EXPLANATORY STATEMENT

Issued by Authority of the Minister for Health

My Health Records Act 2012

My Health Records Rule 2016

The *My Health Records Act 2012* (the Act) provides for the establishment and operation of the My Health Record system to provide individuals and their healthcare providers with access to their key health information online where and when they need it. Section 109 of the Act provides that the Minister may make rules, known as My Health Records Rules, about matters that are required or permitted by the Act to be dealt with in the My Health Records Rules.

The purpose of the *My Health Records Rule 2016* (the Rules), in summary, is to support the secure operation of the My Health Record system by prescribing rules that relate to:

- access control mechanisms provided by the System Operator to individuals to manage their My Health Record;
- the security, integrity and operation of the My Health Record system;
- the handling of specified types of records;
- identity verification; and
- participation requirements for healthcare provider organisations, contracted service providers, repository operators and portal operators to be eligible to register and remain registered with the My Health Record system.

The Rules also repeal the *PCEHR (Participation Agreements) Rules 2012* so that healthcare provider organisations, contracted service providers, repository operators and portal operators will generally no longer need to enter into a participation agreement (a contract) with the System Operator in order to be, and remain eligible to be, registered.

The Rules are part of a suite of My Health Records Rules made by the Minister, including the *My Health Records (Assisted Registration) Rule 2015*, to support the operation of the My Health Record system.

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

Subsection 51(3) of the Act provides that failure to comply with the Act (which is defined in section 5 of the Act to include the My Health Records Rules) may result in a decision by the System Operator to cancel or suspend the registration of a registered healthcare provider organisation, registered repository operator, registered portal operator or registered contracted service provider. Further, section 78 of the Act provides that a person that is, or at any time has been, a registered healthcare provider organisation, a registered repository operator, a registered portal operator or a registered contracted service provider may be subject to a civil penalty of up to 100 penalty units ($18,000 for individuals or $90,000 for bodies corporate) if they contravene the My Health Records Rules.

The Rules do not relate to the professional activities of healthcare providers. Professional obligations and professional bodies exist for this purpose. The Rules only regulate matters necessary to ensure the efficient and secure operations of the My Health Record system, and the other purposes permitted by section 109 of the Act.

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

Detail of the Rules is set out in the Attachment.

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

The Independent Advisory Council and Jurisdictional Advisory Committee were consulted on the changes proposed to be made. These bodies were consulted in April, May, October and November 2015 and they supported the changes. The Australia Health Ministers' Advisory Council was also consulted.

The principal changes being implemented by the Rules were part of a public consultation process conducted in May and June 2015 upon the release of the *Electronic Health Records and Healthcare Identifiers: Legislation Discussion Paper*. The Department received more than 135 submissions from stakeholders including individuals, healthcare providers, research organisations and government agencies. These submissions informed the development of the Rules.

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

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

ATTACHMENT

Details of the *My Health Records Rule 2016*

PART 1—PRELIMINARY

1. Name of Rule

Rule 1 provides that the title of the rule is the *My Health Records Rule 2016*. In this explanatory statement it is referred to as the Rules.

2. Commencement

Rule 2 provides that the Rules will take effect on the day after they are registered on the Federal Register of Legislative Instruments.

3. Repeal

Rule 3 repeals the *PCEHR Rules 2012* and the *PCEHR (Participation Agreements) Rules 2012*.

4. Definitions

Rule 4 defines particular terms used in the Rules, including:

Access control mechanisms

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

Access control mechanisms will provide:

- ***default access controls*** – the settings that apply if an individual does not set controls on the registered healthcare provider organisations or nominated representatives who may access the individual's My Health Record. In summary, default access controls will enable registered healthcare provider organisations involved in the care of an individual to access the individual's My Health Record; and

- ***advanced access controls*** – the settings that allow an individual to specify which registered healthcare provider organisations and nominated representatives may access their My Health Record and to what degree.

Assisted registration

References to assisted registration have the same meaning as in the *My Health Records (Assisted Registration) Rule 2015*.

Contracted service provider officer

References to a contracted service provider officer have the same meaning given by subrule 36(4) of the Rules.

Document code

Document codes form part of the advanced access controls available to individuals. An individual who chooses to set advanced access controls on their My Health Record may choose to set up a document code (effectively a PIN or password) with which they can control access by registered healthcare provider organisations to individual records in their My Health Record.

In practice, a registered healthcare provider organisation provided with the document code by an individual only need to enter the code once. On entering the document code, the registered healthcare provider organisation is able to access all records in the individual's My Health Record which are protected by a document code.

Record code

Record codes form part of the advanced access controls available to individuals. An individual who chooses to set advanced access controls on their My Health Record may choose to set up a record code (effectively a PIN or password) with which they can control access to their My Health Record by registered healthcare provider organisations.

If the individual has set up a record code, registered healthcare provider organisations are unable to access the individual's My Health Record unless the individual has given them their record code (or the System Operator has done so on behalf of the individual) or the organisation was on the individual's ***access list*** before the individual set up a record code.

In practice, a registered healthcare provider organisation that has been given the record code by an individual only needs to enter this record code upon first accessing the individual's My Health Record. It would not be necessary to re-enter the record code each time the provider accessed the My Health Record. On entering the record code, the registered healthcare provider organisation would be added to the individual's ***access list*** which is a list maintained by the System Operator identifying those organisations which are permitted to access the individual's My Health Record. The individual can subsequently change the access level of the organisation if they wish.

Effectively remove

This term refers to the manner in which an individual may remove an individual record from their My Health Record. Effectively removing a record will mean it is not accessible through the individual's My Health Record to the individual, their nominated representatives or healthcare provider organisations, even in circumstances where there is a serious threat to an individual's life, health or safety or to public health or safety.

While an effectively removed record is no longer accessible through the individual's My Health Record, it may still be accessible via the System Operator for medico-legal reasons or other reasons authorised or required by law.

An individual may subsequently choose to ***restore*** a record that has been effectively removed from their My Health Record.

Interoperability requirements

References to interoperability requirements mean 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

References to a linked registered healthcare provider organisation have the same meaning given by subrule 34(2).

Material change

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

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

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

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

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

Network

This term refers to the network of healthcare provider organisations that may be established in accordance with subsection 9A(4) of the HI Act. A network is a group of healthcare provider organisations that comprises a ***seed organisation***, which is the head healthcare provider organisation of the network, and one or more ***network organisations*** that are subordinate to the seed organisation.

Operator

References to an operator mean a repository operator or a portal operator as defined by the Act.

Operator officer

References to an operator officer have the same meaning given by subrule 53(4) of the Rules.

Portal operator

A reference to a 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

References to 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

References to a 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.

Repository operator

A reference to a 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.

The note to rule 4 assists readers by making clear that other terms used in the Rules are have the same meaning as in the Act.

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

PART 2—ACCESS CONTROL MECHANISMS

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

DIVISION 1—DEFAULT ACCESS CONTROLS

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

5. Default access controls

Rule 5 provides that the default access controls must:

- allow any registered healthcare provider organisation that is involved in the care of a registered individual to access the individual's My Health Record (paragraph 4(a));

- include an access list which identifies those registered healthcare provider organisations that are permitted to access the individual's My Health Record (paragraph 4(b)). Upon gaining access to an individual's My Health Record, a registered healthcare provider organisation will be automatically added to the access list;

- allow a registered individual to view her or his access list and see which registered healthcare provider organisations are permitted to access the registered individual's My Health Record (paragraph 4(c));

- automatically remove a healthcare provider organisation from the individual's access list if the organisation has not accessed the individual's My Health Record for three years (paragraph 4(d));

- allow a registered individual to effectively remove a record from his or her My Health Record and to subsequently authorise the System Operator to restore that record (paragraph 4(e)), should the individual so wish; and

- allow a registered healthcare provider organisation that uploaded a record to an individual's My Health Record to access that record. If the organisation is no longer on

the access list for the individual's My Health Record, the organisation must make a request to the System Operator in order to gain access to the record (paragraph 4(f)).

