**Personally Controlled Electronic Health Record (PCEHR) Security and Access Policy**

***Please note that the following is intended as a guide only and should be individualised to meet the needs of your organisation. We do not recommend implementing the policy without first considering whether it meets your needs.***

*This sample policy was developed by Inner East Melbourne Medicare Local.*

1. **PURPOSE**

To provide guidance for staff and contractors about access to, and use of, the Personally Controlled Electronic Health Record system. To provide guidance in the use of information technology in the organisation as it relates to the PCEHR system.

1. **SCOPE OF POLICY**

This policy applies to all staff (including its employees and any healthcare provider to whom the organisation supplies services under contract) with access to the Personally Controlled Electronic Health Record system.

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

The following roles are responsible for implementation and compliance monitoring of the PCEHR policy:

* Responsible Officer: The RO has legal responsibility for compliance with this policy and compliance with the national PCEHR legislation.
* Organisation Maintenance Officer: The OMO is responsible for implementation and compliance monitoring of the PCEHR policy, and for maintenance of the policy.

1. **RELATED DOCUMENTS/LINKS**

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

[*PCEHR Rules 2012*](http://www.comlaw.gov.au/Details/F2012L01703)

[*Personally Controlled Electronic Health Records Act 2012*](http://www.comlaw.gov.au/Details/C2012A00063)

[*Personally Controlled Electronic Health Records Regulation 2012*](http://www.comlaw.gov.au/Details/F2012L01399)

[*RACGP Computer and Information Security Standards*](http://www.racgp.org.au/Content/NavigationMenu/ClinicalResources/ehealth/ciss/2011ComputerInformationSecurityStandards.pdf)

[*Healthcare Identifier 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 PCEHR.
* ***Access list*** means the record associated with a consumer’s PCEHR that specifies the registered healthcare provider organisations permitted to access a consumer’s PCEHR.
* ***Act*** means the *Personally Controlled Electronic Health Records Act 2012*.
* ***Advanced access controls*** means the access controls that enable a registered consumer to set controls on the registered healthcare provider organisations and nominated representatives who may access the consumer’s PCEHR, and the records within the PCEHR.
* ***Consumer-entered health summary*** means the summary of information, including medications and allergies, that a registered consumer may enter into his or her PCEHR and which is available to anyone with access to the consumer’s PCEHR.
* ***Default access controls*** means the access controls that apply where a registered consumer has not set controls on the registered healthcare provider organisations or nominated representatives who may access the consumer’s PCEHR.
* ***Document code*** means a code which may be used to restrict access to individual records within a consumer’s PCEHR in accordance with paragraph 5(1)(c).
* ***Effectively remove***, in relation to a record in a consumer’s PCEHR, means rendering the record inaccessible to the consumer, their nominated representatives and any registered healthcare provider organisations involved in the care of the consumer, including in the case of a serious threat in accordance with rules 6 and 7.
* ***Healthcare identifier*** has the same meaning as in section 9 of the *Healthcare Identifiers Act 2010*.
* ***Identified healthcare provider*** has the same meaning as in the *Healthcare Identifiers Act 2010*.
* ***Network hierarchy*** means a network of healthcare provider organisations created and managed in accordance with subsections 9A(3) to (7) of the *Healthcare Identifiers Act 2010*.
* ***Network organisation*** has the same meaning as in the *Healthcare Identifiers Act 2010*.
* ***Organisation maintenance officer*** has the same meaning as in the *Healthcare Identifiers Act 2010*.
* **PCEHR:** Personally Controlled Electronic Health Record  
  ***Provider portal*** means the portal provided by the System Operator that permits registered healthcare provider organisations to access the PCEHR system without having to use a clinical information system.
* ***Record code*** means acode which may be used to restrict access to a consumer’s PCEHR in accordance with paragraph 5(1)(a).
* ***Responsible officer*** has the same meaning as in the *Healthcare Identifiers Act 2010*.
* ***Restore***, in relation to a record, means making a record, which has previously been effectively removed, accessible to the consumer, their nominated representatives and any registered healthcare provider organisations involved in the care of the consumer in accordance with any applicable access control mechanisms, including in the case of a serious threat to an individual’s life, health or safety.
* ***Seed organisation*** has the same meaning as in the *Healthcare Identifiers Act 2010*.
* ***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*.
* **System operator:** Department of Health and Ageing
* ***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.

