My Health Records Rule 2016

My Health Records Act 2012

I, SUSSAN LEY, Minister for Health, make this Rule under section 109 of the *My Health Records Act 2012*.

Dated 2/2/16

SUSSAN LEY
Minister for Health

Federal Register of Legislative Instruments F2016L00095

Contents

Part 1 Preliminary

1. Name of Rule

This Rule is the *My Health Records Rule 2016*.

2. Commencement

(1) Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information

Column 1	Column 2	Column 3
Provisions	**Commencement**	**Date/Details**
The whole of this instrument	The day after this instrument is registered.	

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

3. Repeal

This Rule repeals the following legislative instruments:

(a) the *PCEHR Rules 2012*; and

(b) the *PCEHR (Participation Agreements) Rules 2012*.

4. Definitions

In this Rule, 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 healthcare recipient's My Health Record.

access list means the record associated with a healthcare recipient's My Health Record that specifies the registered healthcare provider organisations permitted to access the healthcare recipient's My Health Record.

Act means the *My Health Records Act 2012*.

advanced access controls means the access controls that enable a registered healthcare recipient to set controls on the registered healthcare provider organisations and nominated representatives who may access the healthcare recipient's My Health Record, and the records within the My Health Record.

Federal Register of Legislative Instruments F2016L00095

assisted registration has the meaning in the *My Health Records (Assisted Registration) Rule 2015*.

contracted service provider officer has the same meaning given by subrule 36(4).

default access controls means the access controls that apply where a registered healthcare recipient has not set controls on the registered healthcare provider organisations or nominated representatives who may access the healthcare recipient's My Health Record.

document code means a code which may be used to restrict access to individual records within a healthcare recipient's My Health Record in accordance with paragraph 6(1)(c).

effectively remove, in relation to a record in a healthcare recipient's My Health Record, means rendering the record inaccessible to the healthcare recipient, their nominated representatives and any registered healthcare provider organisations involved in the care of the healthcare recipient, including in the case of a serious threat in accordance with rules 7 and 8.

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

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

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

interoperability requirements means the requirements published by the System Operator from time to time specifying the technical and compliance prerequisites that entities must meet in order to connect, and remain connected, with the My Health Record system.

linked registered healthcare provider organisation has the same meaning given by subrule 34(2).

material change in relation to a participant in the My Health Record System includes:

(c) a change in the financial administration status of the participant;

(d) a change in the participant's legal name;

(e) a change in the participant's legal structure; or

(f) the participant being involved in a merger or acquisition.

national registration authority has the same meaning as in the *Healthcare Identifiers Act 2010*.

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

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

Federal Register of Legislative Instruments F2016L00095

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

operator means a repository operator or a portal operator.

operator officer has the same meaning given by subrule 53(4).

portal operator means a person that is the operator of an electronic interface that facilitates, or can facilitate, access to the My Health Record system.

provenance information means:

(a) information or a healthcare identifier that identifies a healthcare recipient, an individual healthcare provider or a healthcare provider organisation; or

(b) a flag which identifies a document type.

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

record code means a code which may be used to restrict access to a healthcare recipient's My Health Record in accordance with paragraph 6(1)(a).

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

repository operator means a person that holds, or can hold, records of information included in My Health Records for the purposes of the My Health Record system.

restore, in relation to a record, means making a record, which has previously been effectively removed, accessible to the healthcare recipient, their nominated representatives and any registered healthcare provider organisations involved in the care of the healthcare recipient 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 My Health Record, has the meaning given by subrule 11(2).

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

Note 2: Unless the contrary intention appears, terms used in this My Health Records Rule have the same meaning as in the Act— see section 13 of the *Legislative Instruments Act 2003*. These terms include:
approved form, ***authorised representative***, ***employee***, ***healthcare provider organisation***, ***healthcare recipient***, ***healthcare recipient -only notes***, ***individual healthcare provider***, ***nominated representative***, ***My Health Record***, ***My Health Record system***, ***participant in the My Health Record system***, ***registered healthcare recipient***, ***registered healthcare provider organisation***, ***shared health summary*** and ***System Operator***.

Federal Register of Legislative Instruments F2016L00095

Part 2 Access control mechanisms

Division 1 Default access controls

5. 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 healthcare recipient to access the healthcare recipient's My Health Record;

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

(c) permit registered healthcare recipients to view the access list for their My Health Record;

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

(e) permit registered healthcare recipients to:

(i) effectively remove records from their My Health Record; 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 healthcare recipient's My Health Record 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 healthcare recipient's My Health Record.

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 — see rules 9 and 10.

