EXPLANATORY STATEMENT

Issued by Authority of the Minister for Health

Personally Controlled Electronic Health Records Act 2012

PCEHR Rules 2012

The *Personally Controlled Electronic Health Records Act 2012* (the Act) establishes the personally controlled electronic health record (PCEHR) system. Section 109 of the Act provides that the Minister may make rules, known as PCEHR Rules, about matters that are required or permitted by the Act to be dealt with in the PCEHR Rules.

The purpose of the PCEHR Rules 2012 is to prescribe requirements for access control mechanisms, identity verification, the handling of specified types of records and participation requirements, including security requirements for healthcare provider organisations. Additional rules will be made in relation to one or more discrete areas where the Act permits rules to be made. For example, separate rules entitled *PCEHR (Participation Agreements) Rules 2012* have been made under subsection 109(4A) of the Act.

The PCEHR Rules 2012 will support the secure operation of the PCEHR system and will specify the requirements that apply to participants in the PCEHR system (that is, registered healthcare provider organisations, registered repository operators, registered portal operators and registered contracted service providers) and the requirements on the System Operator to provide access control mechanisms that will be available to consumers to manage their PCEHR.

Paragraphs 43(b) and 48(a) of the Act provide that healthcare provider organisations, repository operators, portal operators and contracted service providers are not eligible to register to participate in the PCEHR system unless, among other things, they comply with the PCEHR Rules.

Subsection 51(3) of the Act provides that failure to comply with the Act (which is defined in section 5 of the Act to include the PCEHR Rules) may result in a decision by the System Operator to cancel or suspend the registration of a registered healthcare provider organisation, registered repository operator, registered portal operator or registered contracted service provider. Further, section 78 of the Act provides that a person that is, or at any time has been, a registered repository operator or registered portal operator may be subject to a civil penalty of up to 80 penalty units ($8,800) for individuals or 400 penalty units ($44,000) for bodies corporate if they contravene the PCEHR Rules. Other sanctions may also be available against participants in the PCEHR system that do not comply with the PCEHR Rules.

The PCEHR Rules do not relate to the professional activities of healthcare providers. Professional obligations and professional bodies exist for this purpose. The PCEHR Rules only regulate matters necessary to ensure the efficient and secure operations of the PCEHR system.

The PCEHR Rules apply differently to each type of participant, including the System Operator, given the different roles and functions of each participant.

Detail of the PCEHR Rules 2012 is set out in the Attachment.

The PCEHR Rules 2012 commence on the day after registration on the Federal Register of Legislative Instruments.

The PCEHR Rules 2012 are a legislative instrument and are subject to the *Legislative Instruments Act 2003*.

Consultation

The *PCEHR System: Proposals for Regulations and Rules* ('proposals paper') was released for public comment on 21 March 2012. The proposals were subsequently revised to address the submissions made on the proposals paper.

The Minister consulted with state and territory health ministers on 26 April 2012 to provide the opportunity to comment on the revised proposals paper, and the draft PCEHR Rules 2012 were revised to address the feedback provided by health ministers.

Section 109 of the Act requires that, before making PCEHR Rules, the Minister must consult the Jurisdictional Advisory Committee and Independent Advisory Council, although failure to consult these committees does not affect the validity of the PCEHR Rules.

The Independent Advisory Council was consulted on draft PCEHR Rules 2012 on 19 July 2012 and no amendment of the draft PCEHR Rules 2012 was necessary.

In place of the Jurisdictional Advisory Committee, which had not yet been constituted, jurisdictions were consulted on the draft PCEHR Rules 2012 through the National Health Information and Performance Principal Committee, National Health Chief Information Officers Forum and National Health Information Regulatory Framework Working Group. Minor revisions were made to the draft PCEHR Rules 2012 to address jurisdictional feedback.

ATTACHMENT

Details of the *PCEHR Rules 2012*

PART 1—PRELIMINARY

1. Name of rules

Rule 1 provides that the title of the rules is *PCEHR Rules 2012.*

2. Commencement

Rule 2 provides that the PCEHR Rules 2012 commence on the day after they are registered on the Federal Register of Legislative Instruments.

3. Definitions

Rule 3 defines particular terms used in the PCEHR Rules 2012. These terms include:

Access control mechanisms
Under paragraphs 15(b) and (c) of the Act, the System Operator has a function to establish and maintain access control mechanisms, which are subject to any requirements specified in the PCEHR Rules. Access control mechanisms will enable a consumer to manage which healthcare provider organisations and nominated representatives will be able to access the consumer's PCEHR and records within the consumer's PCEHR.

Access control mechanisms will provide:

- ***default access controls*** – the settings that will apply if a consumer does not set controls on the registered healthcare provider organisations or nominated representatives who may access the consumer's PCEHR. In summary, default access controls will enable registered healthcare provider organisations involved in the care of a consumer to access the consumer's PCEHR; and
- ***advanced access controls*** – the settings that will allow a consumer to specify which registered healthcare provider organisations and nominated representatives may access their PCEHR and to what degree.

Document code
Document codes will form part of the advanced access controls available to consumers. A consumer who has chosen to set advanced access controls on their PCEHR may choose to set up a document code (effectively a PIN or password) with which they can control access by registered healthcare provider organisations to individual records in their PCEHR.

In practice, a registered healthcare provider organisation provided with the document code by a consumer would only need to enter the code once. On entering the document code, the registered healthcare provider organisation would be able to access all records in the consumer's PCEHR which were protected by a document code.

Record code
Record codes will form part of the advanced access controls available to consumers. A consumer who has chosen to set advanced access controls on their PCEHR may choose to set up a record code (effectively a PIN or password) with which they can control access to their PCEHR by registered healthcare provider organisations. Where a record code has been set up, registered healthcare provider organisations would be unable to access the consumer's PCEHR unless the consumer had given them their record code (or the System Operator has done so on behalf of the consumer) or the organisation was on the consumer's access list before the consumer set up a record code.

In practice, a registered healthcare provider organisation provided with the record code by a consumer would only need to enter this record code upon first accessing the consumer's PCEHR. It would not be necessary to re-enter the record code each time the provider accessed the PCEHR. On entering the record code, the registered healthcare provider organisation would be added to the consumer's ***access list*** which is a list maintained by the System Operator identifying those organisations which are permitted to access the consumer's PCEHR. The consumer can subsequently change the access level of the organisation if they wish.

