Contents

Recommendations ................................................................................................................. 3
The Office of the Australian Information Commissioner ........................................................ 5
Involvement of the OAIC in the PCEHR System ................................................................. 6
Comments .......................................................................................................................... 6
Background .......................................................................................................................... 7
  3.2 Participation .................................................................................................................... 7
  3.3 Privacy ............................................................................................................................ 7
  3.4 Security .......................................................................................................................... 8
PCEHR regulations .............................................................................................................. 9
  4.4.4 Nomination of members .......................................................................................... 9
PCEHR rules .......................................................................................................................... 9
  5.2 Access control mechanisms ......................................................................................... 9
    Advanced access controls ............................................................................................... 10
    Access flags for registered healthcare providers ......................................................... 11
  5.3 Identity verification ...................................................................................................... 12
  5.4 Restrictions on records that may be uploaded by healthcare providers to the PCEHR System .......................................................................................................................... 12
  5.5 Participation requirements ......................................................................................... 12
  5.6 Technical specifications .............................................................................................. 13
Issues not dealt with in the proposal .................................................................................. 13
Pseudonyms ......................................................................................................................... 13
Recommendations

The OAIC notes the *Personally Controlled Electronic Health Record System (PCEHR): Proposals for Regulations and Rules* (the proposal) outlines the main provisions proposed to be included in the PCEHR regulations and rules to be made under the *Personally Controlled Electronic Health Records Bill 2011* (PCEHR Bill)¹, and outlines the reasons behind those proposals and how they would operate.

The OAIC strongly supports introducing PCEHR regulations and rules to accompany the PCEHR Bill and *Personally Controlled Electronic Health Records (Consequential Amendments) Bill 2011* (PCEHR Consequential Amendments Bill)² which will, when enacted, support the implementation and operation of the PCEHR system.

The recommendations below are provided to the Department of Health and Ageing (DoHA) to assist the development of PCEHR regulations and rules which establish a robust regulatory framework and incorporate strong privacy protections for consumers who opt-in to the PCEHR:

1. Effective consultation and discussion between healthcare providers and consumers is essential to ensure that healthcare providers and consumers have a shared understanding about the information that is to be uploaded to the PCEHR system. The default position should not be that consumers grant standing consent to have all their health information uploaded by virtue of opting into the PCEHR system.

2. Consumers should be able to view which healthcare providers have accessed their PCEHR via the audit trail at an individual level. This will provide an important level of assurance and control for consumers and will also mean that any possible unauthorised access can be easily identified.

3. A data security provision should be included in the PCEHR rules. The provision could be modelled on National Privacy Principle 4.1 in Schedule 3 of the *Privacy Act 1988* (Privacy Act).

4. The PCEHR rules should establish a ‘no access’ control mechanism which could apply to clinical documents. Documents labelled ‘no access’ should only be accessible by the consumer and the author of the document.

5. The advanced access controls should allow consumers to distinguish or group their ‘limited access’ documents, so that healthcare providers could be given access to particular ‘limited access’ documents only.

6. The PCEHR rules should require healthcare provider organisations to make information available to consumers about how access flags are assigned for their organisation, for example, by publishing brochures or on the organisation’s website.

7. The rules should require the System Operator to comply with the requirements of the Privacy Act when satisfying itself that the identity of a consumer has been appropriately verified.

8. Technical specifications should not be included in the PCEHR rules. Instead, the technical specifications could be better regulated by the System Operator in a separate document.

9. The requirements for registering a consumer who has been issued a healthcare identifier under a pseudonym should be included in the rules. The OAIC supports giving individuals the clear option to transact pseudonymously to protect their privacy, where this is lawful and practicable.
The Office of the Australian Information Commissioner

The Office of the Australian Information Commissioner (the OAIC) is established by the Australian Information Commissioner Act 2010 (Cth)\(^3\) (the AIC Act) and commenced operation on 1 November 2010. The OAIC is an independent statutory agency headed by the Australian Information Commissioner. The Information Commissioner is supported by two other statutory officers: the Freedom of Information Commissioner and the Privacy Commissioner. The former Office of the Privacy Commissioner was integrated into the OAIC on 1 November 2010.

The OAIC brings together the functions of information policy, and independent oversight of privacy protection and freedom of information (FOI), in one agency, to advance the development of consistent workable information policy across all Australian government agencies.

