PERSONALLY CONTROLLED ELECTRONIC HEALTH RECORD (PCEHR) SYSTEM POLICY

1. PURPOSE

The purpose of this policy is to:

- Advise WA Health staff (including employees and contractors) about their responsibilities in accessing and using the national PCEHR system (also known as the National eHealth Record system);
- Promote compliance with the requirements of the national Healthcare Identifiers Act, Regulations and Rules; and
- Promote compliance with the requirements of the national PCEHR Act, Regulations and Rules.

2. BACKGROUND

2.1 Personally Controlled Electronic Health Record System

The Australian Personally Controlled Electronic Health Record (PCEHR) system (also known as the National eHealth Record system) was launched on 1 July 2012, following the passage of the Commonwealth PCEHR Act 2012. The Australian Government Department of Health is the System Operator.

People seeking healthcare in Australia can opt-in to register for the PCEHR – a secure, electronic summary of important health information. Participation in the PCEHR is voluntary. Consumers control what information is placed in it and which healthcare organisations may access it.

The PCEHR may hold a shared health summary created by the consumer’s nominated healthcare provider; clinical documents loaded by registered healthcare organisations; a consumer-entered health summary that is visible to healthcare organisations that have access to the consumer’s record; and consumer notes that are visible only to the consumer.

Medicare data, including MBS, PBS, Australian Organ Donor Register and Australian Childhood Immunisation Register data may be incorporated into the PCEHR system for those people who want such information to be part of their record.

The PCEHR system is not intended to replace the medical records maintained by healthcare organisations.

Information on the PECHR system is available at http://www.ehealth.gov.au.
2.2 Healthcare Identifiers

The Healthcare Identifiers Service (HI Service) is a national system for uniquely identifying healthcare providers (organisations and individual healthcare providers) and consumers.

A healthcare identifier is a unique 16 digit number which makes sure the right health information is associated with the right individual. The HI Service forms the basis of other eHealth initiatives such as the PCEHR system.

Individual Healthcare Identifiers have been issued to all Australians who hold a Medicare Card or a Department of Veteran Affairs Card.

Healthcare Provider Identifiers- Individual has been allocated to all healthcare professionals who are registered with the Australian Health Practitioner Regulation Agency.

The Australian Government Department of Human Services is the Healthcare Identifiers Service Operator and manages the allocation, maintenance and disclosure of healthcare identifiers to healthcare providers and the public. This is legislated under the Healthcare Identifiers Act 2010


3. SCOPE

This policy applies to all WA Health staff who have been authorised to access the PCEHR system, within the following entities:

- Department of Health;
- Metropolitan Health Service; and
- WA Country Health Service.

This policy also applies to any contracted service provider of WA Health who has been authorised to access the PCEHR system or the Healthcare Identifiers Service on behalf of WA Health. A contracted service provider of a healthcare provider organisation means an entity that provides

(a) information technology services relating to the PCEHR system; or
(b) health information management services relating to the PCEHR system;

to the healthcare provider organisation under a contract with the healthcare provider organisation.

This policy must be read in conjunction with the following WA Health policies.

- Acceptable Use Policy
- Information Security Policy
- Logon Standard
- Information Access and Disclosure Policy
This policy must be read in conjunction with the following Commonwealth Acts, Regulations and Rules covering the Healthcare Identifiers and the PCEHR which are available at Australian Government ComLaw website

- Healthcare Identifiers Act 2010
- Healthcare Identifiers Regulation 2010
- Personally Controlled Electronic Health Records Act 2012
- Personally Controlled Electronic Health Records Regulation 2012
- PCEHR Rules 2012 and Explanatory Statement
- PCEHR (Participation Agreement) Rules 2012

PCEHR Rules and the PCEHR Rules Explanatory Statement provide further information on the operations of network hierarchy, access flags and advanced access controls as described in sections 4.3 and 4.4.