Effectively remove
This term refers to the manner in which a consumer may remove a record from their PCEHR. Effectively removing a record will mean it will not be accessible through the consumer's PCEHR to the consumer, their nominated representatives or treating healthcare provider organisations, even in circumstances where there is a serious threat to an individual's life, health or safety or to public health or safety. While an effectively removed record will no longer be accessible through the consumer's PCEHR, it may still be accessible via the System Operator for medico-legal reasons or other reasons authorised or required by law. A consumer may subsequently choose to ***restore*** a record that has been effectively removed from their PCEHR by contacting the System Operator.

Network hierarchy
This term refers to the network of healthcare provider organisations that may be established in accordance with subsections 9A(3) to (7) of the *Healthcare Identifiers Act 2010* (HI Act). A network hierarchy is made up a of ***seed organisation***, which is the head healthcare provider organisation of a network hierarchy, and may include one or more ***network organisations***.

The note to rule 3 assists readers by making clear that other terms used in the PCEHR Rules 2012 are as defined in the Act.

In reading the PCEHR Rules 2012 it is important to recognise that, if a consumer has an authorised representative, the Act enables an authorised representative to do anything authorised or required of the consumer in relation to the PCEHR system and the things done by an authorised representative are deemed to be things done by the consumer (see subsection 6(7), and the definition of "this Act" in section 5, of the Act).

PART 2—ACCESS CONTROL MECHANISMS

Paragraphs 15(b) and (c) of the Act specify that a function of the System Operator is to establish and maintain access control mechanisms for the purposes of the PCEHR system. Divisions 1 to 5 of Part 2 of the PCEHR Rules 2012 set out requirements for the access control mechanisms that must be established and maintained by the System Operator.

DIVISION 1—DEFAULT ACCESS CONTROLS

Default access controls are the access controls which apply unless a consumer has set advanced access controls for their PCEHR. The Act provides that it is a function of the System Operator to specify default access controls (see paragraph 15(b) of the Act) and Division 1 sets out the default access controls.

4. Default access controls

Rule 4 provides that the default access controls must:

- allow any registered healthcare provider organisation that is involved in the care of a registered consumer to access the consumer's PCEHR (paragraph 4(a));
- include an access list which identifies those registered healthcare provider organisations that are permitted to access the consumer's PCEHR (paragraph 4(b)). Upon gaining access to a consumer's PCEHR, a registered healthcare provider organisation will be automatically added to the access list;
- allow a registered consumer to view her or his access list and see which registered healthcare provider organisations are permitted to access the registered consumer's PCEHR (paragraph 4(c));
- automatically remove a healthcare provider organisation from the consumer's access list if the organisation has not accessed the consumer's PCEHR for three years (paragraph 4(d));
- allow a registered consumer to effectively remove a record from his or her PCEHR and to subsequently authorise the System Operator to restore that record (paragraph 4(e)), should the consumer so wish; and
- allow a registered healthcare provider organisation that uploaded a record to a consumer's PCEHR to access that record. If the organisation is no longer on the access list for the consumer's PCEHR, the organisation must make a request to the System Operator in order to gain access to the record.

The note to rule 4 makes clear that, where a healthcare provider organisation is added to or omitted from the access list for a consumer's PCEHR, access flags set within the healthcare provider organisation's network hierarchy affect which additional registered healthcare provider organisations (if any) are also added to, or omitted from, the access list for a consumer's PCEHR. See Division 4 of Part 2 for more information about access flags.

DIVISION 2—ADVANCED ACCESS CONTROLS

If a consumer registers for a PCEHR, she or he can choose to set up and use advanced access controls as set out in Division 2. If advanced access controls are not set, the default access controls will apply in relation to the consumer's PCEHR (see Division 1 of Part 2).

5. Advanced access controls

Rule 5 provides that the advanced access control mechanisms to be established and maintained by the System Operator must have the same functionality as the default access controls and must:

- allow a consumer to use a record code to control access to their PCEHR (paragraph 5(1)(a)). If a consumer sets up a record code, it will ensure that registered healthcare provider organisations can only access the consumer's PCEHR in specified circumstances. In summary, these are where the organisation has been given the record code by the consumer or by the System Operator at the request of the consumer. Registered healthcare provider organisations will be able to continue to access the consumer's PCEHR where they are already on the access list for the consumer's PCEHR prior to the consumer setting up a record code. If a consumer forgets their record code, they will need to have the System Operator reset it. It is envisaged that a consumer will be able to do this by phoning the PCEHR call centre, going to a Medicare shopfront or online using the consumer portal;
- allow a consumer to prevent registered healthcare provider organisations' clinical information systems automatically checking and indicating if the consumer has a PCEHR (paragraph 5(1)(b)). However, even if a consumer has chosen to set this advanced access control, a healthcare provider will still be able to manually search the PCEHR system to check if the consumer has a PCEHR using the provider's clinical information system; and
- allow a consumer to control access to individual records within their PCEHR (paragraph 5(1)(c)).

Subrule 5(2) specifies the ways in which consumers may restrict access to individual records within their PCEHR, and the features and limitations of this aspect of advanced access controls.

In summary, a registered consumer may either set up a document code (effectively a PIN or password), or may adjust the settings in her or his PCEHR, to prevent access to particular records by particular registered healthcare provider organisations.

There are some types of records in relation to which consumers cannot restrict access, being shared health summaries, consumer-entered health summaries and information about advanced care directives (paragraph 5(2)(a)).

Paragraph 5(2)(b) specifies circumstances where a record to which access has been restricted will still be accessible, including for nominated representatives and in the case of a serious threat in accordance with rules 6 and 7.

If a registered consumer forgets her or his document code, they will need to have the System operator reset it. It is envisaged that a consumer will be able to do this by

phoning the PCEHR call centre, going to a Medicare shopfront or online using the consumer portal.

Paragraph 5(2)(c) provides that, as a default, records uploaded to a consumer's PCEHR will not have a document code applied to them. The System Operator must ensure that registered consumers may change this default setting if they wish so that all records uploaded by specified registered healthcare provider organisations have a document code applied to them. This will further help consumers protect sensitive records.

Notes 1 to 4 to this rule provide information about how these settings will operate in practice, and note 5 directs readers to rule 28 which prohibits healthcare provider organisations from retaining a consumer's record code or document code for future use to access the consumer PCEHR or a record in the consumer's PCEHR.

DIVISION 3—ACCESS CONTROL MECHANISMS AND SERIOUS THREATS

Section 64 of the Act provides that a participant in the PCEHR system is authorised to collect, use and disclose health information included in a consumer's PCEHR in the case of a serious threat to an individual's life, health or safety, or to public health or safety.

The purpose of Division 3 of Part 2 of the PCEHR Rules 2012 is to ensure that the access control mechanisms established and maintained by the System Operator support access to a consumer's PCEHR in such circumstances.