The Commissioners of the OAIC share two broad functions:

- the FOI functions, set out in s 8 of the AIC Act – providing access to information held by the Australian Government in accordance with the Freedom of Information Act 1982 (Cth),\(^4\) and
- the privacy functions, set out in s 9 of the AIC Act – protecting the privacy of individuals in accordance with the Privacy Act 1988 (Cth)\(^5\) (the Privacy Act) and other legislation.

The Information Commissioner also has the information commissioner functions, set out in s 7 of the AIC Act. Those comprise strategic functions relating to information management by the Australian Government.

As the national privacy regulator the OAIC can provide general advice on privacy issues and the application of the Privacy Act.

The Privacy Act applies to ‘personal information’, which is defined in s 6(1) as information or an opinion, whether true or not, about an individual whose identity is apparent or can be reasonably ascertained from that information. The Privacy Act contains eleven Information Privacy Principles (IPPs) which apply to Australian and ACT Government agencies. It also includes ten National Privacy Principles (NPPs) which generally apply to private sector organisations, but which do not apply to certain exempt organisations including some small businesses and State or Territory authorities.\(^6\)

Health information is a subset of personal information and also defined in s 6(1) of the Privacy Act. In the PCEHR Bill, the information included in a consumer’s PCEHR is referred to as health information. The definition of health information in the PCEHR Bill and the Privacy

Act is substantially the same. The only difference is that under the PCEHR Bill the definition uses the term healthcare rather than health service. Despite this difference, it is intended that health information have same meaning under the PCEHR Bill as it does under the Privacy Act.⁷

Involvement of the OAIC in the PCEHR System

The OAIC has been actively involved to ensure that privacy protections are built into the PCEHR system. The OAIC made the following submissions to Department of Health and Ageing (DoHA) on the PCEHR system:

- The Draft Concept of Operations relating to the introduction of a PCEHR system, in June 2011⁸
- The Legislation Issues Paper, in August 2011⁹

The OAIC also made a submission to the Senate Community Affairs Legislation Committee regarding its inquiry into provisions of the PCEHR Bill 2011 and a related Bill, in January 2012.¹¹

The OAIC will have the role of independent privacy regulator for the PCEHR. The PCEHR Bill confers functions and powers on the Australian Information Commissioner to investigate acts and practices that may be contraventions of the Bill, take enforcement action, provide advice and guidance to PCEHR participants about their privacy obligations when handling healthcare information and report annually to the Minister. To support these functions, the OAIC has signed a Memorandum of Understanding with DoHA which extends to 30 June 2012.

Comments

The PCEHR system aims to give individuals personal control over their health information. Individuals decide whether or not to have a PCEHR, and if they choose to have one, then what information goes into their PCEHR and who gains access to this information. Consumer confidence in the PCEHR system is contingent in part on whether it is secure and provides robust privacy protections. The PCEHR Bill provides that a number of the key privacy protections will be set out in the PCEHR regulations and rules. The OAIC understands the PCEHR rules are intended, in particular, to cover fundamental aspects of the PCEHR system.

---

⁷ Explanatory Memorandum to the PCEHR Bill, p 5.
such as access control mechanisms, identity verification, participation requirements and authorised representatives and nominated representatives.

These are important matters that impose requirements on participants about how health information held within the PCEHR system should be handled. Our submission includes some comment on aspects of the overall regulatory framework as well as the specific proposals for the regulations and rules.

Background

3.2 Participation

The OAIC is concerned that the proposal states that ‘As part of registration, consumers will grant standing consent for their health information to be uploaded to the PCEHR system’. The OAIC considers that this position may reduce consumers’ control of their health information held in their PCEHR.

In general, the OAIC considers that good privacy practice involves individuals maintaining a level of control over when, and to whom, their information is disclosed. For this reason, it is our view that when a consumer opts to have a PCEHR, the default position should not be that the consumer grants standing consent to all healthcare providers to upload all their health information to the PCEHR system.

A better approach would be for healthcare providers to only upload a consumer’s health information into the PCEHR system where there has been appropriate communication and an understanding between healthcare provider and consumer such that it is clear that the consumer consents to their health information being uploaded. Particularly when a consumer visits a new healthcare provider, there should be some discussion about whether the consumer is comfortable with all health information and clinical documentation being uploaded to the consumer’s PCEHR. Further, for particularly sensitive health information, for example regarding mental health, it may be appropriate for the consumer to expressly consent to the information being uploaded.\(^\text{12}\)

3.3 Privacy

The OAIC supports that key measures have been incorporated into the PCEHR Bill to protect privacy including those outlined in the proposal which:

- enable consumers to control which healthcare provider organisations may access their information
- set closely defined limits on the circumstances in which health information may be accessed outside of those controls
- give consumers the ability to view an audit trail of all access to a consumer’s PCEHR

impose penalties and other sanctions for unauthorised viewing of and access to records; and

place obligations on certain PCEHR participants to report all data breaches.