4. POLICY

4.1 Healthcare Identifiers

WA Health’s collection, use and disclosure of the Individual Healthcare Identifiers (IHI), Healthcare Provider Identifiers-Individual (HPI-I) and Healthcare Provider Identifiers-Organisation (HPI-O) must be in compliance with the Healthcare Identifiers Act and Regulations.

WA Health maintains its own patient identifier, the Unique Medical Record Number (UMRN) as its primary patient identifier. WA Health will use the Individual Healthcare Identifiers (IHIs) for e-health communications with external healthcare providers.

WA Health will not create unverified or provisional IHIs for its patients.

IHIs and their status for WA Health patients are maintained in the Enterprise Master Patient Index. Only searches endorsed via the Conformance, Compliance and Accreditation process for the Healthcare Identifiers Service will be used to retrieve IHIs from the HI Service.

4.2 Registration and Authority to Act

The Department of Health WA is registered with the Healthcare Identifiers Service Operator as a Seed Organisation for WA Health and has been issued with a Healthcare Provider Identifier - Organisation (HPI-O).

WA Health has entered into a Participation Agreement with the PCEHR System Operator and is eligible to be registered to access and use the PCEHR System.

The Executive Director Corporate and Strategic Services of the Health Information Network is the WA Health Responsible Officer (RO) in dealing with the Healthcare identifiers Service and the PCEHR System.

The RO is responsible for the registration of Organisational Maintenance Officers (OMOs) with the HI Service and the PCEHR System.

The RO and OMOs for WA Health are authorised to act on its behalf in dealings with the Healthcare Identifiers Service Operator and PCEHR System Operator.
4.3 Organisational Hierarchy and Access Flags

Where appropriate to the size and complexity of WA Health and consistent with WA Health’s internal information sharing norms, the RO/OMO will define an appropriate organisational hierarchy for WA Health and assign access flags appropriately for the structure of WA Health. The organisational hierarchy will define the seed (head) organisation, and where considered necessary, the network (subordinate) organisations that fall under that seed organisation, and the network organisations for which access flags are appropriate.

Access flags are assigned against healthcare organisations to support a consumer’s ability to know and determine which organisations can access their PCEHR record and track over time which organisations have accessed their records. If an access flag is not set at a network organisation then the next organisation up the hierarchy that has an access flag set will appear in the patient’s access List, index lists and audit records.

The RO/OMO will undertake reviews of the network hierarchy 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. WA Health commits to consider requests from the System Operator for reasonable changes to the network hierarchy that are consistent with WA Health’s internal information sharing norms.

The RO/OMO will establish and maintain an up-to-date record with the System Operator that details the WA Health network organisation hierarchy.

To identify the healthcare organisation that has transacted with the PCEHR, WA Health will create a network organisation and set an access flag in the Healthcare Identifiers Service for each WA Health organisation that uploads clinical documents into the PCEHR. This is necessary to identify the organisation in the patients’ index lists and audit logs.

4.4 Advanced Access Controls

A consumer when registering for a PCEHR record can set access controls limiting which healthcare organisations/providers are allowed to access the consumer’s record (record code) or specific documents (document code). The default access control settings permit all PCEHR registered healthcare organisations/providers to upload, view and download their patients’ clinical documents.

A consumer may block direct access to their PCEHR by an organisation that has an Access Flag. They may do so by either removing the organisation from their Access List, or by setting a record code and not providing it to the organisation when they present for care.

Any advanced access controls or access flags set by the consumer for their PCEHR record or documents will not apply to copies of the same clinical documents that are held in WA Health’s local information systems.

Where a document code or record code has been provided to WA Health by a patient to allow access, WA Health staff will not keep a copy of the code for future use, even if the patient requests that the healthcare organisation holds the code for future use.
4.4.1 Access Control Mechanisms and Serious Threats

Section 64 of the PCEHR Act allows healthcare organisations to override advanced access controls in the case of a serious threat to an individual’s life, health or safety, or to public health and safety.

The WA Health clinical software\textsuperscript{1} that are used to access the PCEHR system will allow the override of the advanced access control to permit access to the patient’s PCEHR documents. The functions will invoke the assertion to the System Operator of the existence of the serious threat.