6. Serious threat to an individual's life, health or safety

Subrule 6(1) requires that access control mechanisms established and maintained by the System Operator enable a registered healthcare provider organisation to assert that it reasonably believes that collection, use or disclosure of information in a consumer's PCEHR is necessary to lessen or prevent a serious threat to an individual's life, health or safety, and that it is unreasonable or impracticable to obtain the consumer's consent to the collection, use or disclosure.

Subrule 6(2) provides that, where access is authorised under subsection 64(1) of the Act, the access control mechanisms must allow access regardless of the access controls set by the consumer, and must not allow access to any record that has been effectively removed from the consumer's PCEHR.

Access to a PCEHR under these circumstances will automatically lapse five days after the organisation asserted that the circumstances existed (paragraph 64(1)(c) of the Act). The organisation may re-assert that the circumstances in paragraph 64(1)(a) of the Act exist after this period has lapsed.

Note 1 to this rule refers readers to subsection 64(3) of the Act which provides that consumer-only notes are not available in the case of a serious threat.

Note 2 makes clear that, where a healthcare provider organisation is added to or omitted from the access list for a registered consumer's PCEHR, access flags set within the healthcare provider organisation's network hierarchy affect which

additional registered healthcare provider organisations (if any) are also added to, or omitted from, the access list for the consumer's PCEHR.

Note 3 explains that registered healthcare provider organisations may still access a consumer's PCEHR under paragraph 54(a) of the Act if the consumer's registration has been suspended.

7. Serious threat to public health or public safety

Subrule 7(1) requires that access control mechanisms established and maintained by the System Operator enable a registered healthcare provider organisation to assert that it reasonably believes that collection, use or disclosure of information in a consumer's PCEHR is necessary to lessen or prevent a serious threat to public health or public safety.

Subrule 7(2) provides that, where access is authorised under subsection 64(2) of the Act, the access control mechanisms must allow access regardless of the access controls set by the consumer, and must not allow access to any record that has been effectively removed from the consumer's PCEHR.

Note 1 to this rule refers readers to subsection 64(3) of the Act which provides that consumer-only notes are not available in the case of a serious threat.

Note 2 makes clear that, where a healthcare provider organisation is added to or omitted from the access list for a registered consumer's PCEHR, access flags set within the healthcare provider organisation's network hierarchy affect which additional registered healthcare provider organisations (if any) are also added to, or omitted from, the access list for the consumer's PCEHR.

DIVISION 4—ACCESS FLAGS

The purpose of Division 4 is to specify that the access control mechanisms established and maintained by the System Operator must make use of access flags, and to prescribe the requirements for access flags.

Consumers retain control over which registered healthcare provider organisations are able to access their PCEHR – for example, by setting up a record code using advanced access controls and only giving that record code to the registered healthcare provider organisations to which the consumer wishes to grant access. However, access flags are also a key component of the PCEHR system's access control mechanisms. Where a registered healthcare provider organisation is added to, or omitted from, the access list for a registered consumer's PCEHR, access flags determine which additional registered healthcare provider organisations (if any) in the same network hierarchy are also added to, or omitted from, the access list. Similar to how information is currently shared between healthcare provider organisations as part of providing healthcare, access flags are designed to ensure that registered healthcare provider organisations that legitimately need to access a consumer's PCEHR in order to provide healthcare are able to do so.

Access flags are also intended to improve consumer privacy protections. For example, access flags are designed to deal with the situation where multiple

healthcare provider organisations exist within a single legal entity. This could occur, for instance, where there are multiple healthcare provider organisations (such as public hospitals) within a public sector health service that is a single legal entity. In these circumstances, the absence of access flags would result in all public hospitals in the public sector health service being placed on the access list for a consumer's PCEHR, and all would be able to access the consumer's PCEHR, if the consumer permitted just one public hospital to access their PCEHR. Access flags are designed to help prevent this occurring by restricting the extent to which additional registered healthcare provider organisations in the same network hierarchy are able to gain access to a consumer's PCEHR.

Access flags do not act as an authorisation to collect, use or disclose health information under the Act. As outlined above, where a registered healthcare provider organisation is added to, or omitted from, the access list for a registered consumer's PCEHR, access flags merely determine which additional registered healthcare provider organisations (if any) are added to or omitted from the access list. For example, being added to the access list for a consumer's PCEHR would mean that a registered healthcare provider organisation would gain the technical ability to access the consumer's PCEHR (to the extent it did not already have that ability). However, even if a registered healthcare provider organisation is placed on the access list for a consumer's PCEHR as a result of access flag settings, the organisation must not collect, use or disclose health information in the consumer's PCEHR unless authorised under the Act – for example, where the organisation is providing healthcare to the consumer.

Access flags must be assigned within a network hierarchy in a way that balances reasonable consumer expectations about the sharing of information as part of providing healthcare to the consumer and arrangements within healthcare provider organisations for access to health information (rule 9).

It is important to note that healthcare provider organisations set and maintain access flags in the PCEHR system. Healthcare provider organisations are not required to develop or redesign clinical information systems for this purpose. It is also important to note that the adding of registered healthcare providers organisations to, or the omitting of organisations from, the access list for a consumer's PCEHR is managed by the PCEHR system in accordance with the access flags that have been set by healthcare provider organisations. It is not something that local clinical information systems need to manage.

Access flags only relate to accessing information in the PCEHR system. Once information has been downloaded from the PCEHR system, access flags no longer have any effect. This means that access flags will not restrict arrangements for information exchange between organisations in a network hierarchy where information has been downloaded into local clinical information systems. Instead, existing Commonwealth, state or territory privacy and health information laws and professional obligations will apply to the collection, use and disclosure of that downloaded information (section 71 of the Act).

8. Access control mechanisms must include use of access flags

Rule 8 specifies the requirements for access flags as part of the access control mechanisms established and maintained by the System Operator, including the way in which the access flags are to be set and maintained within a network hierarchy by its seed organisation.

Paragraph 8(b) provides that access flags are to be set and maintained for a registered healthcare provider organisation in the context of the organisation's network hierarchy. A network hierarchy is a network of healthcare provider organisations established and maintained in accordance with subsections 9A(3) to (7) of the HI Act. A network hierarchy comprises a seed organisation and may include one or more network organisations. A network hierarchy may consist of healthcare provider organisations that are all part of the same legal entity, or may consist of healthcare provider organisations that are part of two or more separate legal entities. Setting and maintaining access flags within the context of a registered healthcare provider organisation's network hierarchy ensures that the PCEHR system leverages structures already established under the HI Act.

