relating to their Medicare record (such as details of the last Medicare claim). If the consumer does not consent to their Medicare record being accessed, the online process cannot proceed.
- Following identity verification, the consumer proceeds to set up the eHealth record by:
  - consenting to the ongoing upload of their health information by health providers
  - indicating preferences for the display of Medicare information\(^\text{20}\) in their record
  - indicating (or declining to indicate) their Aboriginal or Torres Strait Islander origin.
- The consumer then clicks on ‘Register and create an eHealth record now’. Onscreen text notes that by proceeding, an eHealth record will be available to all healthcare providers involved in the consumer’s care, and that the consumer can control access by clicking on the ‘restricted access’ setting.

\(^\text{19}\) The documentation provided during the audit refers to [www.australia.gov.au](http://www.australia.gov.au) and australia.gov.au accounts. The auditors understand that the australia.gov.au account has recently been replaced with myGov accounts accessed at [https://my.gov.au](https://my.gov.au) and so have referred to myGov accounts in this report.

\(^\text{20}\) The information which consumers can choose to include is information relating to:
- Medicare Benefits Schedule claims (or DVA claims)
- Pharmaceutical Benefits Scheme claims (or Repatriation Pharmaceutical Benefits Scheme claims)
- Australian Childhood Immunisation Register
- Australian Organ Donor Register.

Consumers can choose whether to display this information for the future only, or also for the previous two years.
Steps in this process can vary depending on a consumer’s circumstances. For example:

- If a consumer already has a myGov account and has previously established their online identity with Medicare, that online identity can be shared with the eHealth Record System so that identity verification does not need to take place.

- Where a consumer has an Identity Verification Code (IVC) from having their identity verified through an alternative channel, the identity verification step can be skipped by entering the IVC.

**In-writing registration**

To register in writing, a consumer completes the ‘Application to register for a Personally Controlled Electronic Health Record’ form:

- Page 1: contains introductory information including the form’s purpose, the documents to be attached to the form, and how to return the form. It notes the consumer must read the ‘Registration Booklet’ before signing the form, and explains how it can be obtained if it did not accompany the form.

- Page 2: contains a privacy notice.

- Pages 2–4: contain the fields a consumer needs to complete to apply to register for their own eHealth record.

- Page 3: contains information about the inclusion of Medicare information in the consumer’s eHealth record and requires the consumer to indicate which of this information (if any) they consent to including in their record.

- Page 4: contains the consumer’s standing consent to health records being uploaded to their eHealth record, and a declaration that the Registration Booklet has been read.

- Certified evidence of identity documents must be attached to completed forms.

The form is available on the ‘Resources’ page of the eHealth.gov.au website. The form is mailed to the address shown on the form, or can be dropped into a DHS Service Centre offering Medicare services.

**Phone registration**

The process for a consumer to register via the eHealth helpline is as follows:

- The consumer’s identity is verified. This involves collecting personal information such as Medicare card and address details, and requiring the consumer to answer questions relating to their Medicare record (such as details of the last Medicare claim). If the consumer does not consent to their Medicare record being accessed, the registration process cannot proceed.

- The consumer is asked if they have read both the ‘essential information’ and the ‘privacy information’ in the Registration Booklet:

---


22 As detailed in the report, there were discrepancies between the phone registration process noted in the formal process documents, and the process explained in training packages available to System Operator staff.
If the ‘essential information’ has not been read, System Operator staff read out the ‘Essential Information for eHealth record applicants’ document.

If the ‘privacy information’ has not been read, System Operator staff read out the ‘Your privacy in the eHealth record system’ document.

- System Operator staff locate the consumer in the CDMS, open the eHealth record system, record that identity was verified, and generate an IVC which is provided to the consumer.
- The consumer can then choose to either continue their registration over the phone, or complete their registration online using their IVC to prove their identity.
- If the consumer chooses to continue over the phone, System Operator staff create the eHealth record, and seek consent for the ongoing upload of health records. Preferences for Medicare data are also entered into the record.
- If the consumer chooses to complete their registration online, then they log into or create a myGov account, use their IVC to bypass identity verification, and then proceed to create their registration as per the online process described above.

