Australian Government
Office of the Australian Information Commissioner

Assisted registration policies

of ten registered healthcare provider organisations

Assessment report

Section 33 C(1)(a) *Privacy Act 1988*

Assessment undertaken: April 2014

Draft report issued: May 2014

Final report issued: December 2014

Contents

Assessment of ten HPO assisted registration policies

Part 1 – Background

The eHealth system

1.1 The personally controlled electronic health record system (eHealth system) commenced operation on 1 July 2012. The system was established by, and is regulated under, the *Personally Controlled Electronic Health Records Act 2012* (Cth) (PCEHR Act), the *PCEHR Rules 2012* (Cth) (PCEHR Rules), the PCEHR (Participation Agreements) Rules 2012 (PA Rules) the PCEHR (*Assisted Registration) Rules 2012* (Cth) (AR Rules) and the *Personally Controlled Electronic Health Records Regulation 2012* (Cth).

1.2 The System Operator of the eHealth system is the Secretary of the Department of Health and is responsible for the operation and management of the eHealth system. Consumers can apply to the System Operator to register for a personally controlled electronic health record (eHealth record). When a consumer registers for an eHealth record they are consenting to have their health information uploaded to their eHealth record by registered healthcare provider organisations (HPOs) involved in their care.

1.3 HPOs must be registered under the eHealth system to upload health information to a consumer's eHealth record, to access or use health information in a consumer's eHealth record or to assist consumers to register for an eHealth record.

HPOs and privacy obligations

1.4 The Australian Privacy Principles (APPs) in the *Privacy Act 1988* (Cth) (Privacy Act) will generally regulate a HPO's handling of a consumer's personal information. State and territory HPOs are not regulated by the APPs but they must comply with relevant state or territory laws.

1.5 In addition, the PCEHR Rules, the AR Rules, the PA Rules and conditions imposed by the System Operator (s 43, PCEHR Act) outline privacy obligations in the context of the eHealth system.

Overview of assisted registration

1.6 Assisted Registration is where a HPO assists a consumer to register for an eHealth record. This is different to a regular online, in person, in writing or over the phone registration with the System Operator.

1.7 An HPO conducting an assisted registration must give the consumer a copy of the *Essential Information about assisted registration and your privacy in the eHealth record system* brochure prepared by the System Operator[1] to read and understand. The consumer then completes and signs a one-page form, *Assisted registration: application to register for a PCEHR*.

1.8 The HPOs use the assisted registration tool (ART) software provided by the System Operator to enter and submit the consumer's details electronically to the System

[1] Essential information about assisted registration brochure (note that Health updated this document on 24 March 2014 in line with the changes to the privacy laws which came into effect on 12 March 2014)

Operator. The HPO must either store the signed registration forms for a period of at least three years or send the forms to the System Operator, or both (AR Rule 7(3)). The System Operator's brochure *Assisted Registration: A Guide for Healthcare Provider Organisations*[2] notes that forms may be sent to the System Operator by post or by scanning and uploading them during the registration process.

1.9 During an assisted registration HPOs undertake collection of the following information:

- personal information required to identify the consumer, including name, contact details (to provide the consumer with an IVC if the registration is successful or to contact the consumer if a registration is unsuccessful), identification documents (the identity documents are sighted only)
- personal information required to register the consumer for an eHealth record; for example Medicare card number, Department of Veterans' Affairs (DVA) file number
- collection of consent to the uploading of health information (sensitive information) into the consumer's eHealth record by HPOs
- the indigenous status of consumers (this is optional)

1.10 For the purposes of this report, an assisted registration can be conducted in either 'point-of-care' or 'non point-of-care' situations:

- **point-of-care assisted registration** – this is usually conducted at the time the consumer is receiving healthcare services, often by a healthcare provider known to the consumer or their staff. Examples may include registrations by a GP 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 registrations being conducted 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 registration is conducted in a healthcare related location such as a hospital).

[2] Assisted Registration: A Guide for Healthcare Provider Organisations brochure current November 2013

Part 2 – Description of assessment

Policies assessed

2.1 Health provided the OAIC with the assisted registration policies of the ten HPOs who had undertaken the highest number of assisted registrations by volume as at December 2013. This excludes one provider who was no longer conducting assisted registrations for Health. We are informed that the policies were current as at 4 April 2014.