Division 2 Advanced access controls

6. 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 7 and 8, permit use of a record code to prevent registered healthcare provider organisations involved in the care of a registered healthcare recipient from accessing the healthcare recipient's My Health Record unless:

Federal Register of Legislative Instruments F2016L00095

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

(A) the healthcare recipient; or

(B) the System Operator at the request of the healthcare recipient; or

(ii) the organisation is already on the access list for the healthcare recipient's My Health Record;

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

(c) permit registered healthcare recipients to control access to individual records in their My Health Record:

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

(ii) using a document code,

in accordance with subrule (2); and

(d) permit registered healthcare recipients to be alerted by means of an electronic communication when their My Health Record is accessed by a third party.

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

(a) registered healthcare recipients are able to prevent access to a record in their My Health Record, other than shared health summaries and healthcare recipient-entered health summaries, unless:

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

(A) the healthcare recipient; or

(B) the System Operator at the request of the healthcare recipient; or

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

(b) where a healthcare recipient 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 My Health Record system, without the need to use the healthcare recipient's document code;

(ii) the record may still be accessed by registered healthcare provider organisations and other participants in the My Health Record system in the case of a serious threat in accordance with rules 7 and 8;

Federal Register of Legislative Instruments F2016L00095

(iii) healthcare recipients 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 healthcare recipient 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 healthcare recipient's My Health Record unless:

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

(B) the healthcare recipient 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 My Health Record system; and

(c) all records uploaded to the healthcare recipient's My Health Record 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 healthcare recipient's My Health Record, the System Operator must ensure that a registered healthcare recipient 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 — see rules 9 and 10. Once a record code has been given to a registered healthcare provider organisation, the healthcare recipient will not subsequently need to give their record code to the same organisation provided that the organisation remains on the access list for the healthcare recipient's My Health Record. Where a registered healthcare provider organisation is given a healthcare recipient's record code, and is added to the access list for the healthcare recipient's My Health Record, the other healthcare provider organisations (if any) on the access list for the healthcare recipient's My Health Record are unaffected.

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

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

Note 4: While records uploaded to a healthcare recipient's My Health Record will, as a default, be uploaded without a document code applied to the record, healthcare recipients will be able to subsequently restrict access to the record by applying a

Federal Register of Legislative Instruments F2016L00095

document code if they wish. Healthcare recipients are able to change the default setting in relation to healthcare provider organisations on the access list for the healthcare recipient's My Health Record.

Note 5: Rule 45 provides that healthcare provider organisations must not retain a healthcare recipient's record code or document code for future use to access the healthcare recipient's My Health Record or a record in the healthcare recipient's My Health Record.

Division 3 Access control mechanisms and serious threats

7. 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 healthcare recipient's My Health Record regardless of whether a healthcare recipient has set up a record code;

(b) must allow access to all records in a healthcare recipient's My Health Record regardless of whether a healthcare recipient has set up a document code; and

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

Note 1: Healthcare recipient-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 — see rules 9 and 10.

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

8. 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 healthcare recipient's My Health Record regardless of whether a healthcare recipient has set up a record code;

Federal Register of Legislative Instruments F2016L00095

(b) must allow access to all records in a healthcare recipient's My Health Record regardless of whether a healthcare recipient has set up a document code; and

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

Note 1: Healthcare recipient-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 — see rules 9 and 10.

Division 4 Access flags

9. 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 healthcare recipient's My Health Record where a registered healthcare provider organisation accesses the healthcare recipient's My Health Record 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 healthcare recipient's My Health Record 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;

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

Principles for setting and maintaining access flags

(d) access flags must be set and maintained in accordance with the principles in rule 10.

Note: A network consists of a seed organisation and one or more network organisations— see subsection 9A(4) of the *Healthcare Identifiers Act 2010*. 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.

Federal Register of Legislative Instruments F2016L00095

10. 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 in a manner which balances:

(a) reasonable healthcare recipient expectations about the sharing of health information as part of providing healthcare to the healthcare recipient; 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 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, 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; 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, 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 28 requires seed organisations to structure their network 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 healthcare recipient's My Health Record

11. Automatic cancellation when a healthcare recipient takes control

(1) The System Operator must automatically cancel access to a healthcare recipient's My Health Record for all the healthcare recipient's authorised representatives and nominated representatives upon the earlier of the following:

(a) the healthcare recipient taking control of his or her My Health Record;

(b) the healthcare recipient reaching the age of 18.

(2) A healthcare recipient takes control of his or her My Health Record if:

Federal Register of Legislative Instruments F2016L00095

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

(b) the healthcare recipient has:

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

(ii) if the healthcare recipient wishes to access his or her My Health Record online or adjust their My Health Record's access control mechanisms online – organised his or her own My Health Record log-in details with the System Operator.

