*Aboriginal Community Controlled Health Services*

ACCHS policy on the My Health Record system security and access

*3rd December 2015*

*[INSERT LOGO]*

*[INSERT POLICY NUMBER] ACCHS policy on the My Health Record System Security and Access Policy*

1. **PURPOSE**

1. To outline the roles and responsibilities of the Responsible Officer, Organisation Maintenance Officer and health care providers in relation to Health Care Identifiers and the My Health Record system.

2. To provide guidance for staff and contractors about access to, and use of, the My Health Record system.

3. To provide guidance in the use of information technology in [INSERT ACCHS NAME] as it relates to the My Health Record system.

1. **SCOPE OF POLICY**

This policy applies to all staff of [INSERT ACCHS NAME] (including its employees and any healthcare provider to whom the organisation supplies services under contract) with access to My Health Record system.

1. **RESPONSIBILITY FOR IMPLEMENTATION AND COMPLIANCE MONITORING**

The following roles are responsible for implementation and compliance monitoring of this My Health Record system security and access policy:

* Responsible Officer (RO): The RO has legal responsibility for understanding and compliance with this policy and compliance with the My Health Record legislation.
* Organisation Maintenance Officer (OMO): The OMO is responsible for understanding, implementation and compliance monitoring of the My Health Record system security and access policy, and for maintenance of the policy on behalf of [INSERT ACCHS NAME].

1. **RELATED DOCUMENTS/LINKS**

This policy is to be read in conjunction with the following documents:

* *My Health Records Rules 2012*
* *My Health Records Act 2012*
* *My Health Records Regulation 2012*
* [*RACGP Computer and Information Security Standards*](http://www.racgp.org.au/Content/NavigationMenu/ClinicalResources/ehealth/ciss/2011ComputerInformationSecurityStandards.pdf)
* [*Healthcare Identifiers Act 2010*](http://www.comlaw.gov.au/Details/C2012C00590)

1. **DEFINITIONS**

* ***Access control mechanisms*** include default access controls and advanced access controls.
* ***Access flag*** means an information technology mechanism made available by the System Operator to define access to a consumer’s My Health Record.
* ***Act*** means the *My Health Record Act 2012*.
* ***Advanced access controls*** means the access controls that enable a registered consumer to set controls on the registered healthcare provider organisations and nominated representatives who may access the consumer’s My Health Record, and the records within the My Health Record system.
* ***Consumer-entered health summary*** means the summary of information, including medications and allergies, that a registered consumer may enter into his or her My Health Record and which is available to anyone with access to the consumer’s My Health Record.
* ***Default access controls*** means the access controls that apply where a registered consumer has not set controls on the registered healthcare provider organisations or nominated representatives who may access the consumer’s My Health Record.
* ***Document code*** means a code that may be used to restrict access to individual records within a consumer’s My Health Record.
* ***Effectively remove***, in relation to a record in a consumer’s My Health Record, means rendering the record inaccessible to the consumer, their nominated representatives and any registered healthcare provider organisations involved in the care of the consumer, including in the case of a serious threat in accordance with rules 6 and 7.
* ***Healthcare identifier*** has the same meaning as in section 9 of the *Healthcare Identifiers Act 2010*.
* ***Identified healthcare provider*** has the same meaning as in the *Healthcare Identifiers Act 2010*.
* ***System Operator*** is the Australian Commission for eHealth
* ***Network hierarchy*** means a network of healthcare provider organisations created and managed in accordance with subsections 9A(3) to (7) of the *Healthcare Identifiers Act 2010*.
* ***Network organisation*** has the same meaning as in the *Healthcare Identifiers Act 2010*.
* ***Organisation maintenance officer*** has the same meaning as in the *Healthcare Identifiers Act 2010*.
* ***Provider portal*** means the portal provided by the System Operator that permits registered healthcare provider organisations to access the My Health Record system without having to use a clinical information system.
* ***Record code*** means acode that may be used to restrict access to a consumer’s My Health Record.
* ***Responsible officer*** has the same meaning as in the *Healthcare Identifiers Act 2010*.
* ***Restore***, in relation to a record, means making a record, which has previously been effectively removed, accessible to the consumer, their nominated representatives and any registered healthcare provider organisations involved in the care of the consumer in accordance with any applicable access control mechanisms, including in the case of a serious threat to an individual’s life, health or safety.
* ***Seed organisation*** has the same meaning as in the *Healthcare Identifiers Act 2010*.
* ***Seed OMO:*** Organisation Maintenance Officer in seed organisation. Has primary responsibility for OMO roles and coordination of OMO activities in network organisations.
* ***Service operator*** has same meaning as in the*Healthcare Identifiers Act 2010*.
* ***Verified healthcare identifier*** means a healthcare identifier assigned to a consumer in relation to which the service operator has evidence, to the service operator’s satisfaction, of the consumer’s identity.