2.2 The policy documents assessed were developed by the HPOs in compliance with the requirement in AR Rule 9 to develop a written policy of the HPO that reasonably addresses:

- the manner of authorising employees of the organisation to provide assisted registration
- the training that will be provided before a person is authorised to provide assisted registration
- the manner of recording a consumer's consent and how that record will be handled for retention purposes; and
- the process and criteria for identifying a consumer for the purposes of assisted registration.

2.3 The assisted registration policies of the following HPOs were assessed:

- ACT Medicare Local
- Barwon Medicare Local
- Eastern Sydney Medicare Local
- Greater Metro South Brisbane Medicare Local
- Hunter Medicare Local
- Inner East Melbourne Medicare Local
- Metro North Brisbane Medicare Local
- Murrumbidgee Medicare Local
- St Vincent's Hospital
- Western Sydney Medicare Local

Objective, scope and purpose

2.4 Section 33C(1)(a) of the Privacy Act allows the OAIC to conduct an assessment of whether personal information held by an APP entity is being maintained and handled in accordance with the APPs.

2.5 The objective of the assessment was to consider whether the assisted registration policies addressed how the HPOs will maintain and handle personal information in accordance with the following APPs:

- APP 3 in respect of the fairness and lawfulness of collection of personal information and consent from consumers during the assisted registration process
- APP 11 in respect of the information security of personal information collected, in particular its storage, retention and destruction.

2.6 The assessment was conducted for the purpose of assisting HPOs to identify privacy risks in the assisted registration context, and how these may be addressed and mitigated through including relevant information in their assisted registration policy and other related policy or procedural documents.

2.7 This assessment only assessed the HPOs’ assisted registration policies. There may be other related policy documents and procedures of the HPOs (including training documents, privacy policies and collection notices) that are relevant to assisted registration. The assessors note that the other related policy documents and procedures of the HPOs may address the potential deficiencies observed with the assisted registration policy documents assessed.

2.8 The assessment focused on the following aspects of conducting assisted registrations, which present areas of potential privacy risk (particularly those conducted in non point-of-care situations):

- the way in which personal information is collected from consumers during the assisted registration process, in particular the need for the collection of that information to be by lawful and fair means, as required under APP 3
- the way in which the consent to be registered for an eHealth record is obtained, particularly to ensure it has been obtained as required by APP 3 and is fully informed
- the manner in which the personal information, once collected, is kept secure in accordance with APP 11.

2.9 As each of the assisted registration policies assessed contained different levels and types of information, each of the recommendations will not apply to all HPOs. The matters covered by the recommendations do not all need to be reflected in an HPO’s assisted registration policy. Rather, the OAIC expects HPOs to use the recommendations to assess whether, when taken together their policies and procedures relevant to assisted registration, they address the privacy risks identified in this report or how they could be improved.

2.10 The scope did not include APP 5 notices that should be issued by the HPOs to notify consumers of certain information required by the Privacy Act when collection of personal information occurs or the HPOs general Privacy Policies.

2.11 The report is structured into: a summary of the recommendations; a summary of the legislation, observations and recommendation in relation to the lawfulness and fairness of the means of collection; a summary of the legislation, observations and recommendation in relation to the security of personal information; and detailed observations of the policies assessed at Appendix A.

Reporting

2.12 To the extent possible, the OAIC publishes final assessment reports in full or in an abridged version on its website: www.oaic.gov.au. It is sometimes inappropriate to publish all or part of a report because of statutory secrecy provisions or for reasons of privacy, confidentiality, information security or privilege.

Part 3 – Summary of the recommendations

3.1 The following is a summary of the recommendations made in Part 4 and 5 of this report. To the extent that HPOs have not already done so in documents and practices not observed by assessors, implementing these recommendations would assist HPOs to minimise potential privacy risks in the assisted registration context:

- **ensuring that privacy requirements are properly addressed in the HPO's policies and procedures** – the HPO's policy documents and procedures should set out the measures that are to be implemented by the HPO to handle personal information in compliance with the relevant privacy requirements when conducting assisted registrations (see related recommendations 1 to 6).
- **ensuring employees undergo adequate privacy training** – providing employees conducting assisted registrations with training on the HPO's approach to handling personal information, including how to implement the relevant policies and procedures of the HPO, to ensure that assisted registrations are conducted in a way that minimises privacy risks (see related recommendation 2). This training would need to be provided in addition to training in the use of the ART software.
- **ensuring that all relevant information is provided to the consumer before they consent to registering for an eHealth record via assisted registration** – the HPO's policies and procedures should specify the information that authorised employees are required to provide to the consumer and the timing of that information being provided. The HPO will need to ensure that consumers are assisted where necessary to understand the information provided (see related recommendation 3)
- **authorising employees** – ensuring that HPOs set clear procedures for the authorisation of employees to conduct the registrations (see related recommendations 4 and 5).