(3) Despite paragraph (1)(b), the System Operator must not cancel access to a healthcare recipient's My Health Record 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 healthcare recipient reaches the age of 18, be an authorised representative for the healthcare recipient under subsection 6(4) of the Act.

Note: Rule 24 requires the System Operator to verify the identity of a healthcare recipient where the healthcare recipient ceases to have an authorised representative.

12. Suspension on death of healthcare recipient

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

Note 1: Where the status of a healthcare recipient's healthcare identifier is deceased, this indicates that evidence of the healthcare recipient'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 healthcare recipient's healthcare identifier has been retired (that is, fact of death data has been received), the System Operator must cancel the healthcare recipient's registration under subsection 51(6) of the Act. Where a healthcare recipient's registration is cancelled, access to the healthcare recipient's My Health Record ceases for authorised representatives and nominated representatives.

13. Suspension and cancellation where representation ceases

(1) The System Operator must cancel access to a healthcare recipient's My Health Record for a person who is an authorised representative or a nominated representative of the healthcare recipient 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;

Federal Register of Legislative Instruments F2016L00095

(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 healthcare recipient; or

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

(2) The System Operator must suspend access to a healthcare recipient's My Health Record for a person who is an authorised representative or a nominated representative of the healthcare recipient 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 healthcare recipient's My Health Record for a healthcare recipient'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 healthcare recipient's My Health Record for an authorised representative under this rule, the System Operator must also suspend or cancel access to the healthcare recipient's My Health Record for all nominated representatives that were nominated by that authorised representative.

Note 1: A nominated representative may not be required to have a healthcare identifier—see subsection 7(3) of the Act.

Note 2: Where access to a healthcare recipient's My Health Record 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 healthcare recipient.

14. Suspension while investigating eligibility

(1) Until a decision is made under subrule (3), the System Operator must suspend access to a healthcare recipient's My Health Record for all a healthcare recipient'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 healthcare recipient'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 healthcare recipient's My Health Record for a person if the System Operator is no longer satisfied that the person is eligible to be the healthcare recipient's authorised representative; or

(b) restore access to the healthcare recipient's My Health Record for a person if the System Operator is satisfied that the person remains eligible to be the healthcare recipient's authorised representative.

Federal Register of Legislative Instruments F2016L00095

(4) If the System Operator cancels access to a healthcare recipient's My Health Record for a person (the ***first person***) under paragraph (3)(a), the System Operator must also cancel access to the healthcare recipient's My Health Record for the nominated representatives (if any) that were nominated by the first person.

Note 1: A decision about whether a person is or is not the authorised representative of a healthcare recipient 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 healthcare recipient's My Health Record 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 healthcare recipient.

15. Temporary suspension in the case of a serious risk to a healthcare recipient

(1) The System Operator must suspend access to a healthcare recipient's My Health Record for all the healthcare recipient's authorised representatives and nominated representatives if:

(a) an authorised representative of the healthcare recipient notifies the System Operator that continuing access to the healthcare recipient's My Health Record 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 15 would not prevent a decision being made to suspend access under rule 14 if a claim about an authorised representative's eligibility is notified to the System Operator under subrule 14(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 15(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 healthcare recipient's registration on request.

16. Effect of suspension or cancellation

Nothing in this Division affects:

(a) a healthcare recipient's registration under the Act; or

(b) the access control mechanisms that were in place for the healthcare recipient's My Health Record immediately before any suspension or

Federal Register of Legislative Instruments F2016L00095

cancellation of access to the healthcare recipient's My Health Record occurred.

Federal Register of Legislative Instruments F2016L00095

Part 3 Security, operations, administration and uploading records

17. Suspension of access in the case of risk to security, integrity or operation of My Health Record system

(1) If the System Operator considers that the security, integrity or operations of the My Health Record system have been, or may be, compromised, the System Operator may suspend access to the My Health Record system with immediate effect for an entity, or for a class or classes of:

(a) healthcare recipients;

(b) authorised representatives;

(c) nominated representatives; or

(d) participants in the My Health Record system.

(2) Without limiting subrule (1), the security, integrity or operations of the My Health Record system may be compromised if:

(a) there is a security problem with the information technology systems of a participant in the My Health Record system, or with the credentials that enable a participant's identity to be authenticated in electronic communications;

(b) there is an issue with verification of the identity of a healthcare recipient or their representative; or

(c) a participant in the My Health Record system has failed to maintain interoperability in accordance with rules 31, 39 or 56.

(3) Where a participant in the My Health Record system has failed to maintain interoperability in accordance with rules 31, 39 or 56, the System Operator may suspend the participant's access to the My Health Record system in full or in part.