1. **POLICY**

**AUTHORITY TO ACT**

The RO and OMO for this seed organisation are authorised to act on its behalf in dealing with the System Operator. Where there is a network hierarchy, the RO and OMO from the seed organisation and the OMO from the network organisation in the network hierarchy are authorised to act on behalf of the organisation in dealing with the System Operator.

**RISK ASSESSMENT**

[INSERT ACCHS NAME] will undertake a risk assessment into [INSERT ACCHS NAME] ICT systems that examines privacy and security risks associated with My Health Record system access. [INSERT ACCHS NAME] will undertake an annual risk assessment.

**ACCESS FLAGS**

Where appropriate to the size and complexity of the Aboriginal Community Controlled Health Service the RO/OMO will define an appropriate network hierarchy for the organisation and assign access flags appropriately for the structure of the organisation. The network hierarchy will define the seed organisation, the network organisations that fall under that seed organisation, and the network organisations for whom access flags are appropriate.

In setting and maintaining access flags, the RO/Seed OMO will ensure that:

* Consumers are able to determine and control access to their My Health Record in a way that meets reasonable public expectations. Network organisations that would not be expected by consumers to be connected will thus have their own access flags.
* The organisation is able to share health information internally in an appropriate manner.

The RO/OMO will undertake reviews of the network structure and access flag assignments at such times as the structure changes, or in the case that a System Operator or consumer query reveals potential structural issues. The organisation commits to making reasonable changes in line with requests from the System Operator.

**MAINTAINING RECORDS OF MY HEALTH RECORD SYSTEM USE WITH THE SYSTEM OPERATOR**

Where [INSERT ACCHS NAME] is part of a network hierarchy, the RO/OMO will establish and maintain an up-to-date record, which details the linkages between organisations in the network hierarchy, with the System Operator.

Where individual healthcare providers in [INSERT ACCHS NAME] are authorised to access the My Health Record system on its behalf, using the provider portal, the OMO(s) will establish and maintain an accurate and up-to-date list of individuals with the System Operator. If an individual healthcare provider is no longer authorised to access the provider portal on behalf of the organisation, the OMO will ensure the System Operator is informed and the individual removed from the list of authorised users.

**ACCESS TO THE MY HEALTH RECORD SYSTEM AND USER ACCOUNT MANAGEMENT**

[INSERT ACCHS NAME] staff must only access the My Health Record system if this access is required by the duties of their role. All staff members whose role requires them to access the My Health Record system will be provided a unique user account with individual login name by the OMO. [INSERT [ACCHS NAME] will maintain records linking user accounts to individual staff so that these can be matched in the case of an audit by the System Operator. Staff will ensure that they assign a secure password to their user account and keep their password secret. Staff will ensure passwords are regularly reviewed, changed and sufficiently complex. For more information about secure passwords and maintaining user accounts, please refer to the RACGP Computer and Information Security Standards.

The RO/OMO will ensure that they immediately suspend or deactivate individual user accounts in cases where a user:

1. leaves [INSERT ACCHS NAME]
2. has the security of their account compromised
3. has a change of duties so that they no longer require access to the My Health Record system

User accounts will not be used by multiple staff members. All users will ensure that they log out of the system when they are not using it to prevent unauthorised access.