Paragraph 8(c) requires that the responsible officer and/or organisation maintenance officer of the seed organisation within a network hierarchy be responsible for setting and maintaining access flags for the registered healthcare provider organisations within the network hierarchy. Retaining this responsibility at the level of the seed organisation will help ensure that access flags are set consistently within a network hierarchy and that a strategic view consistent with the principles in rule 9 is taken when setting access flags.

An example of how access flags work is set out under the discussion for rule 9.

Paragraph 8(d) provides that access flags must be set and maintained in accordance with the principles in rule 9.

9. Principles for assigning access flags

Rule 9 specifies the principles for assigning access flags and deals with related matters, including procedures for reassigning access flags where they have not been assigned in a manner that is consistent with the principles.

Subrule 9(1) provides that access flags must be set and maintained in a way which balances:

- reasonable consumer expectations about the sharing of information as part of providing healthcare to the consumer; and
- arrangements within the organisation for access to health information collected by the organisation.

Under paragraph 9(1)(a), reasonable consumer expectations would include:

- ensuring that a consumer is able to receive the healthcare that he or she needs while also ensuring that access to his or her PCEHR does not extend beyond the

registered healthcare provider organisations reasonably necessary for this to occur; and

- being able to ascertain quickly and simply which additional registered healthcare provider organisations (if any) would have access to the consumer's PCEHR if a particular registered healthcare provider organisation were to be added to the access list for the consumer's PCEHR.

Paragraph 9(1)(b) is intended to ensure that consumer expectations under sub-paragraph 9(1)(a) are balanced against the arrangements that registered healthcare provider organisations may use to ensure that information is shared appropriately for the safe and efficient treatment of consumers.

Subrule 9(2) provides that seed organisations must regularly review the access flags assigned within the network to ensure that they remain consistent with the principles in subrule 9(1).

Subrule 9(3) provides a mechanism to deal with the situation where access flags have not been assigned within a network hierarchy, have been assigned in a manner that is inconsistent with the principles in subrule 9(1) or have been assigned in a manner that is otherwise inappropriate. If the System Operator reasonably considers that one or more of these kinds of situations exist, paragraph 9(3)(a) requires the System Operator to consult with, and consider the views (if any) of the seed organisation of the network hierarchy. Following consideration under paragraph 9(3)(a), the System Operator may by written notice request the seed organisation to make reasonable changes to the access flags within the organisation's network hierarchy, including by adding, omitting or reassigning access flags. As healthcare provider organisations will usually be in a better position than the System Operator to set and maintain access flags, it is envisaged at this stage that the System Operator would generally only give a notice under paragraph 9(3)(a) if other methods did not result in appropriate access flag settings.

Any notice given by the System Operator under paragraph 9(3)(b) must be consistent with the principles in subrule 9(1).

Subrule 9(5) requires that a registered healthcare provider organisation must not unreasonably refuse to comply with a notice given by the System Operator under paragraph 9(3)(b).

The note under subrule 9(5) explains that rule 23 requires seed organisations to structure their network hierarchies in a way that permits access flags to be assigned in accordance with the principles in rule 9.

Example 1 – how access flags limit which organisations are added to the access list for a consumer's PCEHR

A network hierarchy made up of a seed organisation and nine network organisations is structured as shown in ***Diagram 1*** below. The seed organisation and each network organisation is a healthcare provider organisation, and each is assigned a healthcare identifier under section 9A of the HI Act. In this example, the seed and network organisations are all part of the same legal entity, and all the healthcare provider organisations in the network hierarchy are registered under section 44 of the Act.

Based on the principles in rule 9, the seed organisation has assigned access flags to itself and to network organisations 3 and 4.

If a consumer is treated by a medical practitioner who works for the healthcare provider organisation that is network organisation 1, and as a result that healthcare provider organisation is added to the access list for the consumer's PCEHR, the healthcare provider organisations that are the seed organisation and network organisations 2 and 5 (but no other healthcare provider organisations) would also be added to the access list given rule 8 and the way the access flags have been assigned in this example.

The access flags only limit access to information in the PCEHR system. Once information has been downloaded into a local clinical system, the downloaded information is subject to existing Commonwealth, state or territory privacy and health information laws and professional obligations.

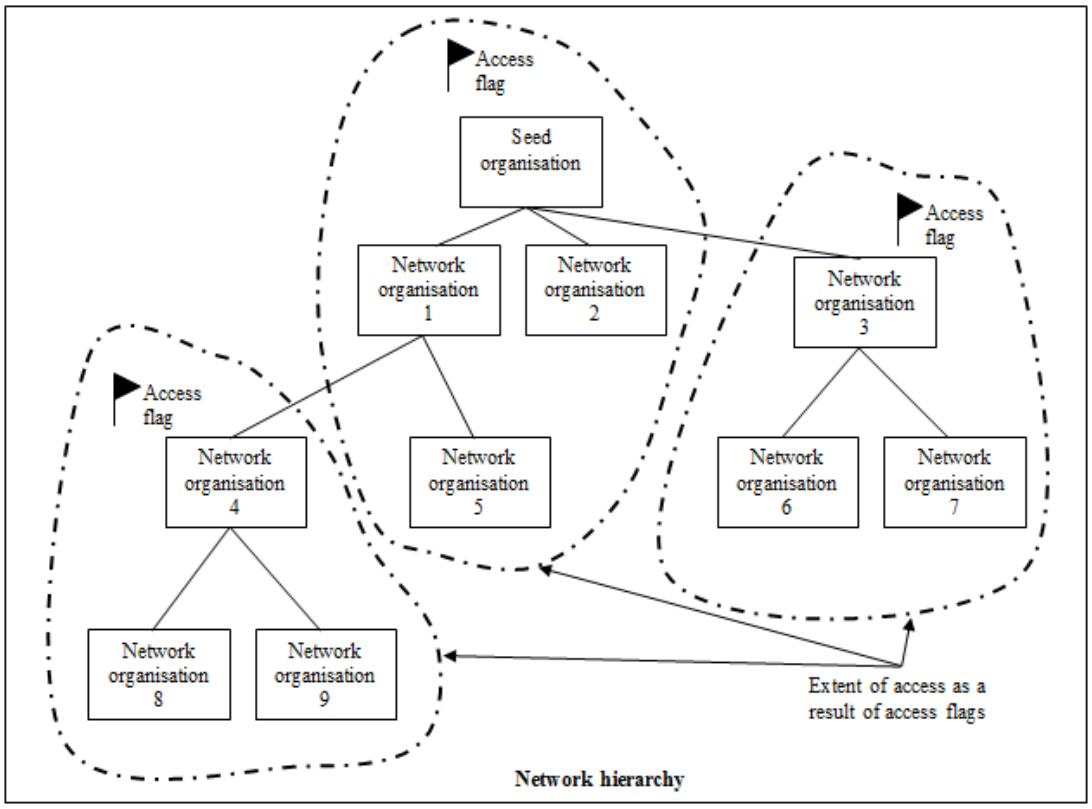

Diagram 1

DIVISION 5—ACCESS CONTROL MECHANISMS RELATING TO SUSPENSION OR CANCELLATION OF ACCESS TO A CONSUMER'S PCEHR

Division 5 sets out the range of circumstances in which the System Operator can suspend or cancel access to a consumer's PCEHR by authorised or nominated representatives. Suspension or cancellation of access to a consumer's PCEHR may be necessary for a range of reasons, including to prevent unauthorised access to a

consumer's PCEHR (where a person is no longer eligible to be a representative) and to protect the security and integrity of the PCEHR system.