**In-person**

**Streamlined registration (the consumer completes a form)**

Streamlined registration can be offered in DHS Service Centres offering Medicare services, using the following process:

- Streamlined registration can be initiated by System Operator staff either approaching consumers in the waiting area, or at the end of a counter transaction.
- The consumer is asked whether they would like to register for an eHealth record, and is provided with background information if it is requested. If the consumer agrees to register for an eHealth record, they are taken to a private area.
- The consumer’s identity is verified by sighting evidence of identity documents.
- The consumer is asked whether they have read both the essential information and privacy information in the Registration Booklet. If not, they are provided with an ‘Essential Information and Privacy’ handout to read.
- The consumer then completes the ‘Application to register for a PCEHR’ form.
- System Operator staff check that the form is complete and has been signed. They advise the consumer that if their registration is successful, their IVC will be sent to them which will enable them to access their record.
- System Operator staff are instructed to store forms securely where personal information is not visible. Each day, ‘simple’ registrations should be delivered to their

---

23 Simple registrations are adults enrolled in the Medicare program or with DVA entitlements registering for their own eHealth record; parents/guardians registering a child under 18 who is on their Medicare card; and young persons over 14 enrolled in the Medicare program or with DVA entitlements registering for their own eHealth record.
managers for processing, while ‘complex’ registrations\textsuperscript{24} should be sent to DHS for processing.

\textit{Without a form}

If a consumer wants to register in a Medicare office, and either does not want to do streamlined registration, or streamlined registration is unavailable, the process is as follows:

- System Operator staff member verifies the consumer’s identity, either by sighting evidence of identity documentation, or by asking a series of questions based on the consumer’s Medicare record (as in online registration).
- The consumer is asked whether they have read both the essential information and privacy information in the Registration Booklet. If not, they are provided with an ‘Essential Information and Privacy’ handout to read.
- The staff member locates the consumer in the CDMS, opens the eHealth record system, records that identity was verified, and generates an IVC which is written down for the consumer.
- The consumer can then choose to either continue their registration face-to-face, or complete their registration online using their IVC to prove their identity.
- If the consumer chooses to continue face-to-face, System Operator staff create the eHealth record, and seek consent for the ongoing upload of health records. Preferences for Medicare data are also entered into the record.
- If the consumer chooses to complete their registration online, then they log into or create a myGov account, use their IVC to bypass identity verification, and then proceed to create their registration as per the online process described above.

\textbf{Assisted registration}

Each registered healthcare provider organisation (HPO) conducting assisted registration is required to have its own assisted registration policy. However, in general, the process is as follows:

- A consumer wishing to register for an eHealth record reads the ‘Essential information for assisted registration’, and completes and signs the one-page form ‘Assisted registration: Application to register for a PCEHR’. An authorised employee for the registered HPO reviews the form to check it is complete and signed, and that the applicant is eligible to apply through assisted registration.
- The authorised employee determines whether the patient is a known customer of the organisation in accordance with the HPO’s assisted registration policy.
- The authorised employee uses the Assisted Registration Tool (or other compliant practice software) to enter and submit the patient’s details to the eHealth record System Operator and to assert the patient’s identity.

\textsuperscript{24} Complex registrations include parents/guardians seeking to register children not on their Medicare card; authorised representatives applying to register an individual over 18 years and independent minors under 14 years of age providing a letter of capacity.
• The authorised employee advises the patient if their application has been successful. If successful, the registration process is complete and an eHealth record has been created. An IVC will be sent to the patient via their elected method.

• Signed forms must be either stored by the HPO for three years, sent to the System Operator, or both.

For the purposes of this report, an assisted registration can be conducted at point-of-care or non point-of-care locations.

‘Point-of-care assisted registration’ or ‘assisted registration’: this is usually conducted at the time the consumer is receiving healthcare services, often by a healthcare provider known to the consumer. Examples may include a local doctor or an aged care nurse.

‘Non point-of-care assisted registration’: this is usually conducted at a time when the consumer is not receiving healthcare services and/or is conducted by a healthcare provider who is not related to the provision of healthcare to the consumer. Examples may include in a shopping mall or by a third party contractor who is not involved in the provision of healthcare services to the consumer (even if the location is a healthcare centre – for example a hospital).
## Appendix B — summary of IPP 2 notices by registration channel