Example: Under subrule 17(3), the System Operator may decide to suspend all access by a participant to the My Health Record system. Alternatively, the System Operator may decide to partially suspend access to the My Health Record system by preventing the participant uploading a class of documents (such as shared health summaries) until the participant restores interoperability with the My Health Record system in accordance with the System Operator's interoperability requirements.

(4) The System Operator must notify, in writing, the healthcare recipient or other entity whose access to the My Health Record system has been suspended under subrule (1).

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

(a) the reasons for suspension; and

(b) the steps, if any, that the System Operator requires the healthcare recipient or other entity to take before the recipient's or entity's access to the My Health Record system is restored.

Federal Register of Legislative Instruments F2016L00095

(6) If, in the reasonable opinion of the System Operator, the suspension of access relates to minor operational matters and is unlikely to last for more than 24 hours, the System Operator does not need to comply with subrules (4) or (5).

(7) If, in the reasonable opinion of the System Operator, the suspension of access affects a significant number of healthcare recipients, the System Operator may notify the general public instead of complying with subrule (4).

(8) The System Operator must restore access to the My Health Record system for a healthcare recipient or other entity whose access was suspended under subrule (1) as soon as practicable after the System Operator is satisfied that the security, integrity or operations of the My Health Record system are no longer compromised or are no longer at risk of compromise.

(9) Nothing in this rule affects:

(a) a healthcare recipient's or other entity's registration under the Act; or

(b) the access control mechanisms that were in place for a healthcare recipient's My Health Record immediately before any suspension of access to the My Health Record system for the recipient or her or his representatives.

18. My Health Record system availability

On the request of a participant in the My Health Record system, the System Operator must provide the participant with details of when the My Health Record System was unavailable.

19. 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 *My Health Records Regulation 2012* place restrictions on the uploading of records to the My Health Record system.

20. Restriction on uploading records prepared by healthcare providers whose registration or membership is suspended, cancelled, etc.

For the purposes of subparagraphs 45(ba)(i) and (ii) of the Act, a healthcare provider organisation may upload to a repository a record prepared by an individual whose registration or membership is, at the time the record is prepared, suspended because the individual's registration or membership fees are less than six month's overdue.

21. Effective removal of records

(1) The System Operator may effectively remove, or may direct a participant in the My Health Record system to effectively remove, a record in the My

Federal Register of Legislative Instruments F2016L00095

Health Record system to the extent that the System Operator reasonably considers that:

(a) the record contains a defamatory statement;

(b) the record affects, or is likely to affect, the security, integrity or operations of the My Health Record system; or

(c) both the following are satisfied:

(i) the record was uploaded in contravention of paragraph 45(ba) of the Act; and

(ii) the record should be effectively removed to reduce the clinical risk that is, or may be, faced by a healthcare recipient if the record is not effectively removed.

Example: The System Operator may decide to effectively remove a record under paragraph 1(c) where the authoring individual healthcare provider's registration with the national registration authority has been suspended for professional negligence, and the System Operator considers that effectively removing the record would reduce the clinical risk faced by the healthcare recipient about whom the record relates.

(2) A participant in the My Health Record 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 My Health Record system to effectively remove, a record under subrule (1):

(a) the System Operator must notify in writing:

(i) the healthcare recipient from whose My Health Record 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 My Health Record 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 My Health Record system.

22. 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 My Health Record purposes without the prior written approval of the System Operator.

Federal Register of Legislative Instruments F2016L00095

Part 4 Identity verification

23. Requirement for verified healthcare identifier

(1) For the purposes of paragraph 41(1)(c) of the Act, and paragraphs 3(1)(b) and 6(3)(c) of Schedule 1 to the Act, the System Operator must be satisfied that the healthcare recipient 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 healthcare recipient has been appropriately verified.

24. Identity verification on ceasing to have an authorised representative

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

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

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

Note: Subrule 11(2) specifies when a healthcare recipient takes control of his or her My Health Record.

Federal Register of Legislative Instruments F2016L00095

Part 5 Participation requirements for healthcare provider organisations and contracted service providers

Division 1 General requirements of healthcare provider organisations

25. Registration Requirements

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.

26. Authority to act on behalf of healthcare provider organisation

A healthcare provider organisation must ensure that:

(a) if the organisation is a seed organisation, or if it is not part of a network – 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 to which the network organisation belongs; and

(ii) the organisation's organisation maintenance officer.

27. Requirements to participate

(1) Healthcare provider organisations must ensure that their organisation maintenance officers establish and maintain with the System Operator an accurate and up-to-date list of all identified healthcare providers who are individuals who are authorised to access the My Health Record system via or on behalf of the organisation using the provider portal.