Staff who use the override option must be able to justify the circumstances for the override during any audit by the Systems Operator.

4.5 Patient’s Authorised Representatives

A patient may have an authorised representative, that is, a parent of a patient who is less than 18 years old, or a person who the System Operator is satisfied is lawfully authorised to act on behalf of the patient.

An authorised representative of a patient registered with the System Operator is entitled to do anything that the PCEHR Act authorises or requires the patient to do, for example, setting access controls or withdrawing consent to upload documents.

4.6 Withdrawing Consent /Setting Document Codes

Each time a patient attends a WA Health organisation the patient can verbally request that certain clinical documents not be uploaded to their PCEHR record or request a document code be applied if they have set advanced access controls.

WA Health will not upload a clinical document to the PCEHR if the patient has withdrawn consent for the event. The requirement not to upload the document(s) for the event will be flagged in the clinical software that is used to access the PCEHR system. This withdrawal of consent is applicable for the particular event/episode/document and only for the specific organisation. If the patient attends the same organisation or another organisation at a future date then it is the patient’s responsibility to request any subsequent withdrawal of consent.

If the patient withdraws consent for uploading an event summary to the PCEHR but consents for it to be sent to another healthcare provider who maintains the patient’s shared health summary, the patient needs to inform that other healthcare provider not to include the relevant information in the shared health summary.

If consent is withdrawn after a clinical document has been uploaded into the PCEHR it is the patient’s responsibility to ‘effectively remove’ the record from the PCEHR system through the System Operator. The patient may also subsequently choose to restore a removed document via the System Operator.

\textsuperscript{1} Initially the WA Health clinical software used to access the PCEHR are the \textit{Notifications and Clinical Summaries} system and the \textit{Communicare} system.
4.7 Identification of WA Health Staff with Authorised Access to the PCEHR System

WA Health staff must only access a patient’s PCEHR, if this access is required by the duties of their role relating to the care of the patient, or for matters prescribed by the PCEHR Act; and their access is authorised.

Staff who have been authorised to access the PCEHR system must not access records that they are not entitled to access. Accessing records of colleagues, friends, relatives, celebrities or other persons that are not for legitimate WA Health business purposes breaches WA Health policies and commonwealth legislation. Such access may constitute misconduct or a breach of discipline under the WA Health Misconduct and Discipline Policy.

Only WA Health staff who have been allocated a national Healthcare Provider Identifier – Individual (HPI-I) may be authorised to access the PCEHR. The processes for user provisioning and revoking access are defined in the Logon Standard. The default mode of access to the PCEHR is via the designated clinical software.

One role that will be assigned to select individuals in an organisation will be an administrator role to enable the removal of incorrect or wrongly posted PCEHR documents.

All access to the PCEHR is logged by the System Operator and consumers can view the access logs relating to their record.

WA Health staff who have not been authorised to access the PCEHR must not seek access to a patient’s PCEHR. Any access of a patient’s PCEHR by a WA Health staff member who is not authorised to access the PCEHR and any person who facilitates access by an unauthorised person will be in breach of WA Health policies and also Commonwealth legislation.

4.7.1 Access via the Clinical Information System

All staff whose roles require them to access the PCEHR will be provided access via the designated clinical software. The WA Health user identifier (‘he’ number) will be the identifier for the PCEHR system access via the clinical software.

WA Health staff will ensure that they assign a secure password to their user account and keep their password secret.

WA Health will immediately suspend or deactivate individual user accounts access to the PCEHR in cases where a user:

(i) leaves the organisation
(ii) has the security of their account compromised
(iii) has a change of duties so that they no longer require access to the PCEHR system

Only user accounts assigned to individual staff will be authorised to access the PCEHR. Staff assigned generic, group or shared identifiers will not have access to the PCEHR system. All users will abide by the Logon Standard.
All access to the PCEHR will be logged and will be available to be audited by the System Operator. The clinical software will pass the WA Health user identifier on to the PCEHR System each time an access is made, and will also maintain a local access log.