Suspension or cancellation of access to a consumer's PCEHR by an authorised representative or a nominated representative does not affect the underlying registration of the consumer under the Act.

10. Automatic cancellation when consumer takes control

Rule 10 deals with circumstances where a consumer takes control of their PCEHR or turns 18 years of age. Under subrule 10(1), the System Operator must cancel access to the consumer's PCEHR for all authorised representatives and nominated representatives upon the earlier of the consumer taking control of her or his PCEHR and the consumer reaching the age of 18.

Subrule 10(3) provides an exception to subrule 10(1) and is intended to deal with situations where a young person turning 18 lacks the capacity to manage her or his PCEHR. Under subrule 10(3), the System Operator must not cancel access for an authorised representative if the System Operator is satisfied that the person who is currently the authorised representative will, when the consumer reaches the age of 18, be an authorised representative under subsection 6(4) of the Act.

Subrule 10(2) provides that a consumer is treated as having taken control of their PCEHR if:

- the System Operator is no longer satisfied that the consumer has an authorised representative under section 6 of the Act;
- the consumer's identity has been verified by the System Operator; and
- if the consumer wishes to access her or his PCEHR online, or adjust their PCEHR's access controls online – the consumer has arranged with the System Operator to have online access to their PCEHR. In summary, this will involve setting up a password and/or other access mechanisms with the System Operator.

The note to this rule refers readers to rule 17 which provides for the verification of a consumer's identity when they cease to have an authorised representative.

11. Suspension on death of consumer

Rule 11 requires the System Operator to suspend access to a consumer's PCEHR for all authorised and nominated representatives of the consumer upon receiving advice from the service operator (that is, the service operator of the Healthcare Identifiers Service under the HI Act) that the status of the consumer's healthcare identifier has been changed to 'deceased'.

The notes to this rule provides information about the healthcare identifier process that occurs when a consumer dies. The status of a consumer's healthcare identifier is changed to 'deceased' when evidence of the consumer's death is provided to the service operator but the formal advice has not yet been provided by the relevant state or territory authority. Once formal advice is provided, the service operator will change the status of the consumer's healthcare identifier to 'retired' and will notify

the System Operator. Upon receipt of notification of 'retired', the System Operator will cancel the registration of the consumer under subsection 51(6) of the Act.

12. Suspension and cancellation where representation ceases

Rule 12 requires the System Operator to cancel or suspend access to the consumer's PCEHR for an authorised representative or a nominated representative in circumstances where the person is no longer representing the consumer.

Paragraph 12(1)(a) provides that the System Operator must cancel access if informed by the service operator that the status of the healthcare identifier of the authorised representative or nominated representative has been changed to 'retired', meaning that formal advice has been received from the service operator that the representative has died.

Nominated representatives who are granted read-only access to a consumer's PCEHR are not required to provide their healthcare identifier to the System Operator. This means that the service operator will be unable to notify the System Operator if such a representative dies. Subparagraph 12(1)(a)(ii) therefore provides that the System Operator must cancel a nominated representative's access when the System Operator is otherwise satisfied that the nominated representative has died.

The System Operator must also cancel a representative's access if the System Operator is no longer satisfied that the person is eligible to be a representative of the consumer under section 6 or 7 of the Act (paragraph 12(1)(b)), or if notified in writing by the person that she or he no longer wishes to represent the consumer for PCEHR purposes (paragraph 12(1)(c)).

While the System Operator investigates whether to cancel access due to the circumstances above, the System Operator may suspend access by the representative (subrule 12(3)).

Subrule 12(2) provides that the System Operator must suspend access to a consumer's PCEHR for an authorised representative or a nominated representative if the System Operator has been informed by the HI Service Operator that the status of the representative's healthcare identifier has been changed to 'deceased', meaning that the System Operator has received evidence that the representative has died but has not yet received formal notice of death from the service operator. Once formal notice of death has been received (that is, the status of the representative's healthcare identifier has been changed to 'retired'), access will be cancelled under subrule 12(1).

If the System Operator suspends or cancels an authorised representative's access to a consumer's PCEHR for any of the circumstances described in rule 12, the System Operator must also suspend or cancel access for all remaining nominated representatives of the consumer (subrule 12(4)).

The notes to this rule direct readers to subsection 7(3) of the Act which provides that not all nominated representatives must have a healthcare identifier. They also make clear that, where a nominated representative's access is cancelled under subrule 12(4), the person's access to the consumer's PCEHR as a nominated representative may subsequently be reinstated by any remaining authorised representative.

13. Suspension while investigating eligibility

Rule 13 allows the System Operator to suspend, cancel or restore the access of authorised representatives in circumstances where a question has been raised about the representative's eligibility to continue as an authorised representative.

The System Operator may be informed of a claim by a person that a person is not eligible to act as an authorised representative of a consumer. Such a claim must be made in the approved form (subrule 13(2)). The System Operator must investigate the claim and determine whether or not the person remains eligible to be an authorised representative within the meaning of section 6 of the Act (subrule 13(3)). Until a decision is made under subrule 13(3), the System Operator must suspend all representatives' access to the consumer's PCEHR (subrule 13(1)) where a claim has been made. Suspending access for representatives would not affect the ability of registered healthcare provider organisations to access the consumer's PCEHR in accordance with the access controls put in place by the consumer's authorised representative(s) immediately prior to the suspension coming into force.

If, after investigating the matter, the System Operator is no longer satisfied that the person is eligible to be the consumer's authorised representative, the System Operator must cancel the person's access to the consumer's PCEHR (paragraph 13(3)(a)). However, if after investigating the matter the System Operator is satisfied that the person remains eligible to be the consumer's authorised representative, the System Operator must restore access for that person (paragraph 13(3)(b)) and all other representatives (subrule 13(1)).

If the System Operator cancels access to a consumer's PCEHR under paragraph 13(3)(a), the System Operator must also cancel access for all of the consumer's nominated representatives (subrule 13(4)).