Part 4 – Lawful and fair collection of personal information

Commentary on relevant legislation

Privacy Act

4.1 HPOs that are APP entities under the Privacy Act are required to take steps that are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions and activities that will ensure compliance with the APPs (APP 1.2)

4.2 Under APP 3, HPOs must ensure that personal information is collected by employees from consumers during the assisted registration process in a lawful and fair way (APP 3.5).

4.3 As outlined in the OAIC's *APP Guidelines*, the term 'lawful' is not defined in the Privacy Act. An example of unlawful collection would be collecting information in breach of legislation.[3]

4.4 A 'fair means' of collecting information is one that does not involve intimidation or deception, and is not unreasonably intrusive. Whether a collection uses unfair means will depend on the circumstances. For example, collecting from an individual who is traumatised, in a state of shock or intoxicated will affect the approach required in the circumstances to ensure that the registration is conducted in a fair way.[4]

Consent and assisted registration

4.5 Under APP 3, any consent to the collection of sensitive information, which includes health information, must come from the individual themselves unless an exception applies (APP 3.3).[5]

4.6 Consent can be express or implied. It must be voluntary, informed, current and specific, and the individual must have capacity to consent.[6]

Requirements in the PCEHR Act and PCEHR (Assisted Registration) Rules (AR Rules)

4.7 The relevant requirements in the PCEHR Act and the AR Rules are as follows:

- The System Operator may refuse to register a consumer for an eHealth record if the consumer does not consent to the uploading of their health information (sensitive information) to their eHealth record by registered HPOs involved in their care (s 40, PCEHR Act); in practice this means the consumer's consent is required to register.

- Registrations can only be undertaken by employees (including contractors) of registered HPOs and authorised by that HPO to do so (AR Rule 5).

[3] *APP Guidelines*, paragraph 3.60
[4] *APP Guidelines*, paragraph 3.63
[5] *APP Guidelines*, paragraphs 3.22 and 3.23
[6] *APP Guidelines*, paragraph B.28

- The HPO's policy for assisted registration must set out:
    - the manner of authorising employees to conduct assisted registration (AR Rule 9(a)), and
    - the training that will be provided before an employee is authorised to conduct assisted registration (AR Rule 9(b))
    - the manner of recording a consumer's consent and how that record will be handled for retention purposes (AR Rule 9(c))
    - the process and criteria for identifying a consumer for the purposes of assisted registration (AR Rule 9(d)).
- The registered HPO must check the identity of the consumer who is making the application in accordance with Rule 6 of the AR Rules.

4.8 Through assisted registration, a consumer can apply to be recognised as an authorised representative of a person who is aged under 18 years (AR Rule 3(2)). In addition to being under 18 years, that person must also be:

- co-located on the consumer's Medicare card
- a person for whom the consumer asserts parental responsibility (defined in s 5, PCEHR Act)
- a person who is applying to be registered under section 41 of the PCEHR Act.

4.9 The AR Rules do not provide for a consumer to apply to be recognised as a person's authorised representative for the purpose of registering that person through assisted registration if the person is aged 18 years or over or in any circumstances other than those described above for under 18s.

Observations

4.10 Below are general observations of the policies in relation to the requirement for information to be collected by lawful and fair means under APP 3. Detailed observations of the policies are outlined in Appendix A.

Meeting privacy obligations

4.11 In general, the policies do not set out the privacy obligations that HPOs are subject to in the assisted registration context, or provide clear information about how the HPOs will meet those obligations. The assessors note that these issues may be dealt with in each HPO's internal procedural documents or other policy documents of the HPOs.

4.12 However, two of the policies did include specific references to the HPO's approach to meeting some privacy obligations. One policy listed specific actions that could be implemented to protect both the privacy of consumers and the security of their information (these mainly referred to information security matters which are considered in Part 5 of this report). A second policy included details of the HPO's approach to meeting privacy obligations and referred specifically to the Privacy Act and the NPPs (which were superseded by the new APPs as of 12 March 2014).

Providing the required information to the consumer to obtain informed consent

4.13 None of the policies referred specifically to obtaining the consumer's informed consent to have health information uploaded to their eHealth record. In addition, none of the policies referred to the requirement in AR Rule 8 to inform the consumer of the other available options for applying to register for an eHealth record, apart from assisted registration.