The note to rule 5 makes clear that, where a healthcare provider organisation is added to or omitted from the access list for an individual's My Health Record, access flags set within the healthcare provider organisation's network affect which additional registered healthcare provider organisations (if any) are also added to, or omitted from, the access list for an individual's My Health Record. See Division 4 of Part 2 for more information about access flags.

DIVISION 2—ADVANCED ACCESS CONTROLS

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

6. Advanced access controls

Rule 6 provides that the advanced access control mechanisms to be established and maintained by the System Operator must have the same functionality as the default access controls and must:

- allow an individual to use a record code to control access to their My Health Record (paragraph 6(1)(a)). If an individual sets up a record code, it will ensure that registered healthcare provider organisations can only access the individual's My Health Record in specified circumstances. In summary, these are where the organisation has been given the record code by the individual or by the System Operator at the request of the individual. Registered healthcare provider organisations will be able to continue to access the individual's My Health Record where they are already on the access list for the individual's My Health Record prior to the individual setting up a record code. If an individual forgets their record code, they will need to have the System Operator reset it. It is envisaged that an individual will be able to do this by phoning the My Health Record call centre, going to a Medicare shopfront or online using the individual portal;

- allow an individual to prevent registered healthcare provider organisations' clinical information systems automatically checking and indicating if the individual has a My Health Record (paragraph 6(1)(b)). However, even if an individual has chosen to set this advanced access control, a healthcare provider will still be able to manually search the My Health Record system to check if the individual has a My Health Record using the provider's clinical information system; and

- allow an individual to control access to individual records within their My Health Record (paragraph 6(1)(c)).

Subrule 6(2) specifies the ways in which individuals may restrict access to individual records within their My Health Record, and the features and limitations of this aspect of advanced access controls.

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

There are some types of records in relation to which individuals cannot restrict access, being shared health summaries and individual-entered health summaries (paragraph 6(2)(a)).

Paragraph 6(2)(b) specifies circumstances where a record to which access has been restricted will still be accessible, including for nominated representatives and in the case of a serious threat in accordance with rules 7 and 8.

If a registered individual forgets her or his document code, they will need to have the System Operator reset it. It is envisaged that an individual will be able to do this by phoning the My Health Record call centre, going to a Medicare shopfront or online using the individual portal.

Paragraph 6(2)(c) provides that, as a default, records uploaded to an individual's My Health Record will not have a document code applied to them. The System Operator must ensure that registered individuals may change this default setting if they wish so that all records uploaded by specified registered healthcare provider organisations have a document code applied to them. This will further help individuals protect sensitive records.

The System Operator must establish and maintain advanced access controls that permit registered healthcare recipients to be alerted by means of an electronic communication when their My Health Record is accessed by a third party (paragraph 6(1)(d)). This will allow healthcare recipients to be alerted (if they choose) each time their record is accessed to have greater privacy control of their My Health Record.

Notes 1 to 4 to this rule provide information about how these settings will operate in practice, and note 5 directs readers to rule 45 which prohibits healthcare provider organisations from retaining an individual's record code or document code for future use to access the individual's My Health Record or a record in the individual's My Health Record.

DIVISION 3—ACCESS CONTROL MECHANISMS AND SERIOUS THREATS

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

The purpose of Division 3 of Part 2 of the Rules is to ensure that the access control mechanisms established and maintained by the System Operator support access to an individual's My Health Record in such circumstances.

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

Subrule 7(1) requires that access control mechanisms established and maintained by the System Operator enable a registered healthcare provider organisation to assert that it reasonably believes that collection, use or disclosure of information in an individual's My Health Record is necessary to lessen or prevent a serious threat to an individual's life, health or safety, and that it is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure.

Subrule 7(2) provides that, where access is authorised under subsection 64(1) of the Act, the access control mechanisms must allow access regardless of the access controls set by the individual, and must not allow access to any record that has been effectively removed from the individual's My Health Record.

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

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

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

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

Note 3 to rule 7 clarifies that where an individual's My Health Record registration has been suspended, paragraph 54(a) of the Act permits access to the individual'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

Subrule 8(1) requires that access control mechanisms established and maintained by the System Operator enable a registered healthcare provider organisation to assert that it reasonably believes that collection, use or disclosure of information in an individual's My Health Record is necessary to lessen or prevent a serious threat to public health or public safety.

Subrule 8(2) provides that, where access is authorised under subsection 64(2) of the Act, the access control mechanisms must allow access regardless of the access controls set by the individual, and must not allow access to any record that has been effectively removed from the individual's My Health Record.

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

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

DIVISION 4—ACCESS FLAGS

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

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

registered healthcare provider organisations that legitimately need to access an individual's My Health Record in order to provide healthcare are able to do so.

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

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

Access flags must be assigned within a network in a way that balances reasonable individual expectations about the sharing of information as part of providing healthcare to the individual and arrangements within healthcare provider organisations for access to health information (rule 10).

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

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

9. Access control mechanisms must include use of access flags

Rule 9 specifies the requirements for access flags as part of the access control mechanisms established and maintained by the System Operator, including the way in which the access flags are to be set and maintained within a network by its seed organisation.

Paragraph 9(b) provides that access flags are to be set and maintained for a registered healthcare provider organisation in the context of the organisation's network. A network is a group of healthcare provider organisations established and maintained in accordance with subsections 9A(3) to (6) of the HI Act. A network comprises a seed organisation and may include one or more network organisations. A network may consist of healthcare provider organisations that are all part of the same legal entity, or may consist of healthcare provider organisations that are part of two or more separate legal entities. Setting and maintaining access flags within the context of a registered healthcare provider organisation's network ensures that the My Health Record system leverages structures already established under the HI Act.

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

An example of how access flags work is set out under the discussion for rule 10.

Paragraph 9(d) provides that access flags must be set and maintained in accordance with the principles in rule 10.

10. Principles for assigning access flags

Rule 10 specifies the principles for assigning access flags and deals with related matters, including procedures for reassigning access flags where they have not been assigned in a manner that is consistent with the principles.

Subrule 10(1) provides that access flags must be set and maintained in a way which balances:

- reasonable individual expectations about the sharing of information as part of providing healthcare to the individual; and

- arrangements within the organisation for access to health information collected by the organisation.

Under paragraph 10(1)(a), reasonable individual expectations would include:

- ensuring that an individual is able to receive the healthcare that he or she needs while also ensuring that access to his or her My Health Record does not extend beyond the registered healthcare provider organisations reasonably necessary for this to occur; and

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

Paragraph 10(1)(b) is intended to ensure that individual expectations under subparagraph 10(1)(a) are balanced against the arrangements that registered healthcare provider organisations may use to ensure that information is shared appropriately for the safe and efficient treatment of individuals.

Subrule10(2) provides that seed organisations must regularly review the access flags assigned within the network to ensure that they remain consistent with the principles in subrule 10(1).