Note 1 to this rule directs the reader to section 6 of the Act in relation to decisions about whether or not a person is an authorised representative of a consumer, and to section 97 in relation to the review of decisions.

Note 2 makes clear that where a nominated representative's access is cancelled under subrule 13(4), the person's access to the consumer's PCEHR as a nominated representative may subsequently be reinstated by any remaining authorised representative.

14. Temporary suspension where there is a serious threat

Subrule 14(1) requires the System Operator to suspend all representatives' access to a consumer's PCEHR if the System Operator has been notified by the consumer's authorised representative that allowing continued representative access to the consumer's PCEHR poses or is likely to pose a serious risk to a person's life, health or safety and the System Operator is satisfied that suspending access would reduce this risk. The notification for the purposes of subrule 14(1) would not need to be provided in writing – for example, it may occur by telephone.

Under subrule 14(2), the suspension of access will continue until the earlier of:

- 30 days from the date access was suspended under subrule 14(1); and
- the day on which the System Operator is notified in writing by the authorised representative (who originally made the claim of risk) that there is no longer such a risk.

Note 1 to this rule makes clear that if the System Operator suspends an authorised representative's access to a consumer's PCEHR under rule 14, the System Operator still has the ability to suspend the same representative's access under rule 13 if necessary.

Note 2 to this rule makes clear that the System Operator can also cancel or suspend a consumer's registration upon request in accordance with subsection 51(1) of the Act.

15. Effect of suspension or cancellation

Rule 15 makes it clear that suspending or cancelling access for an authorised representative or a nominated representative under Division 5 of Part 2 of the PCEHR Rules 2012 has no effect on a consumer's registration under the Act or on the access controls that were in place for the consumer's PCEHR immediately before any suspension or cancellation of access to the consumer's PCEHR occurred.

PART 3—IDENTITY VERIFICATION

16. Requirement for verified healthcare identifier

Subsection 41(1) of the Act provides that the System Operator must register a consumer if, among other things, the System Operator is satisfied that the identity of the consumer has been appropriately verified having regard to any matters (if any) specified in the PCEHR Rules.

Rule 16 provides that, as a minimum requirement in relation to identity verification, the System Operator must be satisfied that the consumer has a verified individual healthcare identifier.

Rule 3 defines a 'verified healthcare identifier' to mean a healthcare identifier in relation to which the service operator has evidence, to the service operator's satisfaction, of the consumer's identity.

Subrule 16(2) makes clear that the System Operator may also have regard to other matters when satisfying itself that the identity of a consumer has been appropriately verified.

17. Identity verification on ceasing to have an authorised representative

Paragraph 109(7)(b) of the Act provides that PCEHR Rules may specify matters relating to authorised representatives, including requiring a consumer to verify her or his identity when the consumer ceases to have an authorised representative.

Rule 17 requires that, if a consumer ceases to have an authorised representative, the System Operator must require the consumer to verify her or his identity before the consumer is able to take control of their PCEHR.

This rule is necessary, for example, where a parent has registered their child for a PCEHR and the child subsequently reaches the age of 18 and is capable of making her or his own decisions. As part of the registration process, the parent will have provided certain information relating to their identity and the identity of the child. When the child reaches the age of 18, their parent will no longer control access to their PCEHR and it will be necessary for the young person to verify their identity with the System Operator. Rule 17 works in conjunction with subrule 10(2) which specifies when a consumer 'takes control' of her or his PCEHR.

Subrule 17(2) provides that a consumer is not required to verify their identity if they have previously done so. This requirement addresses situations where a consumer may have previously verified their own identity before losing capacity and being represented by an authorised representative but then later regains capacity. For example, a consumer has previously verified her or his identity with the System Operator but then suffers acute mental illness and is incapable of managing her or his PCEHR and needs an authorised representative. If the consumer subsequently ceases to have an authorised representative because they have regained capacity, the consumer would not need to verify his or her identity again with the System Operator.

Subrule 17(3) makes clear that the System Operator may have regard to any relevant matter when satisfying itself that the identity of a consumer has been appropriately verified.

PART 4—DEALING WITH CERTAIN TYPES OF RECORDS

Part 4 contains rules about dealing with certain types of records.

18. Restriction on uploading records other than shared health summaries

The Act provides that only nominated healthcare providers may author a shared health summary for uploading to the PCEHR system (sub-paragraph 45(b)(i)). Sub-paragraph 45(b)(ii) of the Act provides that the PCEHR Rules may specify which records, other than shared health summaries, must be prepared by an individual healthcare provider who has been assigned a healthcare identifier.

The effect of rule 18 is that all records, other than shared health summaries, uploaded by registered healthcare provider organisations to the PCEHR system must be prepared by an individual healthcare provider to whom a healthcare identifier has been assigned under paragraph 9(1)(a) of the HI Act. This will ensure transparency and accountability in relation to records that have been uploaded to a consumer's PCEHR by registered healthcare provider organisations.

The note to this rule makes clear that the Act places other restrictions on the uploading of records.

19. Effective removal of records

Some records uploaded to the PCEHR system may contain defamatory statements or may pose a risk to the security or integrity of the PCEHR system – for example, because the electronic record contains a computer virus.

Rule 19 provides that the System Operator may effectively remove, or may direct a participant in the PCEHR system to effectively remove, a record where the System Operator reasonably considers that the record contains a defamatory statement or affects, or is likely to affect, the security or integrity of the PCEHR system.

Where a participant in the PCEHR system – for example, a registered repository operator or a registered healthcare provider organisation – is given a direction by the System Operator under subrule 19(1), the participant must comply with the direction (subrule 19(2)).

If a record is effectively removed under this rule, the System Operator must notify in writing the entity that uploaded the record and explain the reason for the effective removal. The System Operator must also notify in writing the consumer to whom the PCEHR relates (paragraph 19(3)(a)). The entity that uploaded the record may upload a replacement record, provided that at the time of uploading the replacement record the entity is a participant in the PCEHR system and the replacement addresses the System Operator's concerns in the notice given under paragraph 19(3)(a) (paragraph 19(3)(b)).

Subrule 19(4) makes clear that this rule does not by implication affect the System Operator's functions or powers under the Act to manage the PCEHR system.

20. Transfer and disposal of records

This rule applies to any entity that is, or has previously been, a registered repository operator or registered portal operator.

If the registration of a registered repository operator or registered portal operator is cancelled, rule 20 specifies that the entity must not transfer or dispose of health records held by the entity for PCEHR purposes without the prior written approval of the System Operator.