<table>
<thead>
<tr>
<th>Channel and Document in which privacy notice is used and appears</th>
<th>Content of notice</th>
</tr>
</thead>
</table>
| **Online channel** *online Essential information* | • The online Essential Information generally informs consumers of the purpose for which the System Operator is collecting the information. For example, the notice states that the information is collected: ‘...so we know who you are, can work out whether you can be registered, and so we can manage your eHealth record... We will also collect personal information about you from other Commonwealth agencies (such as Chief Executive Medicare) to verify your identity, create an eHealth record and maintain the eHealth record system.’  
• The notice provides information about the usual disclosures made by the System Operator. While it starts with a high-level description (‘...people or organisations that are registered to participate in the eHealth record system’), expanding the layered notice reveals specific federal government agencies and other groups (such as healthcare provider organisations involved in your care, contracted service providers and repository operators) to whom information is usually disclosed.  
• The notice identifies the PCEHR Act and the HI Act as the legislative basis for collection. It also notes there are some circumstances, including in an emergency, where the PCEHR Act authorises collection without consent. |
<table>
<thead>
<tr>
<th><strong>In writing</strong> (possibly also used by in-person and phone channels if the consumer has a copy)</th>
<th><strong>Application form privacy notice</strong></th>
</tr>
</thead>
</table>
|  | • This notice identifies the purpose of collection as deciding whether registration is possible, and managing the consumer’s eHealth record moving forward. It does not reference identity verification.  
• It states that the collection is authorised under the PCEHR Act and HI Act.  
• The notice identifies groups of entities to which disclosures are usually made, including to healthcare providers where consistent with access controls or, in an emergency, to nominated representatives, portal operators, DHS and DVA. |

<table>
<thead>
<tr>
<th><strong>In writing</strong> (possibly also used by in-person and phone channels if the consumer has a copy)</th>
<th><strong>Registration Booklet</strong></th>
</tr>
</thead>
</table>
|  | • The information in this notice about purpose of collection includes ‘registration, administration, maintenance, monitoring and population of your eHealth record. The System Operator will also use your personal information for the purpose of administering the eHealth record system more broadly. This would include, for example, monitoring the security, integrity and efficiency of the system.’  
• The notice identifies the usual disclosures as to specific government agencies (including the purpose for such disclosures) and to other broad groups such as healthcare providers (in accordance with access controls) and repository operators.  
• There is no statement about the legislative authorisation for the System Operator or healthcare provider organisations to collect information from consumers during the registration process. It does note there are some circumstances, including in an emergency, where the PCEHR Act authorises collection without consent. The notice also identifies that the PCEHR Act and HI Act authorise the CEO Medicare to disclose certain information to the System Operator. |
| **Phone and In-person channels** (read out or provided if the consumer has not read the Registration Booklet) | • The auditors considered these two documents together for the purposes of IPP 2 compliance, given they are generally presented simultaneously.  
• ‘Your Privacy’ contains the following information about purpose:  
  ‘Your information is being collected to verify your identity, decide whether your application for registration can be accepted, and for managing the eHealth record system’.  
• It states that ‘the collection, use, disclosure and storage of your information is authorised, for specific purposes, by the PCEHR Act and the HI Act’.  
• In relation to usual disclosures, it states that information provided will be ‘disclosed between a number of Commonwealth agencies because this is necessary for the operation of the system’. It also notes that the System Operator will disclose other personal and health information when that information is uploaded by health providers or the individual, or where permitted by law, and refers consumers to the full Privacy Statement for more information.  
• ‘Essential Information’ notes that there are some circumstances where the PCEHR Act authorises the collection of health information without consent, most likely in an emergency. While it briefly refers to some important privacy-related matters (such as access controls for eHealth records), it does not address other IPP 2 requirements. |
<p>| <strong>Essential Information and Your Privacy scripts/handouts</strong> |</p>
<table>
<thead>
<tr>
<th>Assisted registration channel</th>
<th>AR Essential Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• The content of the AR Essential Information is very similar to pp6-9 of the Registration Booklet (albeit the information is ordered differently in the two documents). The observations identified above are therefore equally applicable to the AR Essential Information.</td>
</tr>
<tr>
<td></td>
<td>• In relation to the additional notification items contained in NPP 1.3, the AR Essential Information does identify that consumers can access their record online, and it does address consequences of not providing information by identifying that registration is voluntary and choosing to register has no effect on entitlement to medical treatment.</td>
</tr>
<tr>
<td></td>
<td>• The notice identifies that a healthcare provider is collecting the information, that the information is passed on to the System Operator, and provides contact details for the System Operator. It does not identify how to contact the healthcare provider.</td>
</tr>
</tbody>
</table>