Subrule 10(3) provides a mechanism to deal with the situation where access flags have not been assigned within a network, have been assigned in a manner that is inconsistent with the principles in subrule 10(1) or have been assigned in a manner that is otherwise inappropriate. If the System Operator reasonably considers that one or more of these kinds of situations exist, paragraph 10(3)(a) requires the System Operator to consult with, and consider the views (if any) of the seed organisation of the network. Following consideration under paragraph 10(3)(a), the System Operator may by written notice request the seed organisation to make reasonable changes to the access flags within the organisation's network, including by adding, omitting or reassigning access flags. As healthcare provider organisations will usually be in a better position than the System Operator to set and maintain access flags, it is envisaged at this stage that the System Operator would generally only give a notice under paragraph 10(3)(a) if other methods did not result in appropriate access flag settings.

Any notice given by the System Operator under paragraph 10(3)(b) must be consistent with the principles in subrule 10(1).

Subrule 10(5) requires that a registered healthcare provider organisation must not unreasonably refuse to comply with a notice given by the System Operator under paragraph 10(3)(b).

The note under subrule 10(5) explains that rule 28 requires seed organisations to structure their networks in a way that permits access flags to be assigned in accordance with the principles in rule 10.

Example 1 – how access flags limit which organisations are added to the access list for an individual's My Health Record

A network made up of a seed organisation and nine network organisations is structured as shown in ***Diagram 1*** below. The seed organisation and each network organisation is a healthcare provider organisation, and each is assigned a healthcare identifier under section 9A of the HI Act. In this example, the seed and network organisations are all part of the same legal entity, and all the healthcare provider organisations in the network are registered under section 44 of the Act. Based on the principles in rule 10, the seed organisation has assigned access flags to itself and to network organisations 3 and 4.

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

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

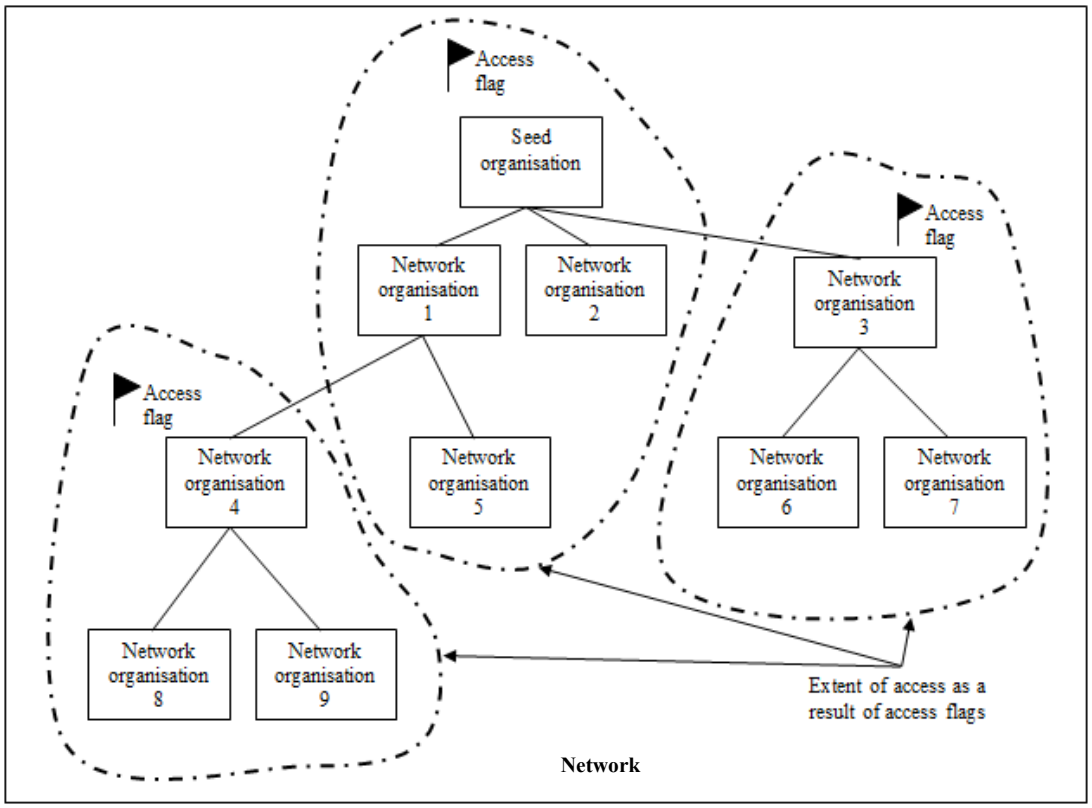

Diagram 1

DIVISION 5—ACCESS CONTROL MECHANISMS RELATING TO SUSPENSION OR CANCELLATION OF ACCESS TO AN INDIVIDUAL'S MY HEALTH RECORD

Division 5 sets out the range of circumstances in which the System Operator can suspend or cancel access to an individual's My Health Record by authorised or nominated representatives. Suspension or cancellation of access to an individual's My Health Record may be necessary for a range of reasons, including to prevent unauthorised access to an individual's My Health Record (where a person is no longer eligible to be a representative) and to protect the security and integrity of the My Health Record system.

Suspension or cancellation of access to an individual's My Health Record by an authorised representative or a nominated representative does not affect the underlying registration of the individual under the Act.

11. Automatic cancellation when individual takes control

Rule 11 deals with circumstances where an individual takes control of their My Health Record or turns 18 years of age. Under subrule 11(1), the System Operator must cancel access to the individual's My Health Record for all authorised representatives and nominated representatives upon the earlier of the individual taking control of her or his My Health Record and the individual reaching the age of 18.

Subrule 11(3) provides an exception to subrule 11(1) and is intended to deal with situations where a young person turning 18 lacks the capacity to manage her or his My Health Record. Under subrule 11(3), the System Operator must not cancel access for an authorised representative if the System Operator is satisfied that the person who is currently the authorised representative will, when the individual reaches the age of 18, be an authorised representative under subsection 6(4) of the Act.

Subrule 11(2) provides that an individual is treated as having taken control of their My Health Record if:

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

The note to this rule refers readers to rule 24 which provides for the verification of an individual's identity when they cease to have an authorised representative.

12. Suspension on death of individual

Rule 12 requires the System Operator to suspend access to an individual's My Health Record for all authorised and nominated representatives of the individual upon receiving advice from the Healthcare Identifiers (HI) Service Operator that the status of the individual's healthcare identifier has been changed to 'deceased'.

The notes to this rule provide information about the healthcare identifier process that occurs when an individual dies. The status of an individual's healthcare identifier is changed to 'deceased' when evidence of the individual's death is provided to the HI Service Operator but the formal advice has not yet been provided by the relevant state or territory authority. Once formal advice is provided, the HI Service Operator will change the status of the individual's healthcare identifier to 'retired' and will notify the System Operator. Upon receipt of notification of 'retired', the System Operator will cancel the registration of the individual under subsection 51(6) of the Act.

13. Suspension and cancellation where representation ceases

Rule 13 requires the System Operator to cancel or suspend access to the individual's My Health Record for an authorised representative or a nominated representative in circumstances where the person is no longer representing the individual.

Paragraph 13(1)(a) provides that the System Operator must cancel access if informed by the HI Service Operator that the status of the healthcare identifier of the authorised representative or nominated representative has been changed to 'retired', meaning that formal advice has been received from the HI Service Operator that the representative has died.