4.14 There was generally a lack of reference in the policies to the particular guidance documents that Health has developed to inform consumers about the consent they are providing when applying to register for an eHealth record. There was also a lack of reference to how and when these documents are to be provided to the consumers to ensure they have received and understood the relevant information.

4.15 Only one of the policies referred specifically to providing the *Essential information* brochure to all consumers interested in registering, and that the consumer needed to understand that information before completing and signing the registration form. Another policy states that staff are required to 'confirm that the Essential information form is provided to the consumer before they give consent for registration'.

4.16 Another policy states 'once the patient has consented to register for their PCEHR they should be provided with the *Essential information* form' – this is of concern because the consumer needs to have read and understood the information included in the brochure before consenting to register.

Legal restrictions on consumers registering on behalf of others via assisted registration

4.17 Two of the policies referred to the restricted eligibility of authorised representatives to register on behalf of others for an eHealth record via assisted registration.

Authorisation of the employee to conduct assisted registrations

4.18 In relation to the requirement that employees be authorised by the HPO to conduct assisted registration (AR Rule 5), in some policies there was a lack of information about how employees were selected for authorisation or which employees were considered 'authorised'; for example, no threshold criteria for selecting employees suitable for authorisation was provided.

4.19 Generally there was an emphasis on the employees being authorised to use the assisted registration software, as opposed to being authorised to conduct the process of assisted registration as a whole.

4.20 Some policies did not identify the officer responsible for the process of authorisation or approving the authorisation.

4.21 Most of the policies referred to maintaining a register of employees that have been authorised to conduct assisted registrations.

4.22 In relation to the training for employees prior to being authorised to conduct assisted registrations (AR Rule 9(b)), most of the policies referred to training in the use of the assisted registration tool to conduct the registration. The policies contained minimal details about the topics the training would cover. Where some details were provided there were no obvious references to training that would cover relevant privacy requirements and the HPO's approach to handling personal information when conducting assisted registrations.

Potential privacy issues

Meeting privacy requirements

4.23 HPOs must comply with a number of requirements in the Privacy Act and PCEHR Act and Rules when conducting assisted registration, in order for the information to be collected by lawful and fair means. It is important that:

- an HPO's policies and procedures address how the HPO will achieve compliance with privacy obligations when conducting assisted registrations
- employees who are subject to an HPO's policy and procedures understand how to implement the HPO's approach to handling personal information, as set out in their policies and procedures, when conducting the assisted registrations.

Recommendation 1

4.24 The OAIC recommends that each HPO's policies and procedures address the HPO's approach to achieving compliance with the requirements of the Privacy Act when collecting personal information through conducting assisted registrations. The OAIC recommends that HPOs achieve this by:

- ensuring that the terms used in the HPO's policies and procedures reflect those used in the Privacy Act and the PCEHR Act and Rules where appropriate
- ensuring that staff are trained in the HPO's approach to ensuring privacy of personal information (as per Recommendation 2 below)
- cross referencing to any other policies and procedures of the HPO that relate to the HPO's approach to meeting the privacy requirements (eg the HPO's APP 1 privacy policy) and information about the relevance of each policy or procedure to the assisted registration process
- allocating responsibility to a particular officer or role for the implementation of the policy and monitoring compliance
- if privacy reference sources are listed in the policy, consider listing the following OAIC privacy resources in addition:
    - the OAIC's *Guide to information security*
    - the OAIC's *A guide to handling personal information security breaches*
    - the OAIC's *APP Guidelines*

Providing appropriate training before employees are authorised

4.25 Employees need to understand the HPO's approach to handling personal information throughout the registration process before being authorised by the HPO to undertake assisted registrations. Employees also need to be able to provide sufficient information to the consumer on assisted registration and the privacy and control aspects of the eHealth system generally to enable the consumer to give their informed consent to the registration (see paragraph 3.1 above).

4.26 The OAIC acknowledges that HPOs will not want to overburden registration staff with large amounts of information, however training should cover the HPO's approach to ensuring privacy is protected including meeting the requirements for information to be collected by 'fair means' under APP 3 and for reasonable steps to be taken to protect the security of that information under APP 11.

Recommendation 2

4.27 The policies and procedures of the HPO should address providing training for employees, before being authorised to conduct assisted registrations. This should include training on the HPO's approach to handling personal information throughout the registration process – including how to implement any relevant policies and procedures. The nature of the training can be tailored to the role of the staff.