PART 5—PARTICIPATION REQUIREMENTS

DIVISION 1—GENERAL REQUIREMENTS

Section 43 of the Act sets out the eligibility criteria for healthcare provider organisations to register to participate in the PCEHR system. Among the criteria, paragraph 43(b) requires that the healthcare provider organisation comply with any requirements specified in the PCEHR Rules.

Section 48 of the Act sets out the eligibility criteria for repository operators, portal operators and contracted service providers to register to participate in the PCEHR system. Among the criteria, paragraph 43(a) requires that the repository operator,

portal operator or contracted service provider comply with any requirements specified in the PCEHR Rules.

Registered healthcare provider organisations, registered repository operators, registered portal operators and registered contracted service providers are required under section 76 of the Act to notify the System Operator in writing within 14 days of ceasing to be eligible to be registered.

The System Operator is able to cancel or suspend the registration of an entity if it no longer meets the eligibility criteria for registration (subsection 51(3) of the Act).

Subsection 109(4A) of the Act provides that the PCEHR Rules may require a person to enter into a certain type of agreement in order to become registered, and remain registered, as a registered healthcare provider organisation, registered repository operator, registered portal operator or registered contracted service provider. The *PCEHR (Participation Agreements) Rules 2012* specify that a person must enter into a participation agreement with the System Operator in order to be and remain registered as one of these kinds of participant.

Subsections 109(3) and (4) of the Act provide that the PCEHR Rules may specify requirements relating to a range of matters, including administration and day-to-day operations.

Division 1 of Part 5 of the PCEHR Rules 2012 prescribes requirements, in addition to those in the *PCEHR (Participation Agreements) Rules 2012*, with which healthcare provider organisations must comply in order to be eligible for registration. As further functionality is developed for the PCEHR system, it is intended that similar requirements to those in Part 5 will be included in the PCEHR Rules for entities other than healthcare provider organisations.

21. Authority to act on behalf of healthcare provider organisation

Rule 21 requires that, in order to be eligible to register, a healthcare provider organisation must ensure that certain people are authorised to act on its behalf in its dealings with the System Operator. This is necessary so that the System Operator is able to verify the identity of the people with whom it is dealing. It will be the responsibility of the healthcare provider organisation to ensure that the necessary authorities have been put in place so that the organisation can comply with this rule.

The following people must to be authorised to act on behalf of a healthcare provider organisation in its dealings with the System Operator:

- if the organisation is a seed organisation – the organisation's responsible officer and organisation maintenance officer; and
- if the organisation is a network organisation – the responsible officer and organisation maintenance officer of the seed organisation for the network hierarchy to which the network organisation belongs, and the organisation maintenance officer of the network organisation itself.

22. Requirements for seed organisation, etc to participate

Paragraphs 22(a) and (b) require that, in order for a healthcare provider organisation to be eligible to register under the PCEHR Act, any organisations hierarchically superior to that organisation (including the seed organisation) within the network hierarchy must also be registered. In essence, this means that a network organisation cannot register unless there is an unbroken chain of registered healthcare organisations between it and the seed organisation within its network hierarchy.

Paragraphs 22(c) and (d) ensure that the System Operator is provided with the information necessary to maintain a record of the linkages of organisations within each network hierarchy and of the identified healthcare providers who are authorised by each healthcare provider organisation to access the PCEHR system via the provider portal.

23. Registration of network organisations

Rule 23 requires that, in order for a seed organisation to be eligible to register, it must ensure its network hierarchy is structured in a manner that permits the assignment of access flags in accordance with rules 8 and 9. This rule is intended to prevent healthcare provider organisations structuring themselves in a way that undermines the purpose behind access flags.

The example below rule 23 outlines one instance where a structure would not be consistent with rules 8 and 9 and, in particular, would be inconsistent with the principles in rule 9.

DIVISION 2—SECURITY REQUIREMENTS

Subsections 109(3) and (4) of the Act provide that the PCEHR Rules may specify requirements relating to a range of matters, including administration and day-to-day operations and physical and information security.

Division 2 of Part 5 sets out security requirements with which healthcare provider organisations must comply in order to be, and remain, registered.

End point security is critical to ensuring that the PCEHR system remains secure and that consumer's health information is adequately protected. The purpose of Division 2 of Part 5 of the PCEHR Rules 2012 is to ensure that healthcare provider organisations participating in the PCEHR system meet specified minimum standards in terms of the security measures they take in relation to their staff and their information technology systems. Failure to comply with these requirements may compromise the integrity or security of the PCEHR system, and may result in suspension or cancellation of a healthcare provider organisation's registration or the imposition of other sanctions under the Act.

24. Requirements for registration

Rule 24 specifies that, in order for a healthcare provider organisation to be eligible to be registered, and to remain registered, it must comply with the requirements in Division 2 of Part 5 of the PCEHR Rules 2012.

25. Healthcare provider organisation policies

Subrule 25(1) requires that, in order to be eligible to register, healthcare provider organisations must have in place a written policy that reasonably addresses the matters specified in subrule 25(4). In summary, those matters are:

- the manner of authorising persons within the organisation to access the PCEHR system, including the manner of suspending and deactivating the user account of any authorised person (paragraph 25(4)(a));
- the training that will be provided to persons before they are authorised to access the PCEHR system, including in relation to how to use the system accurately and responsibly, the legal obligations on healthcare provider organisations and individuals using the PCEHR system and the consequences of breaching those obligations (paragraph 25(4)(b));
- the process for identifying a person who requests access to a consumer's PCEHR and providing identification information to the System Operator, ensuring the organisation is able to satisfy its obligations under section 74 of the Act (paragraph 25(4)(c));
- the physical and information security measures of the healthcare provider organisation, including the procedures for user account management required under rule 27 (paragraph 25(4)(d)); and
- mitigation strategies to ensure PCEHR-related security risks can be identified, acted upon and reported expeditiously (paragraph 25(4)(e)).

If the healthcare provider organisation reasonably considers that it is not necessary for its policy to address certain matters otherwise required by subrule 25(4), on the basis of the organisation's limited size, the organisation's policy need not address those matters (subrule 25(5)). Subrule 25(5) is intended to exempt sole practitioners and very small healthcare provider organisations from having to address all the matters required by subrule 25(4) in their policy required under subrule 25(1) – for example, because there are no other staff that need training.
Subrule 25(6) contains a number of administrative and procedural requirements in relation to policies required under subrule 25(1), including in summary that policies are:

- written in a manner that enables the organisation's performance to be audited against the policy (sub-paragraph 25(6)(a)(i));
- kept current (sub-paragraph 25(6)(a)(ii));
- uniquely identifiable by version (paragraph 26(6)(b)) and each version of an organisation's policy must be retained in accordance with any applicable record keeping obligations (paragraph 25(6)(d)); and
- reviewed no less than once a year for the identification of new risks, and that the review include consideration of anything that may result in unauthorised access, misuse or unauthorised disclosure of information or accidental disclosure of information, and of any changes to the PCEHR system or relevant laws since the last review (paragraph 25(6)(c)).