**IDENTIFICATION OF STAFF MEMBERS WITH AUTHORISED ACCESS TO THE MY HEALTH RECORD SYSTEM**

The OMO will maintain a record of authorised Healthcare Provider Identifier – Individual numbers in the clinical software and in the organisation’s internal records. The clinical software will be used to assign and record unique internal staff member identification codes. This unique identification code will be recorded by the clinical software against any My Health Record system access.

[INSERT ACCHS NAME] will maintain such records (for example staff rostering records) as to allow it to determine which user accessed the system on a particular day. These records must be maintained to allow audits to be conducted by the System Operator.

Where required, the organisation will maintain staff rostering records to assist in identifying particular authorised users that have accessed the My Health Record system.

**STAFF TRAINING**All staff with authorisation to access the My Health Record system on behalf of [INSERT ACCHS NAME] will be required to undertake My Health Record system training. Existing staff will undertake My Health Record system training before they first access the system, while new staff will be required to undertake training, if appropriate to their role, as part of their orientation [INSERT ACCHS NAME].

Staff training will provide information about how to use the [INSERT ACCHS NAME]’s clinical software, and/or the My Health Record system Provider Portal, in order to access the My Health Record system accurately and responsibly. Staff training will consist of a combination of training materials provided by the system operator through the learning centre, and training specific to the clinical software used by [INSERT ACCHS NAME].

Staff who require My Health Record system access will be provided with, and participate in regular privacy and My Health Record system access training provided by [INSERT ACCHS NAME]. If any new functionality is introduced into the system, additional training will be provided to all staff with authorised access to the My Health Record system.

The OMO will oversee a register of staff training as it relates to the My Health Record system.

**REPORTING SECURITY BREACHES**

If any staff member becomes aware of a security breach, it is their responsibility to follow the reporting procedure outlined in the procedures section below. All breaches will be reported to the OMO/RO who will ensure that the breach is reported to the System Operator and the Office of the Australian Information Commissioner.

A security breach is when there is an unauthorised collection, use or disclosure of health information included in a patient’s My Health Record, an example of which is when a staff member with access to the My Health Record system discovers that someone else may have gained access to their user account.

**RESPONDING TO PATIENT COMPLAINTS**[INSERT ACCHS NAME] will make patients aware of the process for raising issues or complaints and will log any issues that they are made aware of. Patients will also be made aware of their ability and the process to remove clinical documents if they so choose (i.e. through the consumer portal or the My Health Record system Call Centre on 1800 723 471).

If a patient raises an issue in relation to unauthorised access to their My Health Record [INSERT ACCHS NAME] shall take steps to investigate the issue. Unauthorised access should be managed through [INSERT ACCHS NAME]’s complaint management and staff performance management processes. If the unauthorised access is found to be by someone not employed by [INSERT ACCHS NAME] the patient and the complaint should be referred to the management of that service and/or the Office of the Information Commissioner.

Where a patient asks [INSERT ACCHS NAME] to remove or amend a shared health summary or other document, and the medical practitioner agrees, the request will be logged with the [INSERT ACCHS NAME]’s OMO and the document removed, or a new amended document uploaded, within 7 days.

If the provider does not consider an amendment to be appropriate then the provider may choose to remove the document. If the provider does not consider the removal of the document to be appropriate, then the provider should discuss this with the patient and where relevant direct the consumer to exercise their personal controls over the document.

**MAINTAINING** [INSERT ACCHS NAME]**’S MY HEALTH RECORD SYSTEM POLICY**The OMO is responsible for ensuring the accuracy of the organisation’s My Health Record system access and security policy and its compliance with My Health Record system legislation. The OMO will ensure that the policy remains current and reflects changes in My Health Record system legislation and in the structure of the organisation.

**ACCESS TO THE MY HEALTH RECORD SYSTEM POLICY**

The OMO/RO will ensure that a copy of the organisation’s My Health Record system access and security policy is made available to the System Operator within 7 days of receiving the request where this request has been made in writing. The OMO/RO will ensure that the version of the My Health Record system access and security policy provided is the version of the organisation’s policy that was in force on the dates specified by the System Operator in its written request.