(2) Within a network:

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

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

Federal Register of Legislative Instruments F2016L00095

(c) healthcare provider organisations must 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.

28. Registration of network organisations

A seed organisation must ensure that its network is established and maintained in a manner that permits the assignment of access flags in accordance with rules 9 and 10.

29. Exercising due care and skill when uploading or downloading records

(1) A healthcare provider organisation must take reasonable steps to ensure that they and their employees exercise due care and skill:

(a) so that any record that they or their employees upload to the My Health Record system is, at the time the record is uploaded, accurate, up-to-date, not misleading and not defamatory; and

(b) about whether any records that they or their employees access via, or download from, the My Health Record system are accurate, up-to-date and fit for purpose.

(2) Subrule (1)(a) does not apply if:

(a) the record being uploaded was created by an individual who was not, at the time the record was created, an employee of the uploading healthcare provider organisation; and

(b) there is nothing in the record that would indicate to a reasonable person in the circumstances that the record was not accurate or up-to-date.

(3) The uploading of a record to the My Health Record system does not affect any other obligation a healthcare provider organisation or their employees may have to:

(a) keep clinical records about a healthcare recipient; or

(b) communicate health information to a healthcare recipient.

30. Requirement to notify the System Operator of certain things

(1) This rule applies if a healthcare provider organisation:

(a) becomes aware or suspects that there is a non-clinical, My Health Record system-related error in a record that has been accessed via, or downloaded from, the My Health Record system by it or its employees; or

(b) undergoes a material change.

(2) A healthcare provider organisation must:

Federal Register of Legislative Instruments F2016L00095

(a) give the System Operator, in writing, details of the error or material change; and

(b) do so within two business days of become aware or suspecting the error, or undergoing the material change.

Example: A healthcare provider organisation must promptly notify the System Operator if they or their employees become aware of an uploaded record which appears to have been corrupted during upload.

31. Requirement to maintain interoperability

A healthcare provider organisation must maintain interoperability with the My Health Record system in accordance with the System Operator's interoperability requirements.

32. Requirement to provide assistance

(1) At the System Operator's request, a healthcare provider organisation must promptly provide all necessary assistance in relation to any inquiry, audit, review, assessment, investigation or complaint in connection with the My Health Record system conducted, handled, requested or facilitated by the System Operator.

(2) Subrule (1) does not apply unless the System Operator gives the healthcare provider organisation reasonable notice of the assistance required.

Division 2 General requirements of contracted service providers

33. Requirements for registration

For paragraph 48(a) of the Act, it is a requirement that a contracted service provider comply with the requirements specified in this Division in order to be eligible, and remain eligible, for registration under Division 3 of Part 3 of the Act.

34. Link to a healthcare provider organisation

(1) A contracted service provider must be linked to one or more registered healthcare provider organisations.

(2) For the purposes of subrule (1), a contracted service provider is ***linked*** to a registered healthcare provider organisation if:

(a) there is a contract in force between the contracted service provider and the registered healthcare provider organisation under which the contracted service provider provides to the registered healthcare provider organisation:

(i) information technology services related to the My Health Record system; or

(ii) health information management services relating to the My Health Record system; and

Federal Register of Legislative Instruments F2016L00095

(b) the registered healthcare provider organisation has:

(i) notified the System Operator of the link between itself and the contracted service provider; and

(ii) not notified the System Operator that the link between itself and the contracted service provider is no longer current.

(3) A contracted service provider will no longer be linked to a registered healthcare provider organisation if:

(a) the contracted service provider's contract with the healthcare provider organisation expires or is terminated; or

(b) the registered healthcare provider organisation notifies the System Operator that the link between itself and the contracted service provider is no longer current.

(4) If a contracted service provider contravenes subrule (1), the System Operator may suspend or cancel the contracted service provider's access to the My Health Record system.

35. Registration with service operator

A contracted service provider must register with the service operator as a contracted service provider.

36. Appointment of contracted service provider officer

(1) A contracted service provider must appoint a contracted service provider officer, who is employed by the contracted service provider.

(2) The contracted service provider must have at least one, but no more than three, contracted service provider officers at all times.

(3) A contracted service provider must ensure that its contracted service provider officer appointed under subrule (1) carries out the duties prescribed under subrule (4).

(4) A person is the ***contracted service provider officer*** for a contracted service provider if the duties of the person include the following:

(a) receiving communications from the System Operator about the operation of the My Health Record system;

(b) acting as a liaison between the System Operator and the contracted service provider; and

(c) maintaining the System Operator's records about the professional and business details of the contracted service provider officer and the contracted service provider.

37. Access to the My Health Record System

(1) A contracted service provider must only use or access the My Health Record system to the extent they have been instructed to do so by a linked registered healthcare provider organisation.

(2) Each time a contracted service provider accesses the My Health Record system, or collects, uses or discloses a record from or to the My Health Record system, the contracted service provider must give the System Operator the healthcare identifier of the linked registered healthcare provider organisation which instructed the contracted service provider to access the My Health Record system or to collect, use or disclose the record.

38. Requirement to notify the System Operator of certain things

(1) This rule applies if a contracted service provider:

(a) becomes aware, or suspects, that:

(i) the contracted service provider has given the System Operator, or uploaded to the My Health Record system, inaccurate provenance information;

(ii) there is a non-clinical, My Health Record system-related error in a record that has been accessed via, or downloaded from, the My Health Record system;

(iii) under rule 34(3), a registered healthcare provider organisation for which the contracted service provider provides services is no longer linked to the contracted service provider;

(b) undergoes a material change;

(c) has appointed, or cancelled the appointment of, a contracted service provider officer under rule 36; or

(d) changes, or becomes aware of a change in, the professional or business details of its currently appointed contracted service provider officer.

(2) A contracted service provider must:

(a) give the System Operator, in writing, details of the event or circumstances; and

(b) do so within two business days of become aware or suspecting the event or circumstance.

39. Requirement to maintain interoperability

A contracted service provider must maintain interoperability with the My Health Record system in accordance with the System Operator's interoperability requirements.

40. Requirement to provide assistance

(1) At the System Operator's request, a contracted service provider must promptly provide all necessary assistance in relation to any inquiry, audit, review, assessment, investigation or complaint in connection with the My Health Record system conducted, handled, requested or facilitated by the System Operator.

Federal Register of Legislative Instruments F2016L00095

(2) Subrule (1) does not apply unless the System Operator gives the contracted service provider reasonable notice of the assistance required.

Division 3 Security requirements for healthcare provider organisations

41. 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.

42. 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 My Health Record 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 My Health Record 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 My Health Record system;

(b) the training that will be provided to healthcare provider organisation employees before they are authorised to access the My Health Record system, including in relation to how to use the My Health Record system accurately and responsibly, the legal obligations on healthcare provider organisations and individuals using the My Health Record system and the consequences of breaching those obligations;

Federal Register of Legislative Instruments F2016L00095

(c) the process for identifying a person who requests access to a healthcare recipient's My Health Record 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 My Health Record system via or on behalf of the healthcare provider organisation, including the user account management measures that must be implemented under rule 44;

(e) mitigation strategies to ensure My Health Record system-related security risks can be promptly identified, acted upon and reported to the healthcare provider organisation's management; and

(f) where the healthcare provider organisation provides assisted registration:

(i) the manner of authorising employees of the organisation to provide assisted registration;

(ii) the training that will be provided before a person is authorised to provide assisted registration;

(iii) the manner of confirming a healthcare recipient's consent for the purposes of rule 9 of the *My Health Records (Assisted Registration) Rule 2015*; and

(iv) the process and criteria for identifying a healthcare recipient for the purposes of assisted registration.

(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 My Health Record system using the healthcare provider organisation's information systems;

(B) the misuse or unauthorised disclosure of information from a healthcare recipient's My

Federal Register of Legislative Instruments F2016L00095

Health Record by persons authorised to access the My Health Record system via or on behalf of the healthcare provider organisation; and

(C) the accidental disclosure of information contained in a healthcare recipient's My Health Record;

(ii) any changes to the My Health Record 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.

43. 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 42(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.

44. 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 My Health Record 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 My Health Record system;

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

(e) suspending a user account that enables access to the My Health Record system as soon as practicable after becoming aware that the

Federal Register of Legislative Instruments F2016L00095

account or its password or access mechanism has been compromised.

45. Retention of record codes and document codes

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

Note: Where a record code or document code is used to access a My Health Record or a record in a My Health Record, 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 healthcare recipient's My Health Record, 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 healthcare recipient's My Health Record, provided the organisation remains on the access list for the healthcare recipient's My Health Record.

Division 4 Security requirements for contracted service providers

46. Requirements for registration

For paragraph 48(a) of the Act, it is a requirement that a contracted service provider comply with the requirements specified in this Division in order to be eligible, and remain eligible, for registration under Division 3 of Part 3 of the Act.

47. Contracted service provider policies

(1) Contracted service providers must have a written policy that reasonably addresses the matters specified in subrule (4).

(2) Contracted service providers must communicate the policy mentioned in subrule (1), and ensure that the policy remains readily accessible, to all its employees.