Subrule 25(2) provides that healthcare provider organisations must ensure their policy is communicated, and remains accessible, to all its employees and any healthcare providers to whom the organisation supplies services under contract. Healthcare provider organisations must enforce their policy (subrule 25(3)).

26. Policy to be provided to the System Operator on request

Rule 26 requires that, if the System Operator requests in writing that a healthcare provider organisation provide a copy of its policy made in accordance with rule 25 to the System Operator, the organisation must comply within seven days.

The request by the System Operator may relate to the organisation's current policy or one in force on a specified date.

27. User account management within healthcare provider organisations

Rule 27 requires that the information technology systems of healthcare provider organisations, used for the purpose of accessing the PCEHR system, employ reasonable information security access management practices, including in summary:

- ensuring that only those people who require access as part of their duties are authorised to access the system (paragraph 27(a));
- uniquely identifying individuals using the healthcare provider's information technology systems and protecting that unique identity using a password or equivalent protection measure (paragraph 27(b));
- following robust and secure password and/or access management practices (paragraph 27(c));
- ensuring user accounts for persons no longer authorised to access the PCEHR system prevent access (paragraph 27(d)); and
- suspending a user account which allows access to the PCEHR system as soon as practicable after becoming aware that the account or its password or access mechanism has been compromised (paragraph 27(e)).

28. Retention of record codes and document codes

Rule 28 requires healthcare provider organisations to ensure that people using their information technology systems to access the PCEHR system via or on behalf of the organisation do not keep any record of a consumer's record code or document code for future use to access the consumer's PCEHR or records in the consumer's PCEHR.

This ensures that a consumer's ability to control access to her or his PCEHR is not undermined by healthcare provider organisations retaining these codes or sharing them with other organisations.

The note explains that, in practice, when a healthcare provider organisation is given a record code or document code in order to access the consumer's PCEHR or a record in the PCEHR consumer's, the organisation will only need to enter this code once. The PCEHR system will then record that the organisation has been added to consumer's access list, or has access to records to which access would otherwise be restricted. The healthcare provider organisation will retain access to the consumer's

PCEHR or to the relevant record in the consumer's PCEHR until the access control mechanisms for the PCEHR or record are changed, e.g. by the consumer setting up a new record code.

DIVISION 3—RESPONDING TO INFORMATION SECURITY THREATS

Subsection 51 (3) of the Act provides that the System Operator may suspend or cancel the registration of an entity if satisfied that it is appropriate with regard to the security or integrity of the PCEHR system.

Subsections 109(3) and (4) of the Act provide that the PCEHR Rules may specify requirements relating to a range of matters, physical and information security.

The rules in Division 4 of Part 5 of the PCEHR Rules 2012 do not affect the registration of an entity under the Act. Rather, they provide a mechanism for temporarily preventing a registered participant in the PCEHR system from accessing the PCEHR system where that participant's information technology system poses a technological threat.

29. Access to the PCEHR system may be suspended

Subrule 29(1) provides that, if the System Operator is satisfied that the information technology system used by a participant to access the PCEHR system has compromised, or may compromise, the security of integrity of the PCEHR system, the System Operator may suspend the participant's access to the PCEHR system with immediate effect.

Subrule 29(2) makes clear that the information technology system of a participant in the PCEHR system includes the digital credentials which enable authentication of the participant's identity in electronic transmissions.

If the System Operator decides to suspend the participant's access, the System Operator must notify the participant (in writing) of the reasons for that decision and what the participant needs to do in order to regain access to the PCEHR system (subrules 29(3) and (4)). The issuing of a notice under subrule 29(3) would not affect the System Operator's ability to otherwise suspend or cancel the participant's registration under the Act if warranted.

Once the System Operator is satisfied that the information technology systems (including credentials) used by the participant no longer pose a threat to the PCEHR system, the System Operator must restore the participant's access to the PCEHR system (subrule 29(5)).

30. Effect of suspension of access

Rule 30 makes clear that any suspension of the participant's access to the PCEHR system under rule 29 does not affect the participant's registration to participate in the PCEHR system. That is, if a participant's access to the PCEHR system is suspended, the participant remains registered and subject to obligations and requirements under the Act.

STATEMENT OF COMPATIBILITY FOR A BILL OR LEGISLATIVE INSTRUMENT THAT RAISES HUMAN RIGHTS ISSUES

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

PCEHR Rules 2012

This Legislative Instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Legislative Instrument

The Legislative Instrument will provide detail necessary to support the operation of the personally controlled electronic health record (PCEHR) system, as established by the *Personally Controlled Electronic Health Records Act 2012* (the Act).

The Legislative Instrument will, in summary:

- prescribe the access control mechanisms that must be established and maintained by the PCEHR System Operator, enabling consumers who choose to have a PCEHR to be able to control access to their PCEHR and to records within their PCEHR;
- specify the matters to which the System Operator must have regard in determining whether a consumer's identity has been appropriately verified;
- restrict the uploading of records to a consumer's PCEHR to healthcare providers who have been assigned a healthcare identifier;
- require that healthcare provider organisations applying to register develop, maintain, enforce and communicate to their staff policies and procedures, including in relation to the security of local systems that can be used to access the PCEHR system; and
- specify details associated with the suspension of access by representatives to a consumer's PCEHR.

Human rights implications

The Legislative Instrument engages the following human rights:

Right to protection of privacy and reputation

Article 17 of the International Covenant on Civil and Political Rights guarantees protection from unlawful interference with a person's privacy and from unlawful attacks on a person's honour and reputation.

The Legislative Instrument is designed to ensure that the PCEHR system is secure and that the privacy of consumers and others involved in the system is protected. The Instrument does this by, amongst other things, specifying requirements for access control mechanisms to enable consumers to control access to their PCEHRs and to records within their PCEHR. The Instrument also includes requirements for access flags which are designed to limit access to consumers' PCEHR, outlines situations where access to a consumer's PCEHR is to be suspended or cancelled, specifies situations where a person's identity must be verified and includes participation requirements to ensure that healthcare provider organisations and other

entities meet specified minimum standards, including in relation to information security, if they wish to participate in the PCEHR system.

Conclusion

The Legislative Instrument is compatible with human rights because it advances the protection of human rights.

Minister for Health, the Hon Tanya Plibersek MP