1. **PROCEDURES**

**ACCESS FLAGS**

The RO/OMO will refer to review ‘Section B’ of the [Registration booklet for healthcare organisations](http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/providerregistration_eBooklet#15) in order to determine whether [INSERT ACCHS NAME] has a simple or complex organisational structure. Where the RO/OMO determines that a complex organisational structure applies, they will ensure that they understand access flags and network hierarchies before applying to the Health Identifier service and assigning access flags.

Where a complex organisational structure applies, and where a patient raises concerns about the ability to control access to their My Health Record within the organisational structure, the RO/OMO will ensure that a review of the network hierarchy and the assignment of access flags is undertaken.

**DOCUMENT MANAGEMENT**

[INSERT ACCHS NAME] will destroy My Health Record system documents and record codes as per health service policies on destruction of confidential records.

**MAINTAINING RECORDS OF MY HEALTH RECORD USE WITH THE SYSTEM OPERATOR**

The OMO will determine whether the practice management software employed by [INSERT ACCHS NAME] keeps a record of the individual staff members assigned to a particular user account. If not, the OMO will create and maintain a separate record which details the links between user accounts and individual staff.

Where individual health providers are authorised by the organisation to access the My Health Record System Provider Portal, the OMO will maintain the currency of this authorisation by adding new staff, and immediately removing any staff who no longer require access to the My Health Record system or leave [INSERT ACCHS NAME].

**REPORTING SECURITY BREACHES**

If any staff member becomes aware that their user account has become compromised or that someone has used their computer to gain unauthorised access to the My Health Record system, they are to immediately inform the OMO/RO. If only the OMO is informed, it is the OMO’s responsibility to ensure that the RO is made aware of the issue.

The RO/OMO will create a log entry of the breach including details of the date and time of the breach, the user account that was involved in the unauthorised access, and which patient’s information was accessed (where known).

The RO/OMO will also undertake appropriate mitigation strategies, including, but not limited to:

* Suspending/deactivating the user account
* Changing the password information for the account
* Reporting the breach to the System Operator and the Office of Australian Information Commission

**MAINTAINING ORGANISATION’S MY HEALTH RECORD SYSTEM POLICY**As part of their responsibility for maintaining the organisation’s My Health Record system access and security policy, the OMO will ensure that:

* The My Health Record system access and security policy has a version number;
* Each time the policy is updated, the new version contains a unique version number and the date when that iteration came into effect;
* The policy is reviewed at least annually.
* The policy is reviewed at any time that changes to the My Health Record system occur, or when changed risks are identified. The review should examine:
  + Any potential security risks that may result in My Health Record system being accessed by unauthorised users
  + Any changes to the My Health Record system that may affect the healthcare provider organisation
  + Any relevant legal or regulatory changes that have occurred since the last review

The OMO will ensure that copies are kept of each version of the My Health Record system access and security policy.

**MY HEALTH RECORD POLICY CHECKLIST**

* Responsible Officer and Organisation Maintenance Officer roles assigned to people with appropriate levels of authority and legal responsibility
* Network hierarchy and access flags set in a way that meets reasonable consumer expectations (where appropriate to size and structure of organisation)
* Individual Clinical Information Software (CIS) logins and secure passwords assigned to all staff with access to the My Health Record system
* Internal record of authorised users with PCEHR access retained including individual clinical software identification codes.
* Policies and procedures in place to govern access to the My Health Record system
* Staff provided with My Health Record system training and given ongoing access to My Health Record system policy
* Where provider portal access is authorised for staff, an up-to-date list of authorised healthcare providers maintained
* On request, patients are provided with information about complaints procedure

|  |  |
| --- | --- |
| **Policy Manager** | **ADD OMO NAME HERE** |
| **Contact** | <Organisation Maintenance Officer>  Tel: **ADD PHONE NUMBER**  Fax: **ADD FAX NUMBER** |
| **Approval Authority** | Responsible Officer |
| **Latest Review Date** | DD/MM/YY (12 months from date of approval) |

**REVISION HISTORY** *(to be maintained by Organisational Maintenance Officer)*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Revision Ref. No.** | **Approved/ Amended/ Rescinded** | **Date** | **Committee/Board** | **Resolution Number** | **Document Reference** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |