Government of **Western Australia**
WA Country Health Service

My Health Record

(MHR)

Manual

System Control, Administration, Access, Upload and Security Requirements

Healthier country communities through partnership and innovation

WACHS My Health Record Manual

Contents

1. Guiding Principles

The purpose of this manual is to:

- Advise WA Country Health Service (WACHS) staff (including employees and contractors) about their responsibilities in accessing and uploading to the National My Health Record (MHR) system ;
- Promote compliance with the requirements of the National Healthcare Identifiers Act, Regulations and Rules; and
- Promote compliance with the requirements of the National *My Health Records Act 2012* (MHR Act), Regulations and Rules.

This manual applies to all WACHS staff who have been authorised to access the MHR system, clinicians that provide document content to upload to the MHR, system administrators and training/support staff that facilitate the Consent Management Protocol for MHR and those that interact or oversee staff that interact with patients that may have a MHR.

This manual also applies to any contracted service provider of WACHS who has been authorised to access the MHR system or the HI Service on behalf of the WA health system and/or WACHS.

2. Consumer Control

The Australian National My Health Record (MHR) system, also known as the National eHealth Record system and previously the Personally Controlled Electronic Health Record (PCEHR), was launched on 1 July 2012. This followed the passage of the Commonwealth *Personally Controlled Health Record Act 2012,* superseded by the MHR Act 2012.

The Australian Digital Health Agency (ADHA) commenced operations on 1 July 2016 and is tasked with improving health outcomes for Australians through the delivery of digital healthcare systems and the National Digital Health Strategy for Australia.

People seeking healthcare in Australia who meet the registration requirements and did not opt out or cancel their MHR post the opt-out period conclusion on 31 January 2019, will have a MHR. The MHR is a secure, electronic summary of important health information. Participation in the MHR is voluntary. Consumers control what information is placed in it and which healthcare organisations may access it.

The MHR 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 and/or Advance Health Directive that is visible to healthcare organisations that have access to the consumer's record; dispensed medications uploaded by a community pharmacy and consumer notes that are visible only to the consumer.

Medicare data, including Medicare Benefits Schedule (MBS) and Pharmaceutical Benefit Scheme (PBS), is automatically uploaded. Australian Organ Donor Register and Australian Immunisation Register (AIR) data may be incorporated into the MHR system for those people who want such information to be part of their record.

The MHR system is not intended to replace the health records maintained by healthcare organisations.

2.1 Authorised Representative

A consumer may have an authorised representative, that is, a person who is responsible for managing the MHR of someone who cannot manage their own. This could be for a child under 14 years, or an adult who lacks the capacity to manage their own record. An authorised representative may be a parent, carer, family member, legal guardian or someone with Enduring Power of Attorney.

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

2.2 Access Controls

At any time a patient can set access controls within their MHR record limiting which healthcare organisations/providers are allowed to access the patient's record (record code) or specific documents (document code). The default access control settings permit all MHR registered healthcare organisations/providers to up-load, view and download their patients' clinical documents.

A patient may block direct access to their MHR 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 patient for their MHR record or documents will not apply to copies of the same clinical documents that are held in the WA health system's enterprise or WACHS local information systems.

Where a document code or record code has been provided to the WACHS by a patient to allow access, WACHS 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.

2.3 Consent to Upload and View

WA health system staff, including WACHS staff, will not ask nor prompt a patient at each attendance to determine if they wish to have their documents uploaded to their MHR or if they have one. The default consent setting is to allow uploading and any recorded consent remains in force until the patient asks for it to change. If a patient does not have a MHR the consent status is not relevant as no information will be uploaded where a MHR does not exist.

As per the MHR Act if a patient is registered in the MHR system a healthcare provider may upload health information about the recipient to the MHR system, unless the record is one which the patient has advised the healthcare provider not to upload or the record is not to be uploaded under prescribed laws of a State or Territory.

Health information may be collected, used and disclosed from a patients' MHR for the purpose of providing healthcare to the recipient, subject to access controls by the recipient (or if none are set, default access controls).

2.4 Withdrawing Consent /Setting Document Codes

Each time a patient attends a WA health system organisation they can request in writing, using the appropriate form, and following the Consent Management Protocol for Publishing to the MHR or the consent management protocol of an external contractor, that certain clinical documents not be uploaded to their MHR. These documents are published on the My Health Records HealthPoint Site.