4.28 The policies and procedures should also address training to ensure that staff can provide information in response to consumer questions about the information contained in the documents developed by the System Operator and by other parties (such as the HPO itself or NeHTA) that are relevant to the eHealth system, including the controls available to consumers. Employees undertaking registrations should have access to an internal contact point who has a full understanding of the Privacy Act to deal with unusual questions or situations whilst undertaking registrations.

4.29 To ensure that assisted registrations are conducted in a fair way, HPOs should consider whether training should include the HPO's approach to managing situations where consumers may be less able to clearly understand privacy issues or the detail of the eHealth System; for example, consumers in vulnerable groups, older persons or consumers with English as a second language.

Providing sufficient information to obtain informed consent to registration

4.30 In order for consumers to provide informed consent to both the collection of their personal information for the purpose of registering and to the uploading of health information to their eHealth record, it is important that consumers:

- are provided with the correct information (including the consumer information developed by the System Operator) in an understandable and accessible format in the particular circumstances of assisted registration

- understand what collections will occur, including the collection of their personal information by the HPO during the assisted registration process, and the subsequent collection of their health information via uploads to their eHealth record by HPOs or the System Operator

- have been given enough time to consider the information provided, in order to make an informed decision based on that information.

4.31 HPOs may need to provide additional information to consumers to help them understand the information in the documents developed by the System Operator.

4.32 Other issues could include consumers apprehending that there is pressure to register – for example if they are not made aware of the fact that registration is voluntary and that if they do wish to register there are other methods available apart from assisted registration. AR Rule 8 requires that consumers are advised of other methods for registration.

Recommendation 3

4.33 The OAIC recommends that HPOs ensure that their policies and procedures include a requirement that sufficient information is provided to the consumer to give informed consent (including that registration is voluntary and that other methods are available). This may involve:

- specifying the information that must be provided to the consumer (eg the *Essential information* brochure developed by the System Operator)
- specifying the timing of providing the information during the assisted registration process
- specifying that the consumer is given enough time to consider the information provided
- training staff to provide information in response to consumer questions as described in recommendation 2 above.

4.34 HPOs may need to address the accessibility of information provided to consumers during the assisted registration process in their policies and procedures. For example, this may involve specifying that the information be read aloud to the consumer where necessary.

Authorisation of the employee to conduct assisted registrations

4.35 Employees of a registered HPO must be appropriately authorised by their HPO to conduct the assisted registration under the AR Rules (AR Rule 5). Many policies did not set out the process for that authorisation to occur or the role that the employee would undertake, but rather focused on the fact that a register would be kept once authorisation had occurred.

Recommendation 4

4.36 The OAIC recommends that HPOs include in their policies and procedures information about the process for authorising an employee to conduct an assisted registration, including:

- the person or position responsible for the authorisation
- a position description for the authorised employee’s role
- detail of the training to be undertaken
- that a register is kept of the authorised employees, and the details included (for example, name, training completed).

Limits to registration via assisted registration

4.37 There are restrictions on the eligibility of authorised representatives to register others via assisted registration, as set out in the AR Rules (AR Rule 3(2)). The AR Rules do not allow authorised representatives to register another adult (a person 18 years or over) through assisted registration, even if they are an authorised representative for that person.

Recommendation 5

4.38 The OAIC recommends that the HPOs’ policies and procedures reflect the limitations on authorised representatives registering others via assisted registration as set out under the AR Rules which outline the circumstances in which an authorised representative can register on behalf of another person who is under 18 years (AR Rule 3(2)).

Part 5 – Information security

Commentary on relevant legislation

5.1 Under APP 11.1, an APP entity must take reasonable steps to protect the personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

5.2 Under APP 11.2, where an APP entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that it is de-identified.[7]

5.3 The AR Rules contain a requirement that HPOs store the record of the consumer's consent for at least three years or provide it to the System Operator, or both (AR Rule 7(3)).

5.4 For further information on information security requirements under the Privacy Act, HPOs should refer to the OAIC's *Guide to information security*, which is available on the OAIC website. The guide outlines some of the circumstances that the OAIC takes into account when assessing the reasonableness of the steps taken by entities to ensure information is kept secure. While not exhaustive, the guide provides a framework which the OAIC uses in its information security assessments.

5.5 For further information on handling and responding to breaches to the security of personal information, HPOs should refer to the OAIC's *A guide to handling personal information security breaches*. The document includes information about notifying individuals when a breach occurs, and outlines that notification may be considered a reasonable step in keeping personal information secure.

Observations

5.6 Below are general observations that are relevant to the requirement in APP 11 to take reasonable steps to handle personal information securely. Further detailed observations are outlined in Appendix A.