Nominated representatives who are granted read-only access to an individual's My Health Record are not required to provide their healthcare identifier to the System Operator. This means that the HI Service Operator will be unable to notify the System Operator if such a representative dies. Subparagraph 13(1)(a)(ii) therefore provides that the System Operator must cancel a nominated representative's access when the System Operator is otherwise satisfied that the nominated representative has died.

The System Operator must also cancel a representative's access if the System Operator is no longer satisfied that the person is eligible to be a representative of the individual under section 6 or 7 of the Act (paragraph 13(1)(b)), or if notified in writing by the person that she or he no longer wishes to represent the individual for My Health Record purposes (paragraph 13(1)(c)).

While the System Operator investigates whether to cancel access due to the circumstances above, the System Operator may suspend access by the representative (subrule 13(3)).

Subrule 13(2) provides that the System Operator must suspend access to an individual's My Health Record for an authorised representative or a nominated representative if the System Operator has been informed by the HI Service Operator that the status of the representative's healthcare identifier has been changed to 'deceased', meaning that the System Operator has received evidence that the representative has died but has not yet received formal notice of death from the HI Service Operator. Once formal notice of death has been received (that is, the status of the representative's healthcare identifier has been changed to 'retired'), access will be cancelled under subrule 13(1).

If the System Operator suspends or cancels an authorised representative's access to an individual's My Health Record for any of the circumstances described in rule 13, the System Operator must also suspend or cancel access to the individual's My Health Record for all nominated representatives that were nominated by that authorised representative. This means that all other nominated representatives will continue to have access.

The notes to this rule direct readers to subsection 7(3) of the Act which provides that a nominated representative may not be required to have a healthcare identifier. They also make clear that, where a nominated representative's access is cancelled under subrule 13(4), the person's access to the individual's My Health Record as a nominated representative may subsequently be reinstated by any remaining authorised representative.

14. Suspension while investigating eligibility

Rule 14 allows the System Operator to suspend, cancel or restore the access of authorised representatives in circumstances where a question has been raised about the representative's eligibility to continue as an authorised representative.

The System Operator may be informed of a claim by a person that a person is not eligible to act as an authorised representative of an individual. Such a claim must be made in the approved form (subrule 14(2)). The System Operator must investigate the claim and determine whether or not the person remains eligible to be an authorised representative within the meaning of section 6 of the Act (subrule 14(3)). Until a decision is made under subrule 14(3), the System Operator must suspend all representatives' access to the individual's My Health Record (subrule 14(1)) where a claim has been made. Suspending access for representatives would not affect the ability of registered healthcare provider organisations to access the individual's My Health Record in accordance with the access controls put in place by the individual's authorised representative(s) immediately prior to the suspension coming into force.

If, after investigating the matter, the System Operator is no longer satisfied that the person is eligible to be the individual's authorised representative, the System Operator must cancel the person's access to the individual's My Health Record (paragraph 14(3)(a)). However, if after investigating the matter the System Operator is satisfied that the person remains eligible to be the individual's authorised representative, the System Operator must restore access for that person (paragraph 14(3)(b)) and all other representatives (subrule 14(1)).

Subrule 14(4) provides that if the System Operator cancels access to an individual's My Health Record for a person (the ***first person***) under paragraph (3)(a) of rule 14, the System Operator must also cancel access to the individual's My Health Record for the nominated representatives (if any) that were nominated by the first person. This means that all other nominated representatives will continue to have access.

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

Note 2 makes clear that where a nominated representative's access is cancelled under subrule 14(4), the person's access to the individual's My Health Record as a nominated representative may subsequently be reinstated by any remaining authorised representative.

15. Temporary suspension where there is a serious threat

Subrule 15(1) requires the System Operator to suspend all representatives' access to an individual's My Health Record if the System Operator has been notified by the individual's authorised representative that allowing continued representative access to the individual's My Health Record poses or is likely to pose a serious risk to a person's life, health or safety and the System Operator is satisfied that suspending access would reduce this risk. The notification for the purposes of subrule 15(1) would not need to be provided in writing – for example, it may occur by telephone.

Under subrule 15(2), the suspension of access will continue until the earlier of:

- 30 days from the date access was suspended under subrule 15(1); and
- the day on which the System Operator is notified in writing by the authorised representative (who originally made the claim of risk) that there is no longer such a risk.

Note 1 to this rule makes clear that if the System Operator suspends an authorised representative's access to an individual's My Health Record under rule 15, the System Operator still has the ability to suspend the same representative's access under rule 14 if necessary.

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

16. Effect of suspension or cancellation

Rule 16 makes it clear that suspending or cancelling access for an authorised representative or a nominated representative under Division 5 of Part 2 of the Rules has no effect on an individual's registration under the Act or on the access controls that were in place for the individual's My Health Record immediately before any suspension or cancellation of access to the individual's My Health Record occurred.

PART 3—SECURITY, OPERATIONS, ADMINISTRATION AND UPLOADING RECORDS

Part 3 contains provisions regarding the suspension of access to My Health Records for security and other administrative and operational purposes, the uploading of records to the system, and the ability of the System Operator to direct the removal of records from the system, and the handling of records by repositories.

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

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

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

Subrule 17(1) provides that 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.

Subrule 17(2) provides that 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 an individual 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.

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 (subrule 17(3)).

The example clarifies that 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

Subrules 17(4) and (5) provide that if the System Operator suspends access under subrule 17(1) the System Operator must notify the healthcare recipient or other entity in writing 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 entity's access to the My Health Record system is restored.

However, 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 (3) or (4) (subrule 17 (6)). If, in the reasonable opinion of the System Operator, the suspension of access affects a significant number of individuals, the System Operator may notify the general public instead of complying with subrule (3) (subrule 17(7)). This could be done, for example, on a website or via a media release.

Subrule 17(8) provides that 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.

Subrule 17(9) makes clear that any suspension of a healthcare recipient's or other entity's access to the My Health Record system under rule 17 does not affect the healthcare recipient's or entity's registration under the Act. That is, if a healthcare recipient's or other entity's access to the My Health Record is suspended the healthcare recipient or entity remains registered and subject to obligations and requirements under the Act. Suspension of access also does not affect the access control mechanisms that were in place for an individual'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

At times the My Health Record system may become unavailable. Rule 18 provides that 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

Subparagraph 45(b)(ii) of the Act provides that the My Health Records Rules may specify records that must be prepared by an individual healthcare provider who has been assigned a healthcare identifier for that record to be authorised to be uploaded. This ensures transparency and accountability in relation to records that have been uploaded to an individual's My Health Record by registered healthcare provider organisations.

The effect of rule 19 is that all records, other than shared health summaries, that are uploaded by registered healthcare provider organisations to the My Health Record system must be prepared by an individual healthcare provider to whom a healthcare identifier has been assigned under paragraph 9(1)(a) of the HI Act. In summary, this means that shared health summaries are not required to have been prepared by an individual healthcare provider.

All other records will need to be prepared by an individual healthcare provider who has a healthcare identifier under the HI Act, before they can be uploaded to the system.

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

Paragraph 45(ba) of the Act requires authors of records to also be an identified healthcare provider whose registration or membership as applicable is not conditional, suspended, cancelled or lapsed, other than in circumstances prescribed in My Health Records Rules. This ensures that at the time a healthcare provider authors a document that is uploaded to the My Health Record system, they are qualified and permitted to do so. However not all instances of a healthcare provider's registration or membership being conditional, suspended, cancelled or lapsed, pose a clinical risk and it may still be appropriate in certain circumstances for the provider to author records that are uploaded to the My Health Record system.