(3) Contracted service providers must enforce the policy mentioned in subrule (1) in relation to all its employees.

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

(a) the manner of authorising persons accessing the My Health Record system via or on behalf of the contracted service provider's linked healthcare provider organisation, including the manner of suspending and deactivating the user account of any authorised person:

Federal Register of Legislative Instruments F2016L00095

(i) who leaves the contracted service provider;

(ii) whose security has been compromised; or

(iii) whose duties no longer require them to access the My Health Record system on behalf of a linked healthcare provider organisation;

(b) the training that will be provided to contracted service provider employees before they are authorised to access the My Health Record system, including in relation to how to use the My Health Record system accurately and responsibly, the legal obligations on contracted service providers and individuals using the My Health Record system and the consequences of breaching those obligations;

(c) the physical and information security measures that are to be established and adhered to by the contracted service provider, including the user account management measures that must be implemented under rule 49; and

(d) mitigation strategies to ensure My Health Record system-related security risks can be promptly identified, acted upon and reported to the contracted service provider's management.

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

(6) Contracted service providers must ensure that:

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

(i) drafted in such a manner that the provider's performance can be audited against the policy to determine if the provider 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 My Health Record system using the contracted service provider's information systems;

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

(C) the accidental disclosure of information contained in a healthcare recipient's My Health Record;

(ii) any changes to the My Health Record system that may affect the contracted service provider; and

Federal Register of Legislative Instruments F2016L00095

(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 contracted service provider.

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

(1) The System Operator may request in writing that a contracted service provider give it a copy of the policy mentioned in subrule 47(1).

(2) A contracted service provider 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 contracted service provider's current policy or the policy that was in force on a specified date.

49. User account management within contracted service providers

Contracted service providers must ensure that their information technology systems, which are used to access the My Health Record system via or on behalf of linked healthcare provider organisations, 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 contracted service provider'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 My Health Record system;

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

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

50. Retention of record codes and document codes

Contracted service providers must ensure that people using their information technology systems to access the My Health Record system via or on behalf of a linked healthcare provider organisation do not record, store or retain a copy of a healthcare recipient's record code or document code for the

Federal Register of Legislative Instruments F2016L00095

purposes of accessing the healthcare recipient's My Health Record, or a record in the healthcare recipient's My Health Record, in the future.

Part 6 Participation requirements for operators

Division 1 General requirements

51. Application of this Division

This Division applies to an operator.

52. Requirements for registration

For paragraph 48(a) of the Act, it is a requirement that an operator complies with the requirements specified in this Division in order to be eligible, and remain eligible, for registration under Division 3 of Part 3 of the Act.

53. Appointment of operator officer

(1) An operator must appoint an operator officer who is employed by the operator.

(2) The operator must have at least one, but no more than three, operator officers at all times.

(3) The operator must ensure that its operator officer appointed under subrule (1) carries out the duties prescribed under subrule (4).

(4) A person is the ***operator officer*** for an operator if the duties of the person include the following:

(a) receiving communications from the System Operator about the operation of the My Health Record system;

(b) acting as a liaison between the System Operator and the operator; and

(c) maintaining the System Operator's records of the professional and business details of the operator and the operator officer.

54. Operator technical and after-hours contacts

An operator must:

(a) provide a point of contact and technical support for the operator during ordinary business hours Monday to Friday, other than public holidays; and

(b) at all other times provide at least two current points of contact who have the authority and are able to resolve, or coordinate the resolution of, any technical, security or operational issues affecting the operator.

55. Requirement to notify the System Operator of certain things

(1) This rule applies if an operator:

(a) becomes aware, or suspects, that:

Federal Register of Legislative Instruments F2016L00095

(i) there is a non-clinical, My Health Record system-related error in a record that has been accessed via, or downloaded from, the My Health Record system;

(ii) the operator has given the System Operator, or uploaded to the My Health Record system, inaccurate provenance information;

(b) undergoes a material change;

(c) has appointed or cancelled the appointment of an operator officer;

(d) changes, or becomes aware of a change in, the professional or business details of its currently appointed operator officer.

(2) An operator must:

(a) give the System Operator, in writing, details of the event or circumstances; and

(b) do so within two business days of become aware or suspecting the event or circumstance.

56. Requirement to maintain interoperability

An operator must maintain interoperability with the My Health Record system in accordance with the System Operator's interoperability requirements.

57. Requirement to provide assistance

(1) At the System Operator's request, an operator must promptly provide all necessary assistance in relation to any inquiry, audit, review, assessment, investigation or complaint in connection with the My Health Record system conducted, handled, requested or facilitated by the System Operator.

(2) Subrule (1) does not apply unless the System Operator gives the operator reasonable notice of the assistance required.