3.4 Security

An important feature of the PCEHR system is that consumers will be able to access an audit trail for their PCEHR which will identify which organisations have accessed their PCEHR and the nature of that access. This will increase transparency and allow consumers to report any possible unauthorised collection, use or disclosure of their health information. The OAIC understands that the audit trail will establish a summary of the flows of information in relation to a consumer’s PCEHR and will be available electronically.13

The OAIC recommends that the PCEHR rules should provide that consumers are able to view which healthcare providers have accessed their PCEHR at an individual level, so that any possible unauthorised access can be easily identified. This capability will also be important from a compliance perspective in enabling the OAIC to identify each individual (by name and healthcare identifier where possible) that has accessed the PCEHR via the audit trail. However, in audit logs viewed by consumers, individual healthcare providers could be identified by their role/branch rather than by name or other unique identifier; for example, the audit trail could display ‘registered nurse, intensive care unit, Western Hospital’.

It is also important for organisations handling personal information to have appropriate security protections in place to limit the risk of a data breach. The OAIC has previously recommended14 that data security provisions which would apply uniformly to the system Operator, portal operators and repository operators should be included in the PCEHR Bill. The OAIC considers that imposing a positive, consistent data security requirement would reinforce the importance of protecting the security of individuals’ health information, in circumstances where different privacy laws may otherwise apply. It could also form the legislative basis for an appropriate civil penalty provision for a serious breach of data security requirements in relation to information held in the PCEHR system to apply uniformly across all jurisdictions. This ensures that PCEHR consumers throughout Australia have access to the same data security protections.

The OAIC’s recommendation was not adopted and there is no such provision in the current version of the Bill. For that reason, the OAIC recommends that a data security provision be included in the PCEHR rules. Such a provision could be modelled on National Privacy Principle 4.1 in Schedule 3 of the Privacy Act. This provision states that ‘an organisation

---

13 Clause 15(h), PCEHR Bill.
must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure’. By virtue of s 78 of the PCEHR Bill, a breach of the provision could lead to the imposition of civil penalties.

**PCEHR regulations**

**4.4.4 Nomination of members**

The OAIC supports the proposal that the Minister will be required, before appointing a person as a member of the Independent Advisory Council, to request specified bodies to nominate a person for appointment to the Council. The OAIC notes it is proposed that it is one of the bodies who will be requested to nominate a person with experience or knowledge in law and/ or privacy for the appointment to the Council in accordance with cl 27(2)(b)(iii) of the PCEHR Bill. The OAIC welcomes this opportunity and considers it is well placed to make such nominations.

**PCEHR rules**

**5.2 Access control mechanisms**

Effective, patient-centred access controls are one of the key elements of the PCEHR. The OAIC considers that the implementation of clear and robust rules about PCEHR access control mechanisms is critical to the success of the system, and fundamental to consumer uptake. The rules will need to contain appropriate access controls to reduce privacy risks and satisfy consumers that their personal information is secure within the system. Without effective access controls, there is a risk that consumers’ health information will be more widely available than the consumer intended.

The OAIC welcomes the proposal that consumers will have a choice about whether they apply default ‘basic access controls’ or ‘advanced access controls’ over their PCEHR. The OAIC also supports the proposal that regardless of the access settings a consumer chooses, they will have the option of being electronically notified when a new organisation accesses their PCEHR, when a new shared health summary has been uploaded and when a nominated representative has accessed their PCEHR. Allowing consumers to view healthcare provider organisations on their access list, and remove providers from the access list, is an important aspect of the proposed rules which gives consumers greater control over their health information and enhances consumers’ privacy.

However, the OAIC recommends that the PCEHR rules should establish a ‘no access’ control mechanism which could apply to clinical documents in addition to ‘general access’ and ‘limited access’ mechanisms outlined in the proposed arrangements. The OAIC notes that a ‘no access’ control mechanism was included in the *Draft Concept of Operations: Relating to*

---

the introduction of a PCEHR system. The OAIC understands that ‘no access’ documents would have only been accessible to the organisation which supplied them and could not be accessed by organisations in emergencies. In contrast, ‘limited access’ documents may be accessed in emergencies.

