PCEHR Rules 2012

Personally Controlled Electronic Health Records Act 2012

I, TANYA PLIBERSEK, Minister for Health, make these Rules under section 109 of the *Personally Controlled Electronic Health Records Act 2012*.

Dated 16th August 2012

TANYA PLIBERSEK
Minister for Health

Contents

Part 1 Preliminary

1. Name of Rules

These Rules are the *PCEHR Rules 2012*.

2. Commencement

The PCEHR Rules commence on the day after they are registered on the Federal Register of Legislative Instruments.

3. Definitions

In these Rules, unless the contrary intention appears:

Access control mechanisms include default access controls and advanced access controls.

Access flag means an information technology mechanism made available by the System Operator to define access to a consumer's PCEHR.

Access list means the record associated with a consumer's PCEHR that specifies the registered healthcare provider organisations permitted to access a consumer's PCEHR.

Act means the *Personally Controlled Electronic Health Records Act 2012*.

Advanced access controls means the access controls that enable a registered consumer to set controls on the registered healthcare provider organisations and nominated representatives who may access the consumer's PCEHR, and the records within the PCEHR.

Consumer-entered health summary means the summary of information, including medications and allergies, that a registered consumer may enter into his or her PCEHR and which is available to anyone with access to the consumer's PCEHR.

Default access controls means the access controls that apply where a registered consumer has not set controls on the registered healthcare provider organisations or nominated representatives who may access the consumer's PCEHR.

Document code means a code which may be used to restrict access to individual records within a consumer's PCEHR in accordance with paragraph 5(1)(c).

Effectively remove, in relation to a record in a consumer's PCEHR, means rendering the record inaccessible to the consumer, their nominated representatives and any registered healthcare provider organisations involved in the care of the consumer, including in the case of a serious threat in accordance with rules 6 and 7.

Healthcare identifier has the same meaning as in section 9 of the *Healthcare Identifiers Act 2010*.

Identified healthcare provider has the same meaning as in the *Healthcare Identifiers Act 2010*.

Network hierarchy means a network of healthcare provider organisations created and managed in accordance with subsections 9A(3) to (7) of the *Healthcare Identifiers Act 2010*.

Network organisation has the same meaning as in the *Healthcare Identifiers Act 2010*.

Organisation maintenance officer has the same meaning as in the *Healthcare Identifiers Act 2010*.

Provider portal means the portal provided by the System Operator that permits registered healthcare provider organisations to access the PCEHR system without having to use a clinical information system.

Record code means a code which may be used to restrict access to a consumer's PCEHR in accordance with paragraph 5(1)(a).

Responsible officer has the same meaning as in the *Healthcare Identifiers Act 2010*.

Restore, in relation to a record, means making a record, which has previously been effectively removed, accessible to the consumer, their nominated representatives and any registered healthcare provider organisations involved in the care of the consumer in accordance with any applicable access control mechanisms, including in the case of a serious threat to an individual's life, health or safety.

Seed organisation has the same meaning as in the *Healthcare Identifiers Act 2010*.

Service operator has same meaning as in the *Healthcare Identifiers Act 2010*.

Taking control, in relation to a PCEHR, has the meaning given by subrule 10(2).

Verified healthcare identifier means a healthcare identifier assigned to a consumer in relation to which the service operator has evidence, to the service operator's satisfaction, of the consumer's identity.

Note 1: Unless the contrary intention appears, terms used in these PCEHR Rules have the same meaning as in the Act— see section 13 of the *Legislative Instruments Act 2003*. These terms include:
approved form, ***authorised representative***, ***consumer***, ***consumer-only notes***, ***employee***, ***nominated representative***, ***PCEHR***, ***PCEHR system***, ***registered consumer***, ***registered healthcare provider organisation***, ***shared health summary*** and ***System Operator***.

Part 2 Access control mechanisms

Division 1 Default access controls

4. Default access controls

For the purposes of paragraph 15(b) and (c) and subsection 109(6) of the Act, the System Operator must establish and maintain default access controls that:

(a) permit all registered healthcare provider organisations involved in the care of a registered consumer to access the consumer's PCEHR;

(b) include an access list of the registered healthcare provider organisations that are permitted to access the consumer's PCEHR because the organisation is involved in the care of the registered consumer;

(c) permit registered consumers to view the access list for their PCEHR;

(d) remove a healthcare provider organisation from the access list for a consumer's PCEHR if the organisation has not accessed the consumer's PCEHR for a period of three years;

(e) permit registered consumers to:

(i) effectively remove records from their PCEHR; and

(ii) authorise the System Operator to restore records which have previously been effectively removed; and

(f) permit registered healthcare provider organisations that uploaded records to a consumer's PCEHR to access those records, but only by request to the System Operator, if the healthcare provider organisation is no longer on the access list for the consumer's PCEHR.