Division 2 Security requirements for operators

58. Requirements for registration

For paragraph 48(a) of the Act, it is a requirement that an operator comply with the requirements specified in this Division in order to be eligible, and remain eligible, for registration under Division 3 of Part 3 of the Act.

59. Operator policies

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

(2) Operators must communicate the policy mentioned in subrule (1), and ensure that the policy remains readily accessible, to all its employees.

(3) Operators must enforce the policy mentioned in subrule (1) in relation to all their employees.

Federal Register of Legislative Instruments F2016L00095

(4) Without limiting the matters an operator's policy must reasonably address, the policy is, subject to subrule (5), to address the following:

(a) the manner of authorising persons accessing the My Health Record system via or on behalf of the operator, including the manner of suspending and deactivating the user account of any authorised person:

(i) who leaves the operator;

(ii) whose security has been compromised; or

(iii) whose duties no longer require them to access the My Health Record system;

(b) the training that will be provided to operator employees before they are authorised to access the My Health Record system, including in relation to how to use the My Health Record system accurately and responsibly, the legal obligations on operators and individuals using the My Health Record system and the consequences of breaching those obligations;

(c) the physical and information security measures that are to be established and adhered to by the operator, including the user account management measures that must be implemented under rule 61; and

(d) mitigation strategies to ensure My Health Record system-related security risks can be promptly identified, acted upon and reported to the operator's management.

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

(6) Operators must ensure that:

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

(i) drafted in such a manner that the operator's performance can be audited against the policy to determine if the operator 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 My Health Record system using the operator's information systems;

(B) the misuse or unauthorised disclosure of information from a healthcare recipient's My Health Record by persons authorised to access the My Health Record system via or on behalf of an operator; and

Federal Register of Legislative Instruments F2016L00095

(C) the accidental disclosure of information contained in a healthcare recipient's My Health Record;

(ii) any changes to the My Health Record system that may affect the operator; 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 operator.

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

(1) The System Operator may request in writing that an operator give it a copy of the policy mentioned in subrule 59(1).

(2) An operator 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 an operator's current policy or the policy that was in force on a specified date.

61. User account management within operators

Operators must ensure that their information technology systems, which are used to access the My Health Record system, 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 operator'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 My Health Record system;

(d) ensuring that the user accounts of persons no longer authorised to access the My Health Record system prevent access to the My Health Record system; and

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

Division 3 Security requirements for portal operators

62. Requirements for registration

For paragraph 48(a) of the Act, it is a requirement that a portal operator comply with the requirements specified in this Division in order to be

Federal Register of Legislative Instruments F2016L00095

eligible, and remain eligible, for registration under Division 3 of Part 3 of the Act.

63. Retention of record codes and document codes by portal operators

(1) Portal operators must ensure that people using their information technology systems to access the My Health Record system do not record, store or retain a copy of a healthcare recipient's record code or document code for the purposes of accessing the healthcare recipient's My Health Record, or a record in the healthcare recipient's My Health Record, in the future.

(2) Subrule (1) does not apply to portal operators to the extent they operate a portal that provides access to the My Health Record system solely to healthcare recipients.

Federal Register of Legislative Instruments F2016L00095

Schedule 1—Application provisions

1. Definitions

In this Schedule:

the amending Act means the *Health Legislation Amendment (eHealth) Act 2015*.

the Rule means the *My Health Records Rule 2016*.

2. Repeal

Paragraph 3(b) of the Rule applies on and after the application day as defined in item 111 of Schedule 1 to the amending Act.

3. Security, operations, administration and uploading records

Paragraph 17(2)(c) and subrule 17(3) of the Rule apply on or after the application day as defined in item 111 of Schedule 1 to the amending Act.

4. Restriction on uploading records prepared by healthcare providers whose registration or membership is suspended, cancelled, etc.

Rule 20 of the Rule applies on or after the application day as defined in item 111 of Schedule 1 to the amending Act.

5. Effective removal of records

Paragraph 21(1)(c) of the Rule applies on or after the application day as defined in item 111 of Schedule 1 to the amending Act.

6. Participation requirements for healthcare provider organisations and contracted service providers

(1) Rules 29, 30, 31 and 32 of the Rule apply on or after the application day, as defined in item 111 of Schedule 1 to the amending Act.

(2) Divisions 2 and 4 of Part 5 of the Rule apply on or after the application day, as defined in item 111 of Schedule 1 to the amending Act.

7. Participation requirements for operators

Part 6 of the Rule applies on or after the application day, as defined in item 111 of Schedule 1 to the amending Act.

Federal Register of Legislative Instruments F2016L00095