Information security regarding personal information including physical copies of assisted registration application forms and use of IT

5.7 Each of the policies refers to some information security measures that promote the secure use of IT while conducting assisted registrations. Some policies contained more detailed information security measures than others.

5.8 In relation to the signed assisted registration forms, each of the policies refer to some information security measures that ensure the physical security of the copies of assisted registration application forms. Some policies contained more detailed information security measures than others.

[7] *APP Guidelines*, paragraph 11

5.9 A collective list of the measures observed in the policies is set out in Appendix A. These are generally of an operational nature and collectively are very useful and should be considered. However, they do not necessarily address the increased privacy risks inherent in assisted registration discussed in this report. Each HPO will need to consider what measures to include in their policies and procedures in order to comply with privacy requirements.

Handling of identification documents

5.10 In relation to identification documents most of the policies refer to 'sighting' them only. One of the policies refers specifically to employees not being required to retain a copy of the person's identification.

Reporting unauthorised access, use or disclosure of personal information

5.11 Some of the policies refer to requiring employees to report any unauthorised use or misuse of the assisted registration software, and some policies refer to staff conduct and disciplinary policies in relation to misuse of the software or the assisted registration process. The policies that include these requirements also include the officer responsible for implementing these processes.

5.12 Some of the policies require employees to report any breaches of the PCEHR Act to a particular officer, in addition to reporting any employee misuse or misconduct. One of the policies includes as an appendix a 'PCEHR breach report' template for employees to use.

5.13 One of the policies requires that any breach include 'loss, damage or theft of personal information' be reported as soon as it occurs, and that possible information security breaches including 'accidental loss, damage or theft of personal information' be reported to the CEO and the Department (Health).

Potential privacy issues

HPOs approach to ensuring compliance with information security requirements

5.14 As assisted registration involves the HPO collecting personal information in both hard copy and, if scanned and stored, electronically, privacy risks can arise if the information is not stored or handled securely and as a result is at risk of being misused or lost or open to unauthorised access or disclosure.

5.15 HPOs will need to be mindful that if registration forms are scanned and uploaded to the System Operator through the ART, electronic versions of that form may remain. For example, they may remain in the hard drive of the scanning machine or on the computer used to send the form to the System Operator through the ART.

5.16 It is necessary for HPOs to have policies and procedures in place about information security to both prevent information security or data breaches occurring, and to have a plan for containing and managing the response in the event of a breach.

Environmental factors affecting information security

5.17 The location or environment in which assisted registrations are conducted can affect the steps that would be reasonably required to be taken by the HPO and their employee to ensure that the registration is conducted securely. Additional steps may be required if, for example, the registration is being conducted in an open, shared and busy location such a hospital ward, emergency department or GP waiting room or if documents (both paper and in electronic form on shared computers) cannot be kept secure.

Recommendation 6

5.18 The OAIC recommends that in developing their policies and procedures, that HPOs have regard to the matters set out in the OAIC's *Guide to information security* and the OAIC's *A guide to handling personal information security breaches.*

5.19 The OAIC recommends that HPOs ensure that their policies and procedures:

- address their approach to implementing information security measures, making specific reference to the particular circumstances which apply to assisted registrations that may increase privacy risks and require additional measures to comply with privacy requirements – such as whether the locations for conducting assisted registrations present risks to privacy, and how physical and electronic copies of personal information will be kept secure in those particular environments
- address their approach to ensuring that employees are aware of information security requirements before being authorised by the HPO to undertake assisted registrations. This may include providing training in the relevant legislative privacy requirements (as per Recommendation 2 above)
- including a specific reference in the policies and procedures that copies of identification documents are not to be collected by employees conducting assisted registrations (Health's *Assisted registration guide for HPOs* notes that taking copies of the documents is not required)
- address the HPO's procedures for responding to data breaches or other information security incidents, and the details of officers or positions responsible for managing the response and for decisions regarding information security.

Appendix A – detailed observations of the policies assessed

Lawful and fair collection of personal information (Part 4)

The detailed observations for Part 4 are set out below.

As noted previously, this assessment only assessed the HPOs' assisted registration policies. There may be other related policy documents and procedures of the HPOs (including training documents, privacy policies and collection notices) that are relevant to assisted registration. The assessors note that the other related policy documents and procedures of the HPOs may address the potential deficiencies observed with the assisted registration policy documents assessed.