We note that the ‘no access’ feature was removed from the final version of the Concept of Operations. Further, it has not been included in the proposed PCEHR rules. Under the currently proposed model, all clinical documents loaded onto the system would be able to be accessed in emergencies. The OAIC suggests that further consideration be given to reinstating a ‘no access’ control mechanism. In doing so, the OAIC recognises that there may be emergency situations where a person could potentially be significantly disadvantaged by having made the choice to label documents as ‘no access’. However, as long as consumers are appropriately educated about the possible consequences, this should be a matter of informed individual choice.

**Advanced access controls**

The proposal to include advanced access controls in the PCEHR rules indicates that consumers will also be given the option to control access to clinical documents in the PCEHR. In principle, the OAIC supports this proposal. However, the OAIC understands that once a consumer, using advanced settings, gives a healthcare provider organisation a special provider access consent code (PACCX) that organisation will be able to access all documents in a consumers’ PCEHR marked ‘limited access’. It is not clear whether all connected or subordinate providers with an access flag will also gain access to ‘limited access’ documents. The OAIC recommends that only the individual healthcare provider who is given a consumer’s PACCX be given access to ‘limited access’ documents, not all associated providers with an access flag.

The proposal does not seem to deal with the limitation that prevents consumers from granting access to one particular ‘limited access’ document, or a group of documents relating to one particular health issue. This reduces the ability for consumers to manage the privacy of their clinical documents. This will be particularly problematic for consumers with comorbidity relating to two or more disorders. For example, a consumer may be sensitive about a mental health condition, a skin condition and a sexual health condition and may label all documents related to these three conditions as ‘limited access’. However, that consumer may wish for their psychologist to be able to view all documents related to their mental health, but not to view documents relating to a skin condition or sexual health. The OAIC recommends that the access controls allow for ‘limited access’ documents to be grouped, for example, into clinically appropriate groupings and for access to be granted by group.

---

17 The Draft Concept of Operations: Relating to the introduction of a personally controlled electronic health record (PCEHR) system (Draft ConOps) was released by the Department of Health and Ageing for public comment on 12 April 2011.
18 Draft ConOps p 57.
Access flags for registered healthcare providers

The proposal indicates that an ‘access list’ will be kept that shows which registered healthcare providers have accessed a consumer’s PCEHR at an organisational level, rather than at the level of the individual healthcare provider. The extent of healthcare provider organisation access will be based on the access flags assigned to the healthcare provider organisation. The OAIC notes that the purpose of the access flags is to limit the extent to which access to a PCEHR is available to related entities once a healthcare provider organisation is authorised to access a consumer’s record. The limitations aim to align access to consumers’ PCEHRs with consumer expectations of privacy and information flows during treatment.20

The OAIC appreciates that this approach may be necessary to allow PCEHRs to be used effectively in large organisations. However, the OAIC considers that a cautious approach should be taken when assigning access flags. Seed organisations21 that are responsible for assigning flags should consider treating some branches or departments of healthcare provider organisations as separate for the purposes of access flags even if the branch or department is not providing services in its own name. For example, consumers may not expect that general hospital staff will have access to their PCEHR when they are receiving treatment at a drug and alcohol rehabilitation clinic or mental health outpatient service which is part of a hospital.

Further, the OAIC considers that the PCEHR rules should require healthcare provider organisations to make information available to consumers about how access flags are assigned for their organisation, such as, by publishing brochures and having them available to consumers when they are registering for a PCEHR or having information available on the organisation’s website. This would help ensure consumers have the ability to make informed choices about who has access to their health information and is consistent with requirements in the Privacy Act that individuals be given notice about how their information will be used and to whom it will be disclosed. Making this information available to consumers will also reduce the risk of complaints arising from unexpected access to a consumer’s PCEHR.

Regardless of the way a seed organisation arranges its access flags, it will be important for healthcare provider organisations to ensure that only those employees or contractors who require access for the delivery of healthcare services access an individual’s PCEHR. In this regard, the OAIC strongly supports the proposed arrangements in Part 5.5. Part 5.5 requires healthcare provider organisations to develop, maintain, enforce and communicate, policies and procedures in relation to access and account management practices ensuring good information security access management practices. It also requires providers to train their

21 Seed organisations and network organisations are defined in subsections 9A(3) and (6) respectively of the Healthcare Identifiers Act 2010. Seed organisation within a network hierarchy will be responsible for setting ‘access flags’ for the seed organisation and all network organisations within the healthcare provider organisation’s network hierarchy.
employees on how to use the system accurately and responsibly and ensure they are informed of their legal obligations.