The WA health system and external contractors will not upload a clinical document to the MHR if the patient has in writing withdrawn consent for the event and that consent is recorded for the event within the timeframe set within the Consent Management Protocol for Publishing to the MHR. The requirement not to upload the document(s) for the event will be flagged in the patient administration system that is linked to systems that upload to the MHR 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 or other information to the MHR 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 MHR it is the patient's responsibility to 'remove' the record from the MHR system through their access to their MHR or via the System Operator. If the patient chooses to send the document to 'restricted and removed documents' the patient may also subsequently choose to restore a removed document. If however a patient chooses to remove a document from the MHR then it cannot be reinstated. If a patient chooses to cancel/delete their MHR then documents will not be reinstated should the patient choose to re-register in the future.

3. System Administration

The WA health system, Health Information Hub (HIH) as part of the Health Support Services (HSS) will ensure systems are compliant with the requirements of the MHR system including identifiers, terminologies and technical standards.

3.1 Individual Healthcare Identifiers

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

The WA health system maintains its own patient identifier, the Unique Medical Record Number (UMRN) as its primary patient identifier. The WA health system will use the IHI for communication with the MHR. The WA health system does not create unverified or provisional IHIs for its patients.

The Enterprise Master Patient Index (EMPI) which is used by the WA health system to store the UMRN and the IHI is the source for the patient administration system and clinical applications that link to the MHR. The Patient Administration System and Notification System (PAaNS) provides access to the EMPI and IHIs are viewable where linked to a UMRN.

3.2 Standard National Terminologies

The WA health system will use approved (Australian Standards and as are set by the Australian Digital Health Agency) terminologies in systems and fields that are the source for upload of information to the MHR. External contracted agencies providing services and systems uploading documents to the MHR will outline under contract negotiation the terminologies that will be used in uploading documents to MHR on behalf of the WA health system or WACHS.

3.3 Organisational Hierarchy

The Department of Health WA is registered with the HI Service Operator as a Seed Organisation for the WA health system and has been issued with a Healthcare Provider Identifier - Organisation (HPI-O). The WA health system has entered into a Participation Agreement with the MHR System Operator and is eligible to be registered to access and use the MHR System. The Chief Information Officer, Health Support Services (HSS) is the WA health system Responsible Officer (RO) in dealing with the HI Service and the MHR System. The RO is responsible for the registration of Organisational Maintenance Officers (OMOs) with the HI Service and the MHR System. The RO and OMOs for the WA health system are authorised to act on its behalf in dealings with the HI Service Operator and MHR System Operator.

Where appropriate due to the size and complexity of the WA health system and consistent with the WA health system's internal information sharing norms, the RO/Seed OMO (Senior Analyst, Digital Health, HSS) will define an appropriate organisational hierarchy for the WA health system and assign access flags appropriately for the structure of the WA health system. 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 patient's ability to know and determine which organisations can access their MHR 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/Seed 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 patient query reveals potential structural issues. The WA health system commits to consider requests from the System Operator for reasonable changes to the network hierarchy that are consistent with the WA health system's internal information sharing norms.

RO/Seed OMO will establish and maintain an up-to-date record with the System Operator that details the WA health system network organisation hierarchy.
To identify the healthcare organisation that has transacted with the MHR, the WA health system will create a network organisation and set an access flag in the HI Service for each WA health system organisation that uploads clinical documents into the MHR. This is necessary to identify the organisation in the patients' index lists and audit logs.

External contracted agencies providing services and uploading documents to the MHR will outline under contract negotiation the Healthcare Provider Identifiers that staff and patients will expect to relate to documents uploaded and any access to the MHR on behalf of the WA health system or WACHS. This is necessary to identify the organisation in the patients' index lists and audit logs.

4. System Access

Staff who have been authorised to access the MHR 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 system business purposes breaches WA health system policies and Commonwealth legislation. Such access may constitute misconduct or a breach of discipline under the WA health system Code of Conduct MP 0031/16 and Discipline Policy MP 0040/16.