Note: The extent of access by registered healthcare provider organisations under paragraph (a), and the extent to which they will be omitted from the access list under paragraph (d), depends on how access flags have been assigned within the healthcare provider organisation's network hierarchy— see rules 8 and 9.

Division 2 Advanced access controls

5. Advanced access controls

(1) For the purposes of paragraphs 15(b) and (c) and subsection 109(6) of the Act, the System Operator must establish and maintain advanced access controls that have the same functionality as default access controls and that:

(a) subject to rules 6 and 7, permit use of a record code to prevent registered healthcare provider organisations involved in the care of a registered consumer from accessing the consumer's PCEHR unless:

(i) the record code is given to the organisation by:

(A) the consumer; or

(B) the System Operator at the request of the consumer; or

(ii) the organisation is already on the access list for the consumer's PCEHR;

(b) if a registered consumer wishes, prevent registered healthcare provider organisations' clinical information systems automatically checking and displaying whether the consumer has a PCEHR; and

(c) permit registered consumers to control access to individual records in their PCEHR:

(i) by adjusting the advanced access controls for their PCEHR to only permit specified registered healthcare provider organisations on the access list for the consumer's PCEHR to access specified records; or

(ii) using a document code,

in accordance with subrule (2).

(2) For the purposes of paragraph (1)(c), the System Operator must ensure that:

(a) registered consumers are able to prevent access to a record in their PCEHR, other than shared health summaries, consumer-entered health summaries and information about advance care directives, unless:

(i) the registered healthcare provider organisation has been given a document code in relation to the record by:

(A) the consumer; or

(B) the System Operator at the request of the consumer; or

(ii) the consumer has set the advanced access controls for their PCEHR to permit the registered healthcare provider organisation, which is on the access list for the consumer's PCEHR, to access the record;

(b) where a consumer has restricted access to a record using the access controls in paragraph (1)(c):

(i) the record will still be accessible to the registered healthcare provider organisation that uploaded the record to the PCEHR system, without the need to use the consumer's document code;

(ii) the record may still be accessed by registered healthcare provider organisations and other participants in the PCEHR system in the case of a serious threat in accordance with rules 6 and 7;

(iii) consumers are able to choose whether their nominated representatives who do not have the ability to set and maintain access controls are able to access records to which a document code has been applied;

(iv) registered healthcare provider organisations involved in the care of the consumer are not able to determine that records to which access has been restricted using the access controls in

paragraph 1(c) exist solely by viewing the consumer's PCEHR unless:

(A) the organisation has been given a document code in accordance with paragraph (2)(a)(i);

(B) the consumer has set access controls in accordance with paragraph (2)(a)(ii) permitting the organisation to access the relevant record; or

(C) the organisation uploaded the relevant record to the PCEHR system; and

(c) all records uploaded to the consumer's PCEHR are, as a default, uploaded without a document code applied to the record. Where a registered healthcare provider organisation is on the access list for a consumer's PCEHR, the System Operator must ensure that a registered consumer is able to choose whether a record uploaded by that healthcare provider organisation is uploaded with or without a document code applied to the record.

Note 1: The extent of access by registered healthcare provider organisations under paragraph (1)(a) depends on how access flags have been assigned within the healthcare provider organisation's network hierarchy— see rules 8 and 9. Once a record code has been given to a registered healthcare provider organisation, the consumer will not subsequently need to give their record code to the same organisation provided that the organisation remains on the access list for the consumer's PCEHR. Where a registered healthcare provider organisation is given a consumer's record code, and is added to the access list for the consumer's PCEHR, the other healthcare provider organisations (if any) on the access list for the consumer's PCEHR are unaffected.

Note 2: The access control specified in paragraph (1)(b) will not prevent a registered healthcare provider organisation determining if a consumer has a PCEHR if the organisation carries out a manual search of the PCEHR system. However, it will prevent the organisation's clinical information system from automatically checking and displaying whether a consumer has a PCEHR.