Given the complexity of the access control mechanisms outlined in the proposed arrangements, the OAIC considers that the rules should include a requirement that the System Operator must educate consumers about access controls. The OAIC notes that cl 15(m) of the PCEHR Bill broadly requires the System Operator to educate consumers, participants in the PCEHR system and members of the public about the PCEHR system. However, specific obligations around access control education for consumers should be outlined in the rules.

5.3 Identity verification

The OAIC supports the proposal that as a minimum requirement in relation to identity verification for the purposes of cl 41(1)(c), the System Operator must be satisfied that the consumer has a verified individual healthcare identifier (IHI). The OAIC considers that identity verification is critical to the security and integrity of the PCEHR system.

However, the System Operator should also ensure that it complies with the requirements of the Privacy Act when satisfying itself that the identity of the consumer has been appropriately verified. For example, consistent with Information Privacy Principle 1.1, the System Operator must only collect the minimum identifying information necessary to verify a consumer’s identity.

5.4 Restrictions on records that may be uploaded by healthcare providers to the PCEHR System

The OAIC supports the proposal that the rules will require all records, other than shared health summaries (which are dealt with in the PCEHR Bill), to be uploaded to the PCEHR system must have been authored by a healthcare provider who has been assigned a healthcare identifier under s 9(1)(a) of the Healthcare Identifiers Act 2010. This will be critical not only for clinical safety but also to ensure that the identity of the person or organisation uploading a document to the PCEHR can be verified.

This functionality will be particularly important for the OAIC’s compliance activities, for example, it will be useful if the OAIC is undertaking an investigation into a complaint about a possible unauthorised collection, use and disclosure of health information included in a consumer’s PCEHR.

5.5 Participation requirements

The OAIC supports the proposed requirement in the rules that healthcare provider organisations, in order to be eligible to register, must develop, maintain, enforce and communicate to their staff and policies and procedures relevant to their access to the PCEHR system. The OAIC considers that requiring healthcare providers to address the issues of staff authorisation, suspension and deactivation of access, staff training, identification of authorised access, security of IT equipment, use of physical and system access controls and
mitigation strategies will enhance the privacy and security of the system and reduce the risk of unauthorised use, collection and disclosure of health information.

Further, the OAIC considers the proposal that organisations must implement access and account management practices that ensure all authorised users’ accounts accessing the PCEHR system employ good information security access management practices supports the protection of sensitive health information within the PCEHR system.

However, the OAIC suggests that, if a specific rule is not made setting out the data security obligations of PCEHR participants and no obligations are included in the PCEHR Bill, then consideration is given to making the participation requirements relating to IT security more comprehensive.

5.6 Technical specifications

The OAIC is concerned that the technical specifications that will apply to healthcare provider organisations, repository operators, portal operators and contracted service providers will be published as a schedule to the PCEHR rules. Clause 78 of the PCEHR Bill provides that a civil penalty may apply if a person that is, or has at any time been, a registered repository operator or a registered portal operator contravenes a PCEHR rule that applies to the person. Under cl 79 of the PCEHR Bill, the Information Commissioner is the only person who may apply to a Court to seek the application of a civil penalty order. The issue for the OAIC is that technical specifications may fall outside the scope of privacy regulation, which may limit the Information Commissioner’s ability to effectively investigate a possible breach and seek a civil penalty order. For example, if an entity does not comply with a rule in the schedule relating to a particular software interoperability specification, but no data breach or interference with privacy has resulted, the Information Commissioner may not have the appropriate powers or expertise to investigate and remedy the contravention. For this reason, the OAIC recommends that the technical specifications should not be included in the PCEHR rules. The OAIC suggests that technical specifications could be better regulated by the System Operator in a separate document such as in the terms and conditions of participation in the system.

Issues not dealt with in the proposal

Pseudonyms

The OAIC understands that the registration arrangements in Division 1 of Part 3 of the PCEHR Bill will allow a person to register for a PCEHR using a pseudonym, by first obtaining a pseudonymous healthcare identifier from the healthcare identifier service. Clause 109(5) of the PCEHR Bill states the PCEHR rules may specify the requirements for registering a consumer who has been issued a healthcare identifier under a pseudonym, and for that purpose may specify such modifications of PCEHR legislation as are necessary to facilitate

22 PCEHR: Proposals for Regulations and Rules, p 25.
23 PCEHR Bill Explanatory Memorandum, p 22.
such registration. The OAIC supports giving individuals the clear option to transact pseudonymously to protect their privacy, where this is lawful and practicable\textsuperscript{24} and considers that this aspect of the PCEHR system should be included in the rules.