Rule 20 provides that, 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

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

Rule 21 provides that the System Operator may effectively remove, or may direct a participant in the My Health Record system to effectively remove, a record where the System Operator reasonably considers that the record contains a defamatory statement or affects, or is likely to affect, the security or integrity of the My Health Record system.

Where a participant in the My Health Record system – for example, a registered repository operator or a registered healthcare provider organisation – is given a direction by the System Operator under subrule 21(1), the participant must comply with the direction (subrule 21(2)).

If a record is effectively removed under this rule, the System Operator must notify in writing the entity that uploaded the record and explain the reason for the effective removal. The System Operator must also notify in writing the individual to whom the My Health Record relates (paragraph 21(3)(a)). The entity that uploaded the record may upload a replacement record, provided that at the time of uploading the replacement record the entity is a participant in the My Health Record system and the replacement addresses the System Operator's concerns in the notice given under paragraph 21(3)(a) (paragraph 21(3)(b)).

Subrule 21(4) makes clear that this rule does not by implication affect the System Operator's functions or powers under the Act to manage the My Health Record system.

22. Transfer and disposal of records

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

If the registration of a registered repository operator or registered portal operator is cancelled, rule 22 specifies that 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.

PART 4—IDENTITY VERIFICATION

Part 4 contains provision regarding the verification of an individual's identity.

23. Requirement for verified healthcare identifier

Subsection 41(1) of the Act provides that the System Operator must register an individual if, among other things, the System Operator is satisfied that the identity of the individual has been appropriately verified having regard to any matters (if any) specified in the My Health Records Rules. Paragraphs 3(1)(b) and 6(3)(c) of Schedule 1 to the Act provide a similar rule making power for the opt-out model.

Rule 23 provides that, as a minimum requirement in relation to identity verification, the System Operator must be satisfied that the individual has a verified individual healthcare identifier.

Rule 4 defines a 'verified healthcare identifier' to mean a healthcare identifier in relation to which the HI Service Operator has evidence, to the HI Service Operator's satisfaction, of the individual's identity.

Subrule 23(2) makes clear that the System Operator may also have regard to other matters when satisfying itself that the identity of an individual has been appropriately verified.

24. Identity verification on ceasing to have an authorised representative

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

Rule 24 requires that, if an individual ceases to have an authorised representative, the System Operator must require the individual to verify her or his identity before the individual is able to take control of their My Health Record.

This rule is necessary, for example, where a parent has registered their child for a My Health Record and the child subsequently reaches the age of 18 and is capable of making her or his own decisions. As part of the registration process, the parent will have provided certain information relating to their identity and the identity of the child. When the child reaches the age of 18, their parent will no longer control access to their My Health Record and it will be necessary for the young person to verify their identity with the System Operator. Rule 24 works in conjunction with subrule 11(2) which specifies when an individual 'takes control' of her or his My Health Record.

Subrule 24(2) provides that an individual is not required to verify their identity if they have previously done so. This requirement addresses situations where an individual may have previously verified their own identity before losing capacity and being represented by an authorised representative but then later regains capacity. For example, an individual has previously verified her or his identity with the System Operator but then suffers acute mental illness and is incapable of managing her or his My Health Record and needs an authorised representative. If the individual subsequently ceases to have an authorised representative because they have regained capacity, the individual would not need to verify his or her identity again with the System Operator.

Subrule 24(3) makes clear that the System Operator may have regard to any relevant matter when satisfying itself that the identity of an individual has been appropriately verified.

PART 5—PARTICIPATION REQUIREMENTS FOR HEALTHCARE PROVIDER ORGANISATIONS AND CONTRACTED SERVICE PROVIDERS

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

Section 48 of the Act sets out the eligibility criteria for repository operators, portal operators and contracted service providers to register to participate in the My Health Record system. Among the criteria, paragraph 43(a) requires that the repository operator, portal operator or contracted service provider comply with any requirements specified in the My Health Records Rules.

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

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

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

DIVISION 1—GENERAL REQUIREMENTS OF HEALTHCARE PROVIDER ORGANISATIONS

Division 1 of Part 5 of the Rules prescribes requirements with which healthcare provider organisations must comply in order to be, and remain, eligible for registration.

End point security is critical to ensuring that the My Health Record system remains secure and that individual's health information is adequately protected. Division 1 of Part 5 of the Rules ensures that healthcare provider organisations participating in the My Health Record system meet specified minimum standards in terms of the security measures they take in relation to their staff and their information technology systems. Failure to comply with these requirements may compromise the integrity or security of the My Health Record system, and may result in suspension or cancellation of a healthcare provider organisation's registration or the imposition of other sanctions under the Act.

Under the *PCEHR (Participation Agreements) Rules 2012* all healthcare provider organisations were parties to a participation agreement with the System Operator when they registered to participate in the My Health Record system.

Participation agreements contained a number of requirements that healthcare provider organisations are obligated to comply with in order to be and remain registered. As part of measures to reduce the regulatory burden on healthcare provider organisations, the registration process will be simplified and the need to enter into participation agreements will be removed. Where appropriate, obligations that were contained in participation agreements have been moved from the participation agreement to the Rules. It is intended that the *PCEHR (Participation Agreements) Rules 2012* will be repealed in the future.

25. Requirements for registration

Rule 25 specifies that, in order for a healthcare provider organisation to be eligible to be registered, and to remain registered, it must comply with the requirements of Division 1 of Part 5 of the Rules.

26. Authority to act on behalf of healthcare provider organisation

Rule 26 requires that, in order to be eligible to register, a healthcare provider organisation must ensure that certain people are authorised to act on its behalf in its dealings with the System Operator. This is necessary so that the System Operator is able to verify the identity of the people with whom it is dealing. It will be the responsibility of the healthcare provider organisation to ensure that the necessary authorities have been put in place so that the organisation can comply with this rule.

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

- if the organisation is a seed organisation, or is not part of a network – the organisation's responsible officer and organisation maintenance officer; and

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

27. Requirements to participate

Subrule 27(1) states that 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.

Paragraphs 27(2)(a) and (b) require that, in order for a healthcare provider organisation to be eligible to register under the My Health Record Act, any organisations superior to that organisation (including the seed organisation) within the network must also be registered. In essence, this means that a network organisation cannot register unless there is an unbroken chain of registered healthcare organisations between it and the seed organisation within its network.

Paragraphs 27(2)(c) ensures that the HI Service Operator is provided with the information necessary to maintain a record of the linkages of organisations within each network.

28. Registration of network organisations

Rule 28 requires that, in order for a seed organisation to be eligible to register, it must ensure its network is structured in a manner that permits the assignment of access flags in accordance with rules 9 and 10. This rule is intended to prevent healthcare provider organisations structuring themselves in a way that undermines the purpose behind access flags.

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

As the My Health Record system contains sensitive health information that will be used to direct and assist future healthcare of an individual, care must be exercised when uploading or downloading documents.

Subrule 29(1) provides that a healthcare provider organisation must take reasonable steps to ensure that they and their employees exercise due care and skill 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 (paragraph (1)(a)). Further, they must exercise due and care and skill 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 (paragraph (1)(b)).

Subrule 29(2) creates an exception to paragraph (1)(a) – that is, paragraph 29(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.

Subrule 29(3) clarifies that 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 keep clinical records about an individual or to communicate health information to an individual.