Note 3: If a consumer has set up a record code, that code will prevent a registered healthcare provider organisation, which is not on the access list for the consumer's PCEHR, accessing the consumer's PCEHR unless the consumer, or the System Operator at the consumer's request, gives the organisation the record code. Record codes and document codes will not prevent access to a PCEHR or a record in a PCEHR where access is permitted in the case of a serious threat under section 64 of the Act.

Note 4: While records uploaded to a consumer's PCEHR will, as a default, be uploaded without a document code applied to the record, consumers will be able to subsequently restrict access to the record by applying a document code if they wish. Consumers are able to change the default setting in relation to healthcare provider organisations on the access list for the consumer's PCEHR.

Note 5: Rule 28 provides that healthcare provider organisations must not retain a consumer's record code or document code for future use to access the consumer's PCEHR or a record in the consumer's PCEHR.

Division 3 Access control mechanisms and serious threats

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

(1) The access control mechanisms established and maintained by the System Operator must permit registered healthcare provider organisations to assert to the System Operator that the circumstances in paragraph 64(1)(a) of the Act exist.

(2) Where access is authorised under subsection 64(1) of the Act, the access control mechanisms:

(a) must allow access to a consumer's PCEHR regardless of whether a consumer has set up a record code;

(b) must allow access to all records in a consumer's PCEHR regardless of whether a consumer has set up a document code; and

(c) must not permit access to records that have been effectively removed.

Note 1: Consumer-only notes are not available under subsection 64(1) of the Act— see subsection 64(3) of the Act.

Note 2: The extent of access by registered healthcare provider organisations under subsection 64(1) of the Act depends on how access flags have been assigned within the healthcare provider organisation's network hierarchy— see rules 8 and 9.

Note 3: Where a consumer's PCEHR registration has been suspended, paragraph 54(a) of the Act permits access to the consumer's PCEHR in the case of a serious threat under subsection 64(1) of the Act.

7. Serious threat to public health or public safety

(1) The access control mechanisms established and maintained by the System Operator must permit registered healthcare provider organisations to assert to the System Operator that the collection, use or disclose of health information is necessary to lessen or prevent a serious threat to public health or public safety for the purposes of subsection 64(2) of the Act.

(2) Where access is authorised under subsection 64(2) of the Act, the access control mechanisms:

(a) must allow access to a consumer's PCEHR regardless of whether a consumer has set up a record code;

(b) must allow access to all records in a consumer's PCEHR regardless of whether a consumer has set up a document code; and

(c) must not permit access to records that have been effectively removed.

Note 1: Consumer-only notes are not available under subsection 64(2) of the Act— see subsection 64(3) of the Act.

Note 2: The extent of access by registered healthcare provider organisations under subsection 64(2) of the Act depends on how access flags have been assigned within the healthcare provider organisation's network hierarchy— see rules 8 and 9.

Division 4 Access flags

8. Access control mechanisms must include use of access flags

For the purposes of paragraphs 15(b) and (c) and subsection 109(6) of the Act, the System Operator must establish and maintain access control mechanisms that comply with the following requirements:

(a) access flags must be used to determine which additional registered healthcare provider organisations (if any) are to be:

(i) added to the access list for a consumer's PCEHR where a registered healthcare provider organisation accesses the consumer's PCEHR in accordance with default access controls, advanced access controls or in the case of a serious threat to an individual's life, health or safety; and

(ii) omitted from the access list for a consumer's PCEHR where a healthcare provider organisation ceases to be on the access list;

(b) access flags must be set and maintained for a registered healthcare provider organisation in the context of the organisation's network hierarchy;

(c) the responsible officer and/or the organisation maintenance officer of a registered healthcare provider organisation that is the seed organisation within a network hierarchy must be responsible for setting and maintaining the access flags for the registered healthcare provider organisations within the seed organisation's network hierarchy; and

Principles for setting and maintaining access flags

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

Note: A network hierarchy consists of a seed organisation and may include one or more network organisations— see subsections 9A(3) to (7) of the *Healthcare Identifiers Act 2010*. There are only two classes of healthcare provider organisations— that is, seed organisations and network organisations. A network organisation may, but is not required to, be part of the same legal entity as its seed organisation or be a related body corporate of its seed organisation. There can be one or more healthcare provider organisations within a single legal entity.

9. Principles for assigning access flags

(1) Subject to subrules (3) to (5), access flags must be set and maintained for registered healthcare provider organisations in a network hierarchy in a manner which balances:

(a) reasonable consumer expectations about the sharing of health information as part of providing healthcare to the consumer; and

(b) arrangements within the organisation for access to health information collected by the organisation.

(2) A registered healthcare provider organisation that is a seed organisation must ensure that access flags assigned within its network hierarchy are regularly reviewed and adjusted as necessary so that their assignment remains consistent with the principles in subrule (1).

(3) If the System Operator reasonably considers that access flags have not been assigned within a network hierarchy, have been assigned in a manner that is inconsistent with the principles in subrule (1) or have been assigned in a manner that is otherwise inappropriate, the System Operator:

(a) must consult with, and consider the views (if any) of, the seed organisation of the network hierarchy; and

(b) following consideration under paragraph (3)(a), 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.

(4) A notice from the System Operator under paragraph (3)(b) must be consistent with the principles in subrule (1).

(5) A registered healthcare provider organisation must not unreasonably refuse to comply with a request from the System Operator under paragraph (3)(b).

Note: Rule 23 requires seed organisations to structure their network hierarchies in a manner that allows access flags to be assigned in accordance with the principles in this rule.

Division 5 Access control mechanisms relating to suspension or cancellation of access to a consumer's PCEHR

10. Automatic cancellation when consumer takes control

(1) The System Operator must automatically cancel access to a consumer's PCEHR for all the consumer's authorised representatives and nominated representatives upon the earlier of the following:

(a) the consumer taking control of his or her PCEHR;

(b) the consumer reaching the age of 18.

(2) A consumer takes control of his or her PCEHR if:

(a) the System Operator is no longer satisfied that the consumer has an authorised representative under section 6 of the Act; and

(b) the consumer has:

(i) verified his or her identity with the System Operator; and

(ii) if the consumer wishes to access his or her PCEHR online or adjust their PCEHR's access control mechanisms online –

organised his or her own PCEHR log-in details with the System Operator.

(3) Despite paragraph (1)(b), the System Operator must not cancel access to a consumer's PCEHR for a person who is an authorised representative under subsections 6(1) or (2) of the Act if the System Operator is satisfied that the person will, when the consumer reaches the age of 18, be an authorised representative for the consumer under subsection 6(4) of the Act.

Note: Rule 17 requires the System Operator to verify the identity of a consumer where the consumer ceases to have an authorised representative.

11. Suspension on death of consumer

The System Operator must suspend access to a consumer's PCEHR for all the consumer's authorised representatives and nominated representatives if informed by the service operator that the status of the consumer's healthcare identifier has been changed to deceased.

Note 1: Where the status of a consumer's healthcare identifier is deceased, this indicates that evidence of the consumer's death has been received but the service operator has not yet received formal confirmation in the form of fact of death data from the relevant State or Territory authority.

Note 2: Once the service operator informs the System Operator that the consumer's healthcare identifier has been retired (that is, fact of death data has been received), the System Operator must cancel the consumer's registration under subsection 51(6) of the Act. Where a consumer's registration is cancelled, access to the consumer's PCEHR ceases for authorised representatives and nominated representatives.

12. Suspension and cancellation where representation ceases

(1) The System Operator must cancel access to a consumer's PCEHR for a person who is an authorised representative or a nominated representative of the consumer if:

(a) the System Operator:

(i) has been informed by the service operator that the status of the authorised representative's, or nominated representative's (if applicable), healthcare identifier has been changed to retired; or

(ii) is otherwise satisfied that the nominated representative has died;

(b) the System Operator is no longer satisfied under sections 6 or 7 of the Act that the person is an authorised representative or nominated representative of the consumer; or

(c) the person has notified the System Operator in writing that they no longer wish to act as the consumer's authorised representative or nominated representative.

(2) The System Operator must suspend access to a consumer's PCEHR for a person who is an authorised representative or a nominated representative of the consumer if informed by the service operator that the status of the authorised representative's or nominated representative's healthcare identifier has been changed to deceased.

(3) The System Operator may suspend access to a consumer's PCEHR for a consumer's authorised representative or nominated representative while the System Operator investigates whether to take action under subrule (1).

(4) If the System Operator suspends or cancels access to a consumer's PCEHR for an authorised representative under this rule, the System Operator must also suspend or cancel access to the consumer's PCEHR for all nominated representatives.

Note 1: Not all nominated representatives will have a healthcare identifier— see subsection 7(3) of the Act.

Note 2: Where access to a consumer's PCEHR is cancelled for a nominated representative under subrule (4), any remaining authorised representative may agree with a person that that person is to be a nominated representative for the consumer.

13. Suspension while investigating eligibility

(1) Until a decision is made under subrule (3), the System Operator must suspend access to a consumer's PCEHR for all a consumer's authorised representatives and nominated representatives if the System Operator is notified of a claim that an authorised representative is not eligible to be the consumer's authorised representative.

(2) The notice in subrule (1) must be given in the approved form.

(3) If notified of a claim under this rule, the System Operator must investigate the claim and decide to:

(a) cancel access to the consumer's PCEHR for a person if the System Operator is no longer satisfied that the person is eligible to be the consumer's authorised representative; or

(b) restore access to the consumer's PCEHR for a person if the System Operator is satisfied that the person remains eligible to be the consumer's authorised representative.

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

Note 1: A decision about whether a person is or is not the authorised representative of a consumer is made by the System Operator under section 6 of the Act. Paragraph 97(1)(a) of the Act gives a right of review in relation to such decisions.

Note 2: Where access to a consumer's PCEHR is cancelled for a nominated representative under subrule (4), any remaining authorised representative may agree with a person that that person is to be a nominated representative for the consumer.

14. Temporary suspension in the case of a serious risk

(1) The System Operator must suspend access to a consumer's PCEHR for all the consumer's authorised representatives and nominated representatives if:

(a) an authorised representative of the consumer notifies the System Operator that continuing access to the consumer's PCEHR by an

authorised representative or nominated representative poses, or is likely to pose, a serious risk to an individual's life, health or safety; and

(b) the System Operator is satisfied that suspending access would be likely to reduce the risk to the individual's life, health or safety.

(2) The suspension of access under subrule (1) is to continue until the earlier of the following:

(a) 30 days from the date on which access was suspended under subrule (1);

(b) the day on which the System Operator is notified in writing by the authorised representative who lodged the notification in paragraph (1)(a) that there is no longer a risk to the individual's life, health or safety.

Note 1: A decision to suspend access under rule 14 would not prevent a decision being made to suspend access under rule 13 if a claim about an authorised representative's eligibility is notified to the System Operator under subrule 13(1) within the 30 day period. In such circumstances, access could, if necessary, continue to be suspended after the 30 day period specified in subrule 14(2) ends.

Note 2: A decision to suspend access under rule 14 would not prevent a decision being made under subsection 51(1) of the Act to cancel or suspend a consumer's registration on request.

15. Effect of suspension or cancellation

Nothing in this Division affects:

(a) a consumer's registration under the Act; or

(b) the access control mechanisms 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

(1) For the purposes of paragraph 41(1)(c) of the Act, the System Operator must be satisfied that the consumer has a verified healthcare identifier.

(2) Subrule (1) does not limit the matters to which the System Operator may have regard when satisfying itself that the identity of a consumer has been appropriately verified.

17. Identity verification on ceasing to have an authorised representative

(1) For the purposes of paragraph 109(7)(b) of the Act, if a consumer ceases to have an authorised representative the System Operator must require the consumer to verify his or her identity before the consumer is able to take control of their PCEHR.

(2) Subrule (1) does not apply if the consumer has previously verified his or her identity with the System Operator.

(3) In deciding whether a consumer has verified his or her identity under subrule (1), the System Operator may have regard to any relevant matter.

Note: Subrule 10(2) specifies when a consumer takes control of his or her PCEHR.

Part 4 Dealing with certain types of records

18. Restriction on uploading records other than shared health summaries

For the purposes of paragraph 45(b)(ii) of the Act, all records other than shared health summaries are specified.

Note: The Act and the *Personally Controlled Electronic Health Records Regulation 2012* place restrictions on the uploading of records to the PCEHR system.

19. Effective removal of records

(1) The System Operator may effectively remove, or may direct a participant in the PCEHR system to effectively remove, a record in the PCEHR system to the extent that the System Operator reasonably considers that the record:

(a) contains a defamatory statement; or

(b) affects, or is likely to affect, the security or integrity of the PCEHR system.

(2) A participant in the PCEHR system who is given a direction under subrule (1) must comply with the direction.

(3) Where the System Operator effectively removes, or directs a participant in the PCEHR system to effectively remove, a record under subrule (1):

(a) the System Operator must notify in writing:

(i) the consumer from whose PCEHR the record was effectively removed; and

(ii) the entity that uploaded the record,

specifying the reasons for its decision; and

(b) the entity may upload a replacement record provided that:

(i) at the time of uploading the replacement record, the entity is a participant in the PCEHR system; and

(ii) the replacement record addresses the System Operator's concerns specified in the notice.

(4) Nothing in subrule (1) affects by implication the System Operator's functions or powers to manage the PCEHR system.

20. Transfer and disposal of records

(1) This rule applies to an entity that is, or at any time was, a registered repository operator or a registered portal operator.

(2) If the entity's registration under Division 3 of Part 3 of the Act is cancelled, 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

21. Authority to act on behalf of healthcare provider organisation

For paragraph 43(b) of the Act, it is a requirement that a healthcare provider organisation ensure that:

(a) if the organisation is a seed organisation – the organisation's responsible officer and organisation maintenance officer are authorised to act on the organisation's behalf in its dealings with the System Operator; and

(b) if the organisation is a network organisation – the following individuals are authorised to act on the organisation's behalf in its dealings with the System Operator:

(i) the responsible officer and the organisation maintenance officer of the seed organisation for the network hierarchy to which the network organisation belongs;

(ii) the organisation's organisation maintenance officer.

22. Requirements for seed organisation, etc to participate

For paragraph 43(b) of the Act, it is a requirement that within a network hierarchy:

(a) the seed organisation be registered under Division 2 of Part 3 of the Act in order for any network organisation within the network hierarchy to be registered;

(b) the healthcare provider organisation that is directly hierarchically superior to a network organisation (***the applicant organisation***) be registered under Division 2 of Part 3 of the Act in order for the applicant organisation to be registered;

(c) healthcare provider organisations ensure that their organisation maintenance officer, and if relevant their responsible officer, establish and maintain an accurate and up-to-date record with the service operator of the linkages between organisations within the network hierarchy; and

(d) healthcare provider organisations ensure that their organisation maintenance officers establish and maintain with the service operator an accurate and up-to-date list of all identified healthcare providers who are individuals who are authorised to access the PCEHR system via or on behalf of the organisation using the provider portal.

23. Registration of network organisations

For paragraph 43(b) of the Act, it is a requirement that a seed organisation ensure that its network hierarchy be established and maintained in a manner that permits the assignment of access flags in accordance with rules 8 and 9.

Division 2

Security requirements

24. Requirements for registration

For paragraph 43(b) of the Act, it is a requirement that a healthcare provider organisation comply with the requirements specified in this Division in order to be eligible, and remain eligible, for registration under Division 2 of Part 3 of the Act.

25. Healthcare provider organisation policies

(1) Healthcare provider organisations must have a written policy that reasonably addresses the matters specified in subrule (4).

(2) Healthcare provider organisations must communicate the policy mentioned in subrule (1), and ensure that the policy remains readily accessible, to all its employees and to any healthcare providers to whom the organisation supplies services under contract.

Example: A healthcare provider organisation that supplies information technology services to individual healthcare providers, via which those providers access the PCEHR system, must communicate the policy to the providers.

(3) Healthcare provider organisations must enforce the policy mentioned in subrule (1) in relation to all its employees and any healthcare providers to whom the organisation supplies services under contract.

(4) Without limiting the matters a healthcare provider organisation's policy must reasonably address, the policy is, subject to subrule (5), to address the following:

(a) the manner of authorising persons accessing the PCEHR system via or on behalf of the healthcare provider organisation, including the manner of suspending and deactivating the user account of any authorised person:

(i) who leaves the healthcare provider organisation;

(ii) whose security has been compromised; or

(iii) whose duties no longer require them to access the PCEHR system;

(b) the training that will be provided before a person is authorised to access the PCEHR system, including in relation to how to use the PCEHR system accurately and responsibly, the legal obligations on

healthcare provider organisations and individuals using the PCEHR system and the consequences of breaching those obligations;

(c) the process for identifying a person who requests access to a consumer's PCEHR and communicating the person's identity to the System Operator so that the healthcare provider organisation is able to meet its obligations under section 74 of the Act;

(d) the physical and information security measures that are to be established and adhered to by the healthcare provider organisation and people accessing the PCEHR system via or on behalf of the healthcare provider organisation, including the user account management measures that must be implemented under rule 27; and

(e) mitigation strategies to ensure PCEHR-related security risks can be promptly identified, acted upon and reported to the healthcare provider organisation's management.