**ACCESS FLAGS**

Where appropriate to the size and complexity of this organisation, 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 eHealth records 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 PCEHR USE WITH THE SYSTEM OPERATOR**

Where this organisation 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 the organisation are authorised to access the PCEHR 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 PCEHR**

Organisational staff must only access the PCEHR if this access is required by the duties of their role. All staff members whose role requires them to access the PCEHR will be provided a unique user account with individual login name by the OMO. The organisation 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. 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 the organisation
2. has the security of their account compromised
3. has a change of duties so that they no longer require access to the PCEHR 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 PCEHR 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 PCEHR system access.

The organisation 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 PCEHR system.

**STAFF TRAINING**All staff with authorisation to access the PCEHR system on behalf of the organisation will be required to undertake PCEHR training. Existing staff will undertake PCEHR 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 to the organisation.

Staff training will provide information about how to use the organisation’s clinical software, and/or the PCEHR Provider Portal, in order to access the eHealth 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 the organisation.

If any new functionality is introduced into the system, additional training will be provided to all staff with authorised access to the PCEHR system.

The OMO will oversee a register of staff training as it relates to the PCEHR.

**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.

A security breach is when any unauthorised person accesses the PCEHR, or when a staff member with access to the PCEHR discovers that someone else may have gained access to their user account.

**RESPONDING TO PATIENT COMPLAINTS**The organisation will make patients aware of the process for raising issues or complaints and will log any issues that they are made aware of. Where a patient asks the organisation to remove or amend a shared health summary or other document, and the medical practitioner agrees, the request will be logged with the organisation’s OMO and the document removed within 7 days.

In cases where there is disagreement between the medical practitioner and the patient about amendments to a shared health summary, the patient will be made aware of the ability to lodge a complaint with the Office of the Information Commissioner.

**MAINTAINING ORGANISATION’S PCEHR POLICY**The OMO is responsible for ensuring the accuracy of the organisation’s PCEHR policy and its compliance with PCEHR legislation. The OMO will ensure that the policy remains current and reflects changes in PCEHR legislation and in the structure of the organisation.

**ACCESS TO THE PCEHR POLICY**

The OMO/RO will ensure that a copy of the organisation’s PCEHR 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 PCEHR 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. **RESPONSIBILITY FOR IMPLEMENTATION AND COMPLIANCE MONITORING**

The following roles are responsible for implementation and compliance monitoring of the PCEHR policy:

* Responsible Officer: The RO has legal responsibility for compliance with this policy and compliance with the national PCEHR legislation.
* Organisation Maintenance Officer: The OMO is responsible for implementation and compliance monitoring of the PCEHR policy, and for maintenance of the policy.

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 the organisation has a simple or complex organisational structure. Where the RO/OMO determines that a complex organisational structure applies, they will ensure that the understand [access flags](http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/providerregistration_eBooklet#14) and [network hierarchies](http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/providerregistration_eBooklet#17) 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 eHealth 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.

**MAINTAINING RECORDS OF PCEHR USE WITH THE SYSTEM OPERATOR**

The OMO will determine whether the practice management software employed by the organisation 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 PCEHR 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 PCEHR or leave the organisation.

**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 PCEHR, 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

**MAINTAINING ORGANISATION’S PCEHR POLICY**As part of their responsibility for maintaining the organisation’s PCEHR policy, the OMO will ensure that:

* The PCEHR 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 PCEHR system occur, or when changed risks are identified. The review should examine:
  + Any potential security risks that may result in PCEHR records being accessed by unauthorised users
  + Any changes to the PCEHR 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 PCEHR policy.

|  |  |
| --- | --- |
| **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** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**PCEHR 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 PCEHR
* 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 PCEHR
* Staff provided with PCEHR training and given ongoing access to PCEHR 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