References to the Privacy Act, APPs, PCEHR Act and Rules

A1. Most of the policies do not specifically refer to the Privacy Act, the National Privacy Principles (NPPs, now the APPs) and the HPO's privacy obligations under them. Some of the policies did refer to the NPPs (now APPs) however they do not explain the relevance of the privacy obligations in the NPPs to the assisted registration process. Further, although the policies all reference the PCEHR Act, some of the policies make no reference at all to either the Privacy Act or the PCEHR Rules, or PCEHR (AR) Rules.

A2. One of the policies does refer specifically to the need for authorised employees to 'maintain confidentiality of records at all times in accordance with the Privacy Act' and another policy referred to the fact that managing the privacy of patients is the responsibility of the HPO.

A3. One policy includes, as an appendix, a 'Confidentiality agreement' to be signed by employees who may have access to confidential patient data, in order to comply with privacy requirements under legislation including the Privacy Act – for example, the confidentiality agreement requires an employee to agree to notify their supervisor immediately if they become aware of any breach of privacy or information security in the course of their duties.

A4. In a number of the policies there is a lack of emphasis on the HPO's approach to the process of assisted registration generally (in addition to the use of the Assisted registration tool software), and the HPO's approach to meeting the relevant privacy and information security obligations.

A5. For example, some of the policies refer in the opening paragraph to the policy providing 'an understanding of how the software will be implemented and used' – although this is important, the policy should also relate more broadly to the assisted registration process including the HPOs approach to managing the relevant privacy and information security requirements.

Use of terminology that is consistent with the legislation

A6. Some of the policies use or refer to terminology that is not consistent with the terms used and defined in the Privacy Act, PCEHR Act and Rules. For example, where the policies describe the information handled by the HPO they do not refer to the collection of ‘personal information’ or ‘sensitive information’, as defined in the Privacy Act, as part of the process of conducting assisted registration.

Reference documents that may include privacy and information security measures used by the HPO

A7. Some of the policy documents list other policies of the HPO that operate in conjunction with their assisted registration policy that may cover privacy matters relevant to the registration of consumers – such as the HPO’s privacy policy, PCEHR policy, or the HPO’s PCEHR assisted registration software tool procedures. However, there is no information provided about the relevance of those policies to the HPO’s approach to conducting assisted registrations in compliance with the privacy and information security requirements in the legislation. The same is the case with other reference documents listed in the policies such as the *RACGP Computer and Information Security Standards*.

Implementing the policy

A8. Not all of the policies identify the particular officer or position responsible for the implementation and monitoring of compliance with the policy or how often the policy needs to be reviewed and updated.

Authorisation of employees including training requirements

A9. Most policies include a statement to the effect that ‘training must be completed before employees are authorised to perform assisted registration’. This is compliant with the requirement in AR Rule 9(b) to specify training that is to be completed *before* conducting assisted registrations.

A10. Some of the policies are not clear about who the organisation views as an ‘authorised employee’ for the purpose of conducting assisted registrations in line with the policy. For example, one of the policies refers to ‘training staff within external organisations to provide assisted registration’[8]. However, other policies provide greater clarity. In particular, one of the policies provides the organisation’s definition of an ‘authorised employee’ for the purpose of conducting assisted registrations.

A11. Some of the policies use terms referring to authorised employees that do not necessarily match with the definition of the term ‘employee’ given in s 5 of the PCEHR Act, and Rule 5 of the AR Rules. This could contribute to confusion about the implementation of the policy. For example, one of the policies refers to an authorised employee being someone who has ‘agreed to assist the organisation facilitate the assisted registration workflow’.

A12. Another policy refers to ‘authorised users’ of the assisted registration tool, rather than ‘authorised employees’, and focusses the employee authorisation criteria on competence in the use of the software.

[8] The assessors note that if staff of other organisations are undertaking assisted registration, those organisations would need their own assisted registration policy.

A13. Some of the policies contain a statement in the first paragraph which authorises the HPO's staff generally to use the assisted registration tool, without any reference to the requirement for employees to be authorised and the threshold criteria for authorisation, however the policies later include the specific employee authorisation requirements. This creates uncertainty around how to apply the authorisation requirements.

A14. In relation to employee authorisation and training, which is required to be set out in the policy as per the AR Rules, the following was observed:

- some of the policies did not specify the position or person in the organisation that was responsible for authorisation of the employees
- some policies referred to maintaining a register of authorised employees and a record of the training completed by those employees, while other policies did not
- some policies were not clear in their description of the organisation's approach to authorising an employee and ensuring that the required training is completed prior to authorisation

A15. In some policies information was provided about how employees are authorised to conduct assisted registrations. For example, there are brief references to the 'minimum training' required, which is usually described as the employee being able to use the Assisted Registration Tool User Guide provided by the System Operator. Other policies provided more detailed information about the type of training employees are required to complete prior to authorisation, such as an introduction to eHealth.