These records will be maintained to allow audits to be conducted by the System Operator.

4.7.2 Access via the Provider Portal

The Provider Portal has been established by the PCEHR System Operator to provide authorised healthcare professionals working for a registered Healthcare Organisation with read-only access to the PCEHR.

This is achieved by the OMO establishing a list of healthcare professionals with the System Operator whose HPI-Is are linked to WA Health’s HPI-O.

A PCEHR compliant digital credential on a token (smartcard or USB) is also required to be issued by the National Authentication Service for Health (NASH) to the individual healthcare provider to access the PCEHR.

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.

4.8 Uploading Clinical Document to the PCEHR

In uploading clinical documents to the PCEHR system, WA Health must:

- not infringe intellectual property or moral rights;
- not upload documents that contains defamatory material;
- only upload contents for registered consumers;
- not upload documents if the patient has asked that the documents not be uploaded;
- only upload documents approved by an authorised clinician and who has been allocated a Healthcare Provider Identifier - Individual;
- not upload documents created by or sourced from another organisation which is not part of WA Health;
- take appropriate measures to ensure data quality and accurate identification of the patient;

Uploading a record to the PCEHR does not relieve WA Health staff of their obligations to maintain their healthcare organisation’s own clinical records and other local obligations.

4.9 Document Versions

A patient’s PCEHR document uploaded by a WA Health organisation may be superseded at any time by uploading a new document version that contains updates or corrections, using the same document identifier. The previous version(s) will remain as superseded documents to provide an audit trail of the changes.
4.10 Removing Documents from the PCEHR

If a clinical document is loaded in error or posted to the wrong patient, WA Health will remove the document from the PCEHR. A specialist role of local administrator will be allocated to a select group of individuals in each WA healthcare organisation to review and action such requests. The process to remove the PCEHR document will also include removal of the copies of the incorrect documents from local repositories and withdrawal of those sent point-to-point, for example, to General Practitioners.

4.11 Viewing PCEHR Documents

Every time a clinical decision is made based on the information in a viewed PCEHR clinical document, it is recommended that the source document information such as the document identifier and version number, are noted in the patient’s medical record, as the source document may subsequently be removed from the PCEHR by the patient or the creating healthcare organisation.

4.12 Responding to Patient Requests/Complaints

WA Health staff will make patients aware of the process for raising issues or complaints with regard to their WA Health PCEHR transactions and will log any issues of which they are made aware with the healthcare organisation’s patient/client liaison department.

Where a patient asks a WA Health organisation to amend a PCEHR document created by that organisation, and the organisation agrees, an amended version of the document will be uploaded.

Any document loaded to the PCEHR by WA Health is a copy of a document held in a local WA Health repository; therefore a WA Health organisation will not amend a PCEHR document unless it is prepared to amend the local document in the first instance. In the event the organisation will not amend a document, the patient still has the ability to have the document removed from the PCEHR via the System Operator.

In cases where there is disagreement between the WA Health organisation and the patient about amendments to a clinical document loaded into the PCEHR, the patient will be made aware of the process to escalate the issue within WA Health.

If the issue is not able to be resolved by WA Health to the patient’s satisfaction, the patient has the ability to lodge a complaint with the System Operator or the Office of the Australian Information Commissioner. Where a PCEHR document is a copy of the local document, the patient must also be made aware of the WA State processes for access to patient records and making complaints. WA Health has published a Complaints Management Policy.

4.13 PCEHR Training

All staff with authorisation to access the PCEHR system on behalf of WA Health will be required to undertake training on the PCEHR system before they first access the systems.

The PCEHR training will provide information about how to use WA Health’s clinical information software in order to access the PCEHR system accurately and responsibly. 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 WA Health to access the PCEHR.

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

WA Health will maintain records of staff training as it relates to the PCEHR.

The individual projects that implement the clinical software that access the PCEHR system will provide access to the training materials and will work with the healthcare organisation on the processes for ensuring the training is effectively carried out and recorded.