30. Requirement to notify the System Operator of certain things

For the System Operator to maintain the security and operability of the My Health Record system, it relies on participants to advise it of certain things. Rule 30 provides that 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;

the healthcare provider organisation must:

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

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

31. Requirement to maintain interoperability

Rule 31 provides that a healthcare provider organisation must maintain interoperability with the My Health Record system in accordance with the System Operator's interoperability requirements. A similar obligation applies to other participants in the My Health Record System. Interoperability requirements is defined as meaning 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.

The materials likely to be specified as interoperability requirements are IT and security-related documents, such as the *National eHealth Security and Access Framework*. These requirements are typically technical in nature and complex, detailing IT-related security measures. The requirements may quickly and at relatively short notice change to address emerging IT and security threats. It is important to be able to deal with rapidly changing IT security threats in a responsive manner that also allows requirements to be enforced. If this does not occur, the security risks to the My Health Record system will increase given the large number of interconnecting healthcare provider organisations (currently more than 7,000 and expected to increase substantially with the trial of opt-out arrangements). A failure by healthcare provider organisations to comply with IT security requirements may put individuals' health information at increased risk.

32. Requirement to provide assistance

Rule 32 provides that 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. However, this rule 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

Division 2 of Part 5 of the Rules prescribes requirements with which contracted service providers must comply, including security requirements, in order to be, and remain, eligible for registration.

Like healthcare provider organisations, under the *PCEHR (Participation Agreements) Rules 2012* contracted service providers were required to be a party to a participation agreement with the System Operator to participate in the My Health Record system. Participation agreements contain a number of requirements. As part of measures to reduce the regulatory burden on participants, the registration process will be simplified and the need to enter into participation agreements will be removed. Where appropriate, some of the requirements under that were in participation agreements have been moved to the Rules. It is proposed that the *PCEHR (Participation Agreements) Rules 2012* will be repealed at a future date.

33. Requirements for registration

Section 48 of the Act sets out eligibility criteria for contracted service providers to register to participate in the My Health record system. Among the criteria, paragraph 48(a) requires that the contracted service provider complies with any requirements set out in the My Heath Records Rule.

Rule 33 specifies that in order for a contracted service provider to be eligible to be registered, and to remain registered, it must comply with the requirements under Division 2 of Part 5 of the Rules.

34. Link to a healthcare provider organisation

Subrule 34(1) provides that a contracted service provider must be linked to one or more registered healthcare provider organisations. 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 (subrule 34(4)).

Subrule 34(2) provides that 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

(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.

A contracted service provider will no longer be linked to a registered healthcare provider organisation if the contracted service provider's contract with the healthcare provider

organisation expires or is terminated or the registered healthcare provider organisation notifies the System Operator that the link between itself and the contracted service provider is no longer current (subrule 34(3)).

35. Registration with service operator

Rule 35 provides that a contracted service provider must register with the HI Service Operator as a contracted service provider.

36. Appointment of contracted service provider officer

To ensure the System Operator has a point of contact with the contracted service provider, subrule 36(1) provides that a contracted service provider must appoint a contracted service provider officer who is employed by the contracted service provider. There must be at least one, but no more than three, contracted service provider officers for a contracted service provider at all times (subrule 36(2)).

Subrules 36(3) and (4) provide that a contracted service provider must ensure that its appointed contracted service provider officer carries out the following duties:

(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

Rule 37 provides that 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. This provides security for the system and is a privacy positive aspect for individuals.

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 (subrule 37(2)).

38. Requirement to notify the System Operator of certain things

For the System Operator to maintain the security and operability of the My Health Record system, it relies on participants to advise it of certain things. Rule 38 provides that 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, defined in rule 4;

(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,

the 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

Rule 39 provides that a contracted service provider must maintain interoperability with the My Health Record system in accordance with the System Operator's interoperability requirements. Interoperability requirements is defined as meaning 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.

The materials likely to be specified as interoperability requirements are IT and security-related documents, such as the *National eHealth Security and Access Framework*. These requirements are typically technical in nature and complex, detailing IT-related security measures. The requirements may quickly and at relatively short notice change to address emerging IT and security threats. It is important to be able to deal with rapidly changing IT and security threats in a responsive manner that also allows requirements to be enforced. If this does not occur, the security risks to the My Health Record system will increase given the large number of interconnecting healthcare provider organisations (currently more than 7,000 and expected to increase substantially with the trial of opt-out arrangements). A failure by contracted service providers to comply with IT security requirements may put individuals' health information at increased risk.

40. Requirement to provide assistance

Rule 40 provides that 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. However, this rule 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

Division 3 of Part 5 of the Rules prescribes security requirements with which healthcare provider organisations must comply in order to be, and remain, eligible for registration.

41. Requirements for registration

Rule 41 specifies that, in order for a healthcare provider organisation to be eligible to be registered, and to remain registered, it must comply with the requirements of Division 3 of Part 5 of the Rules.

42. Healthcare provider organisation policies

Subrule 42(1) requires that, in order to be eligible to register, healthcare provider organisations must have in place a written policy that reasonably addresses the matters specified in subrule 42(4). In summary, those matters are:

- the manner of authorising persons within the organisation to access the My Health Record system, including the manner of suspending and deactivating the user account of any authorised person (paragraph 42(4)(a));

- 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 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 (paragraph 42(4)(b));

- the process for identifying a person who requests access to an individual's My Health Record and providing identification information to the System Operator, ensuring the organisation is able to satisfy its obligations under section 74 of the Act (paragraph 42(4)(c));

- the physical and information security measures of the healthcare provider organisation, including the procedures for user account management required under rule 44 (paragraph 42(4)(d)); and

- mitigation strategies to ensure My Health Record-related security risks can be identified, acted upon and reported expeditiously (paragraph 42(4)(e)).

If the healthcare provider organisation reasonably considers that it is not necessary for its policy to address certain matters otherwise required by subrule 42(4), on the basis of the organisation's limited size, the organisation's policy need not address those matters (subrule 42(5)). Subrule 42(5) is intended to exempt sole practitioners and very small healthcare provider organisations from having to address all the matters required by subrule 42(4) in their policy required under subrule 42(1) – for example, because there are no other staff that need training.

Subrule 42(6) contains a number of administrative and procedural requirements in relation to policies required under subrule 42(1), including in summary that policies are:

- written in a manner that enables the organisation's performance to be audited against the policy (subparagraph 42(6)(a)(i));

- kept current (subparagraph 42(6)(a)(ii));

- uniquely identifiable by version (paragraph 42(6)(b)) and each version of an organisation's policy must be retained in accordance with any applicable record keeping obligations (paragraph 42(6)(d)); and

- reviewed no less than once a year for the identification of new risks, and that the review include consideration of anything that may result in unauthorised access, misuse or unauthorised disclosure of information or accidental disclosure of information, and of any changes to the My Health Record system or relevant laws since the last review (paragraph 42(6)(c)).

Subrule 42(2) provides that healthcare provider organisations must ensure their policy is communicated, and remains accessible, to all its employees and any healthcare providers to whom the organisation supplies services under contract. Healthcare provider organisations must enforce their policy (subrule 42(3)).

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

Rule 43 requires that, if the System Operator requests in writing that a healthcare provider organisation provide a copy of its policy made in accordance with rule 42 to the System Operator, the organisation must comply within seven days.