A16. Other policies referred to the training that will be provided as 'full training', however the training referred to in those policies did not include references to training on the assisted registration process or eHealth registration generally, and does not appear to refer to training that would necessarily cover the relevant privacy and information security considerations.

A17. Some of the policies refer to the requirement that employees be trained in the HPO's document handling procedures, which would involve training on information security considerations.

A18. One policy referred to training consisting of '1.5 days of theory training and half a day in the field conducting registrations' and referred the reader to training materials stored on the HPO's internal website for details about the training program.

Eligibility to register others via assisted registration

A19. One of the policies specifically refers to the conditions (set out under the AR Rules) for authorised representatives registering dependents who are under 18 years of age, which include that:

- they can be registered if they are listed on the same Medicare care as the consumer (parent)
- the consumer registering the dependent must indicate that they have parental responsibility for the dependent

- dependents that are between 14 years and under 18 years are eligible to apply for their own record if they prefer

A20. One of the policies specifically refers to not being able to offer assisted registration to consumers who are under enduring guardianship, which includes a consumer acting as an authorised representative of another person aged 18 years or over.

Information security (Part 5)

The detailed observations for Part 5 are set out below.

Addressing privacy and information security obligations

A21. The HPO policies varied in how and whether they addressed the requirement to conduct assisted registrations in a way that would be compliant with information security and privacy obligations.

A22. Some policies provided detailed lists of privacy and information security reference documents such as the *RACGP computer and information security standards*, the relevant HPO's privacy policy, or document handling policy, and also the relevant legislation. However there was no additional information provided as to the relevance of each reference document to the conduct of assisted registrations by the HPO.

A23. One policy used the words 'when [Assisted registration tool] is used to assist a consumer to register, appropriate measures must be taken to protect the privacy of a consumer' and listed examples of specific measures that could be implemented to protect the privacy of a consumer and the security of their information.

A24. One policy outlined the organisations approach to achieving compliance with the NPPs (now APPs) relevant to information security by including statements about the following:

- data quality
- data information security
- access and correction
- anonymity
- interstate data flows

Information security measures in relation to signed registration forms

A25. In relation to copies of the signed registration forms, the policies refer to either some or most of the following information security measures:

- secure treatment of the hardcopy forms:
  - sending the forms securely by express post, or registered post, to the System Operator within 30 days of processing
  - submitting completed forms at the end of each business day
  - providing employees with a secure system for transporting patient information from other sites to the HPO, for example locked satchels

    - use of locked cabinets and locked satchels to store hardcopies
    - requiring that any printed or written materials containing consumer's details must not be left unattended or unsecured
    - securely disposing of unwanted printouts and keeping any forms that are retained in a secure environment
- access to the forms (only to staff trained and authorised to perform assisted registration)
- setting out the length of time that the completed forms will be stored by the HPO, and that following the retention period the forms will be securely destroyed.

A26. One of the policies sets out the length of time that records of 'unsuccessful registrations' would be kept before being securely destroyed and processes for follow up contact with the consumer.

Information security measures in relation to software systems

A27. In relation to software systems used in conducting an assisted registration, the policies refer to either some or most of the following information security measures:

- staff not being allowed to access or attempt to use the assisted registration software until they have completed required training
- that where possible, entering or viewing consumer's details should not be performed in an open area
- that all the consumer data must be cleared from the screen where appropriate e.g. if sharing a computer or in an open area
- that computer screens must be locked when unattended
- ensuring staff use their unique network username when using the software, for audit purposes
- information security requirements for handling a consumer's eHealth Personal Identification Code (PIC), to prevent unauthorised use or access
- information security requirements for accessing the eHealth record system using a a National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) certificate
- information security requirements for handling the consumer's eHealth Identity Verification Code (IVC) – including that the IVC shall not be retained, stored or saved once issued to the consumer
- the proper use of the HPI-O certificate and password to ensure information security when using the assisted registration software
- ensuring authorised employees adhere to the HPO's password management policy
- ensuring the organisation has current IT system anti-viral software
- ensuring the organisation has current disaster recovery policies and procedures
- ensuring the organisation's IT systems and hardware are physically protected against unauthorised access

- keeping a secure register of all contacts made with consumers using their personal contact details e.g. use of email or mobile phone numbers.