4.14 Reporting Security Incidents related to the PCEHR

If any person becomes aware of a security incident, it is their responsibility to follow the reporting procedure outlined in the procedures section below.

WA healthcare organisations will audit access logs for potential information security incidents.

A security incident is

- When any unauthorised person accesses the PCEHR; or
- When an officer with access to the PCEHR discovers that someone else may have gained access to their user account; or
- When an individual’s password is disclosed to another individual or individuals; or
- The accidental, misuse or unauthorised disclosure of information from a person’s PCEHR.

Security breaches will be managed in accordance with the healthcare organisation’s procedures which may result in the following:

- The relevant user account may be suspended until the extent and severity of the security incident is determined.
- The OMO is notified of the incident
- The OMO advises the System Operator of the incident

4.15 Auditing/Investigating Breaches

The Commonwealth Information Commissioner is empowered to undertake investigations of breaches of privacy relating to the PCEHR. This can be either in response to complaints or ‘own motion investigations’.

The System Operator can request to see WA Health’s PCEHR Policies and records of access of the PCEHR System by WA Health staff.

5. IMPLEMENTATION

Chief Executives and Executive Directors are responsible for ensuring that all staff within their areas of responsibility adhere to this policy.

The RO has legal responsibility for compliance with this policy and the PCEHR legislation.
The Seed OMO is responsible for the implementation and compliance monitoring of the PCEHR Policy and for its maintenance.

The Seed OMO will maintain a copy the authorised current and all previous versions of this policy and make them available on request by the System Operator.

The OMO is responsible for ensuring the accuracy of this 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.

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.

6. ASSOCIATED WA HEALTH POLICIES, STANDARDS AND GUIDELINES
   - Information Security Policy
   - Acceptable Use Policy – Information and Communications Technology
   - Logon Standard
   - Information Access and Disclosure Policy
   - WA Health Complaints Management Policy
   - WA Health Misconduct and Discipline Policy

7. RELEVANT LEGISLATION AND GOVERNMENT POLICIES
   (WA Acts are available at the State Law Publisher website; Commonwealth Acts are available at the Australian Government ComLaw website)

   - Freedom of Information Act 1992 (WA)
   - Healthcare Identifiers Act 2010
   - Healthcare Identifiers Regulation 2010
   - Personally Controlled Electronic Health Records Act 2012
   - Personally Controlled Electronic Health Records Regulation 2012
   - PCEHR Rules 2012
   - PCEHR (Participation Agreement) Rules 2012
   - State Records Act 2000 (WA)

8. REFERENCES
   - Inner East Melbourne Medicare Local Sample Security and Access Policy template
   - Victorian Eastern Health Service PCEHR System (eHealth Record) Policy.
   - AMA Guide to Medical Practitioners on the use of the Personally Controlled Electronic Health Record System.
9. 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 restrict the extent to which additional registered healthcare provider organisations in the same network hierarchy are able to gain access to a consumer’s PCEHR. Seed organisations are assigned an access flag by default.

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.

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, which 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.

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 PCEHR rules 6 and 7.

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

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

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

Organisation Maintenance Officer has the same meaning as in the Healthcare Identifiers Act 2010.

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

Record code means a code which may be used to restrict access to a consumer’s PCEHR.

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** is the Organisation Maintenance Officer in a seed organisation. Has primary responsibility for OMO roles and coordination of OMO activities in network organisations.

**Service Operator** is the Commonwealth Department of Human Services.

**System Operator** is the Commonwealth Department of Health

### 10. VERSION CONTROL

<table>
<thead>
<tr>
<th>Current Version</th>
<th>Effective Date:</th>
<th>Operational Directive No:</th>
<th>SHEF ICT Approved Date:</th>
<th>Next Review Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>15 October 2013</td>
<td></td>
<td>11 October 2013</td>
<td>15 June 2014</td>
</tr>
</tbody>
</table>

**Responsible Group:**
Health Information Network - Strategy

**Enquiries Contact:**
Manager E-Health Policy and Governance

v1.0 October 2013 - Original document.