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

44. User account management within healthcare provider organisations

Rule 44 requires that the information technology systems of healthcare provider organisations, used for the purpose of accessing the My Health Record system, employ reasonable information security access management practices, including in summary:

- ensuring that only those people who require access as part of their duties are authorised to access the system (paragraph 44(a));

- uniquely identifying individuals using the healthcare provider's information technology systems and protecting that unique identity using a password or equivalent protection measure (paragraph 44(b));

- following robust and secure password and/or access management practices (paragraph 44(c));

- ensuring user accounts for persons no longer authorised to access the My Health Record system prevent access (paragraph 44(d)); and

- suspending a user account which allows 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 (paragraph 44(e)).

45. Retention of record codes and document codes

Rule 45 requires healthcare provider organisations to 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 future use to access the individual's My Health Record or records in the individual's My Health Record.

This ensures that an individual's ability to control access to her or his My Health Record is not undermined by healthcare provider organisations retaining these codes or sharing them with other organisations.

The note explains that, in practice, when a healthcare provider organisation is given a record code or document code in order to access the individual's My Health Record or a record in the My Health Record individual's, the organisation will only need to enter this code once. The My Health Record system will then record that the organisation has been added to individual's access list, or has access to records to which access would otherwise be restricted. The healthcare provider organisation will retain access to the individual's My Health Record or to the relevant record in the individual's My Health Record until the access control mechanisms for the My Health Record or record are changed, e.g. by the individual setting up a new record code.

DIVISION 4—SECURITY REQUIREMENTS FOR CONTRACTED SERVICE PROVIDERS

Division 4 of Part 5 of the Rules prescribes security requirements with which contracted service providers must comply in order to be, and remain, eligible for registration.

46. Requirements for registration

Section 48 of the Act sets out eligibility criteria for contracted service providers to register to participate in the My Health record system. Among the criteria, paragraph 48(a) requires that the contracted service provider complies with any requirements set out in the My Heath Records Rules.

Rule 46 specifies that in order for a contracted service provider to be eligible to be registered, and to remain registered, it must comply with the requirements under Division 4 of Part 5 of the Rules.

47. Contracted service provider policies

Subrule 47(1) provides that it is a requirement of registration that contracted service providers must have a written policy that reasonably addresses the matters specified in subrule 47(4). In summary, those matters are:

(a) the manner of authorising persons accessing the My Health Record system, including the manner of suspending and deactivating the user account of any authorised person (paragraph 47(4)(a)):

  (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(paragraph 47(4)(b));

(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 (paragraph 47(4)(c)); 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 (paragraph 47(4)(d)).

Contracted service providers must communicate the policy and ensure that the policy remains readily accessible, to all its employees (subrule 47(2)). Contracted service providers must enforce the policy in relation to all its employees (subrule 47(3)).

If the contracted service provider reasonably considers that it is not necessary for its policy to address certain matters otherwise required by subrule 47(4), on the basis of the provider's limited size, the provider's policy need not address those matters (subrule 47(5)). Subrule 47(5) is intended to exempt sole practitioners and very small contracted service providers from having to address all the matters required by subrule 47(4) in their policy required under subrule 47(1) – for example, because there are no other staff that need training.

Subrule 47(6) contains a number of administrative and procedural requirements in relation to policies required under subrule 47(1), including in summary that policies are:

- written in a manner that enables the provider's performance to be audited against the policy (subparagraph 47(6)(a)(i));

- kept current (subparagraph 47(6)(a)(ii));

- uniquely identifiable by version (paragraph 47(6)(b)) and each version of a provider's policy must be retained in accordance with any applicable record keeping obligations (paragraph 47(6)(d)); and

- reviewed no less than once a year for the identification of new risks, and that the review include consideration of anything that may result in unauthorised access, misuse or unauthorised disclosure of information or accidental disclosure of information, and of any changes to the My Health Record system or relevant laws since the last review (paragraph 47(6)(c)).

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

Rule 48 requires that, if the System Operator requests in writing that a contracted service provider give a copy of its policy made in accordance with rule 47 to the System Operator, the provider must comply within seven days.

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

49. User account management within contracted service providers

Rule 49 requires that the information technology systems of contracted service providers, used for the purpose of accessing the My Health Record system, employ reasonable information security access management practices, including in summary:

- ensuring that only those people who require access as part of their duties are authorised to access the system (paragraph 49(a));

- uniquely identifying individuals using the contracted service provider's information technology systems and protecting that unique identity using a password or equivalent protection measure (paragraph 49(b));

- following robust and secure password and/or access management practices (paragraph 49(c));

- ensuring user accounts for persons no longer authorised to access the My Health Record system prevent access (paragraph 49(d)); and

- suspending a user account which allows 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 (paragraph 49(e)).

50. Retention of record codes and document codes

Rule 50 requires contracted service provider's to 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 future use to access the healthcare recipient's My Health Record or records in the healthcare recipient's My Health Record.

This ensures that a healthcare recipient's ability to control access to her or his My Health Record is not undermined by contracted service provider's retaining these codes or sharing them with other participants.

PART 6—PARTICIPATION REQUIREMENTS FOR OPERATORS

Part 6 prescribes requirements with which repository operators and portal operators must comply in order to be, and remain, eligible for registration.

DIVISION 1—GENERAL REQUIREMENTS

51. Application of this Division

This Division applies to an operator which is defined as a repository operator or a portal operator.

Like healthcare provider organisations and contracted service providers, under the *PCEHR (Participation Agreements) Rules 2012* repository operators were required to be a party to a participation agreement with the System Operator to participate in the My Health Record system.

Participation agreements contained numerous registration requirements that the registered repository operator was obligated to comply with. As part of measures to reduce the regulatory burden on participants, the registration process will be simplified and the need to enter into participation agreements will be removed. Where appropriate, participation requirements have been moved from the participation agreement to the Rules. It is proposed that the *PCEHR (Participation Agreements) Rules 2012* will be repealed in the future.

52. Requirements for registration

Section 48 of the Act sets out eligibility criteria for operators to register to participate in the My Health Record system. Among the criteria, paragraph 48(a) requires that operators comply with any requirements set out in the My Heath Records Rules.

Rule 52 specifies that in order for an operator to be eligible to be registered, and to remain registered, it must comply with the requirements under Division 1 of Part 6 of the Rules.

53. Appointment of operator officer

To ensure the System Operator has a point of contact with the operators, subrule 53(1) provides that an operator must appoint an operator officer, who is employed by the operator. There must be at least one, but no more than three, operator officers for an operator at all times (subrule 53(2)).

Subrules 53(3) and (4) provide that an operator must ensure that its appointed operator officer carries out the following duties:

(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 about the professional and business details of the operator and the operator officer.

54. Operator technical and after-hours contacts

Paragraph 54(a) provides that an operator must provide a point of contact and technical support for the operator during ordinary business hours Monday to Friday, other than public holidays. Further, under paragraph 54(b) the operator must 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. Requirements to notify the System Operator of certain things

For the System Operator to maintain the security and operability of the My Health Record system, it relies on participants to advise it of certain things. Rule 55 provides that if an operator:

(a) becomes aware, or suspects, that:

  (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, as defined in rule 4;

(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,

the 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

Rule 56 provides that an operator must maintain interoperability with the My Health Record system in accordance with the System Operator's interoperability requirements. Interoperability requirements are defined as meaning 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.

The materials likely to be specified as interoperability requirements are IT and security-related documents, such as the *National eHealth Security and Access Framework*. These requirements are typically technical in nature and complex, detailing IT-related security measures. The requirements may quickly and at relatively short notice change to address emerging IT and security threats. It is important to be able to deal with rapidly changing IT and security threats in a responsive manner that also allows requirements to be enforced. A failure by operators to comply with IT security requirements may put individuals' health information at increased risk.