(5) If in the reasonable opinion of a healthcare provider organisation, a requirement in subrule (4) is not applicable to the organisation due to the limited size of the organisation, the organisation's policy need not address that requirement.

(6) Healthcare provider organisations must ensure that:

(a) the policy mentioned in subrule (1) is:

(i) drafted in such a manner that the organisation's performance can be audited against the policy to determine if the organisation has complied with the policy; and

(ii) kept up-to-date;

(b) each iteration of the policy contains a unique version number and the date when that iteration came into effect;

(c) without limiting paragraph (6)(a)(ii) – the policy is reviewed at least annually and when any material new or changed risks are identified. The review must include consideration of:

(i) factors that might result in:

(A) unauthorised access to the PCEHR system using the healthcare provider organisation's information systems;

(B) the misuse or unauthorised disclosure of information from a consumer's PCEHR by persons authorised to access the PCEHR system via or on behalf of the healthcare provider organisation; and

(C) the accidental disclosure of information contained in a consumer's PCEHR;

(ii) any changes to the PCEHR system that may affect the healthcare provider organisation; and

(iii) any relevant legal or regulatory changes that have occurred since the last review; and

(d) a record of each iteration of the policy mentioned in subrule (1) is retained in accordance with the record keeping obligations (if any) applicable to the healthcare provider organisation.

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

(1) The System Operator may request in writing that a healthcare provider organisation give it a copy of the policy mentioned in subrule 25(1).

(2) A healthcare provider organisation must comply with a request from the System Operator under this rule within 7 days of receiving the request.

(3) The System Operator may request a healthcare provider organisation's current policy or the policy that was in force on a specified date.

27. User account management within healthcare provider organisations

Healthcare provider organisations must ensure that their information technology systems, which are used by people to access the PCEHR system via or on behalf of the healthcare provider organisation, employ reasonable user account management practices including:

(a) restricting access to those persons who require access as part of their duties;

(b) uniquely identifying individuals using the healthcare provider organisation's information technology systems, and having that unique identity protected by a password or equivalent protection mechanism;

(c) having password and/or other access mechanisms that are sufficiently secure and robust given the security and privacy risks associated with unauthorised access to the PCEHR system;

(d) ensuring that the user accounts of persons no longer authorised to access the PCEHR system via or on behalf of the healthcare provider organisation prevent access to the PCEHR system; and

(e) suspending a user account that enables access to the PCEHR system as soon as practicable after becoming aware that the account or its password or access mechanism has been compromised.

28. Retention of record codes and document codes

Healthcare provider organisations must ensure that people using their information technology systems to access the PCEHR system via or on behalf of the organisation do not record, store or retain a copy of a consumer's record code or document code for the purposes of accessing the consumer's PCEHR, or a record in the consumer's PCEHR, in the future.

Note: Where a record code or document code is used to access a PCEHR or a record in a PCEHR, the code is not stored in the healthcare provider organisation's clinical information system. For example, using a record code places the organisation on the access list for the consumer's PCEHR, and information about this permitted access is stored by the System Operator. It will not be

necessary for a healthcare provider organisation to enter the record code each time access is needed to the same consumer's PCEHR, provided the organisation remains on the access list for the consumer's PCEHR.

Division 3 Responding to information security threats

29. Access to the PCEHR system may be suspended

(1) If the System Operator considers that the security or integrity of the PCEHR System has been, or may be, compromised by the information technology systems of a participant in the PCEHR system, the System Operator may suspend the participant's access to the PCEHR system with immediate effect.

(2) In this rule, the information technology systems of a participant in the PCEHR system include the credentials that enable a participant's identity to be authenticated in electronic transmissions.

(3) The System Operator must notify in writing a participant whose access to the PCEHR system has been suspended under subrule (1).

(4) The notice in subrule (3) must be given as soon as practicable after suspension occurs and must specify:

(a) the reasons for suspension; and

(b) the steps that the System Operator requires the participant to take before the participant's access to the PCEHR system is restored.

(5) The System Operator must restore access to the PCEHR system for a participant whose access was suspended under subrule (1) as soon as practicable after the System Operator is satisfied that the participant's information technology systems no longer compromise, or may compromise, the security or integrity of the PCEHR system.

30. Effect of suspension of access

Nothing in rule 29 affects the registration of a participant in the PCEHR system under the Act.