57. Requirement to provide assistance

Rule 57 provides that 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. However, this rule 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

Section 48 of the Act sets out eligibility criteria for operators to register to participate in the My Health Record system. Among the criteria, paragraph 48(a) requires that operators comply with any requirements set out in the My Heath Records Rules.

Rule 58 specifies that in order for an operator to be eligible to be registered, and to remain registered, it must comply with the requirements under Division 2 of Part 6 of the Rules.

59. Operator policies

Subrule 59(1) requires that it is a requirement of registration that operators must have a written policy that reasonably addresses the matters specified in subrule 59(4). In summary those matters are:

(a) the manner of authorising persons accessing the My Health Record system, including the manner of suspending and deactivating the user account of any authorised person (paragraph 59(4)(a));

  (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(paragraph 59(4)(b));

(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 (paragraph 59(4)(c)); 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 (paragraph 59(4)(d)).

Operators must communicate the policy and ensure that the policy remains readily accessible, to all its employees (subrule 59(2)). Operators must enforce the policy in relation to all its employees (subrule 59(3)).

If the operator reasonably considers that it is not necessary for its policy to address certain matters otherwise required by subrule 59(4), on the basis of the operator's limited size, the operator's policy need not address those matters (subrule 59 (5)). Subrule 59(5) is intended to exempt very small operators from having to address all the matters required by subrule 59(4) in their policy required under subrule 59(1) – for example, because there are no other staff that need training.

Subrule 59(6) contains a number of administrative and procedural requirements in relation to policies required under subrule 59(1), including in summary that policies are:

- written in a manner that enables the operator's performance to be audited against the policy (sub-paragraph 59(6)(a)(i));

- kept current (sub-paragraph 59(6)(a)(ii));

- uniquely identifiable by version (paragraph 59(6)(b)) and each version of an operator's policy must be retained in accordance with any applicable record keeping obligations (paragraph 59(6)(d)); and

- reviewed no less than once a year for the identification of new risks, and that the review include consideration of anything that may result in unauthorised access, misuse or unauthorised disclosure of information or accidental disclosure of information, and of any changes to the My Health Record system or relevant laws since the last review (paragraph 59(6)(c)).

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

Rule 60 requires that, if the System Operator requests in writing that an operator give a copy of its policy made in accordance with rule 59 to the System Operator, the operator must comply within seven days.

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

61. User account management within operators

Rule 61 requires that the information technology systems of operators used for the purpose of accessing the My Health Record system, employ reasonable information security access management practices, including in summary:

- ensuring that only those people who require access as part of their duties are authorised to access the system (paragraph 61(a));
- uniquely identifying individuals using the operator's information technology systems and protecting that unique identity using a password or equivalent protection measure (paragraph 61(b));
- following robust and secure password and/or access management practices (paragraph 61(c));
- ensuring user accounts for persons no longer authorised to access the My Health Record system prevent access (paragraph 61(d)); and
- suspending a user account which allows 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 (paragraph 61(e)).

DIVISION 3—SECURITY REQUIREMENTS FOR PORTAL OPERATORS

62. Requirements for registration

Section 48 of the Act sets out eligibility criteria for portal operators to register to participate in the My Health Record system. Among the criteria, paragraph 48(a) requires that portal operators comply with any requirements set out in the My Heath Records Rules.

Rule 62 specifies that in order for a portal operator to be eligible to be registered, and to remain registered, it must comply with the requirements under Division 3 of Part 6 of the Rules.

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

Rule 63 requires portal operator's to 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 future use to access the healthcare recipient's My Health Record or records in the healthcare recipient's My Health Record.

This ensures that a healthcare recipient's ability to control access to her or his My Health Record is not undermined by portal operator's retaining these codes or sharing them with other participants.

SCHEDULE 1 – APPLICATION PROVISIONS

Some of the rules have been based on clauses from the participation agreements between participants in the My Health Record system and the Commonwealth, which will no longer be necessary. However the requirement to enter into these agreements will continue until "application day" as defined in Schedule 1 to the *Health Legislation Amendment (eHealth) Act 2015*. To avoid any confusion with inconsistencies between the Rules and the participation agreements, the relevant provisions in the Rules will apply on or after application day.

Schedule 1 to the Rules describes how the relevant rules that have been based on participation agreements would operate and have effect.

Clause 1

Clause 1 of the Schedule defines terms used in the Schedule being "amending Act" (which means the *Health Legislation Amendment (eHealth) Act 2015*) and "the Rule" (which means the *My Health Records Rule 2016*.).

Clause 2

Clause 2 of the Schedule provides that the repeal of the *PCEHR (Participation Agreements) Rules 2012* will apply on and after the application day as defined in item 111 of Schedule 1 to the amending Act.

Clauses 3-7

Clauses 3 to 7 provide that the following provisions of the Rules will apply on or after the application day as defined in item 111 of Schedule 1 to the amending Act:

- paragraph 17 (2)(c) and subrule 17(3);
- rule 20;
- paragraph 21(1)(c);
- rules 29, 30, 31 and 32;
- Divisions 2 and 4 of Part 5; and
- Part 6.

Statement of Compatibility with Human Rights

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

My Health Records Rules 2016

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

Overview of the Legislative Instrument

The Legislative Instrument is part of a suite of My Health Records Rules made by the Minister, including the *My Health Records (Assisted Registration) Rule 2015*, to support the operation of the My Health Record system.

The Legislative Instrument, in summary, prescribes rules that relate to:

- access control mechanisms;
- the security, integrity and operation of the My Health Record system;
- the handling of specified types of records;
- identity verification; and
- participation requirements for healthcare provider organisations, contracted service providers, repository operators and portal operators to be eligible to register and remain registered in the My Health Record system.

Human rights implications

The Legislative Instrument engages the following human rights:

Right to protection of privacy and reputation

Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) prohibits the unlawful or arbitrary interference with a person's privacy and unlawful attacks on a person's reputation. This right is also reflected in Article 22 of the *Convention on the Rights of Persons with Disabilities* (CRPD) and Article 16 of the *Convention on the Rights of the Child* (CRC). The right to privacy includes respect for informational privacy including the right to respect the storing, use and sharing of private information and right to control the dissemination of private information.

The Legislative Instrument promotes the right to protection of privacy and is designed to ensure that the My Health Record system is secure and that the privacy of healthcare recipients and others involved in the system are protected.

Due to the sensitive nature of health information that is collected, used and disclosed in the My Health Record system, the right to protection of a healthcare recipient's information is vital. The Instrument does this by, amongst other things, specifying requirements for access control mechanisms to enable healthcare recipients to control access to the My Health Records and to records within their My Health Record. The Instrument also includes requirements for access flags which are designed to limit access to a healthcare recipient's My Health Record.

The Instrument outlines situations where access to the My Health Record system or a healthcare recipient's My Health Record is to be suspended or cancelled. The ability to suspend or cancel access if there is a risk to the security, integrity or operations of the system, is a privacy positive outcome that ensures that the My Health Record system protects the privacy of participants. The Instrument also specifies situations where a person's identity must be verified ensuring that the correct people are accessing sensitive information and includes participation requirements to ensure that healthcare provider organisations, contracted service providers, repository operators and portal operators meet specified standards, including in relation to information security, if they wish to participate in the My Health Record system.

Conclusion

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

The Hon Sussan Ley, MP

Minister for Health