All access to the MHR is logged by the System Operator and patients can view the access logs relating to their record. WA health system staff who do not have duties of their role relating to the care of the patient, or for matters prescribed by the MHR Act for accessing or have not been authorised to access the MHR must not seek access to a patient's MHR. Any access of a patient's MHR by a WA Health system staff member who is not authorised to access the MHR and any person who facilitates access by an unauthorised person will be in breach of WA health system policies and also Commonwealth legislation.

4.1 Staff with Authorised Access to the MHR System

As noted above, WA health system staff must only access a patient's MHR, if this access is required by the duties of their role relating to the care of the patient, or for matters prescribed by the MHR Act; and their access is authorised.

The processes for user provisioning and access are defined in the Information Security Policy MP 0067/17 however the role allocation within each application sits with the local system administrator. The default mode of access to the MHR is via links in the designated clinical software for roles deemed appropriate.

Only user accounts assigned to individual staff will be authorised to access the MHR. Staff assigned generic, group or shared identifiers will not have access to the MHR system. All users are required to abide by the Acceptable Use of Information and Communications Technology Policy.

4.2 Access via the Clinical Information System

All staff whose roles require them to access the MHR will be provided access via the designated clinical software. The WA health system user identifier ('he' number) will be the identifier for the MHR system access via the clinical software.

WA health system staff will ensure that they assign a secure password to their user account and keep their password secret.
WA health system will immediately suspend or deactivate individual user accounts access to the MHR 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 MHR system

All access to the MHR will be logged and will be available to be audited by the System Operator. The clinical software will pass the WA health system user identifier on to the MHR 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.

External contractor organisations accessing WA health system enterprise systems or WACHS local systems will not add information to WACHS records, upload information to the MHR or access the links from clinical information systems to the MHR unless as stipulated in their contract arrangements.

4.3 Viewing and Referencing MHR Documents

Every time a clinical decision is made based on the information in a viewed MHR clinical document, it is recommended that the source document information such as the document identifier and version number, are noted in the patient's health record. This will assist in preserving source document information in cases where the source document may subsequently be removed from the MHR by the patient or the creating healthcare organisation.

4.4 Access Control Mechanisms and Serious Threats / Emergency Breakglass

In instances where a patient has access controls on their MHR, Section 64 of the MHR 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 (also known as Emergency Breakglass).

Emergency Breakglass should only be used in instances where a patient has access controls on their MHR and the treating clinician is authorised by the most senior clinician on duty, or, in the instance where the treating clinician is the most senior clinician on duty, in agreement with another senior colleague on duty, that there is a need to access controlled information in the MHR. If the patient has no access controls on their MHR there is no need to use the Emergency Breakglass function.

The WA health system clinical software used to access the MHR system will allow the override of the advanced access control to permit access to the patient's MHR documents. The functions will invoke the assertion to the System Operator of the use of the emergency access.

When the "Emergency Access/Breakglass" function is used an automatic notification is sent to the ADHA who will in turn notify the WA health system via HSS to the OMO.

Where a clinician has used the Emergency Breakglass function, documentation must be contained in the patient's WACHS health record confirming that they have consulted with the senior clinician and the reasons for breaking glass. Staff who use the override/Emergency Breakglass option must be able to justify the circumstances for the override during any audit by the Systems Operator.

Where a request for advice about the circumstances that led to the use of the Emergency Breakglass function is received the Seed OMO will forward the request to the WACHS Executive Director Medical Services with a copy to the WA Health Chief Clinical Information Officer (CCIO). The request must be investigated and responded to within three weeks. The request will contain the date and time of access, HPI-O under which access was requested, user identifier (ID) or identifier of the individual who used the emergency access function and the IHI of the patient whose record was accessed. The patient's UMRN will be provided separately upon request.

5. System Uploads

In uploading clinical documents to the MHR system, WACHS staff and contractors as part of the WA health system must:

- not infringe intellectual property or moral rights
- not upload documents that contains defamatory materia;
- only upload contents for registered patients
- not upload documents if the patient has asked and provided in writing on a relevant consent form that the documents not be uploaded or has withdrawn consent for the documents to be uploaded

- only upload documents approved by an authorised healthcare provider clinician
- not upload documents created by or sourced from another organisation which is not part of the WA health system
- take appropriate measures to ensure data quality and accurate identification of the patient. These measures should include but are not limited to
  - verifying demographic information with the patient before and during a consultation
  - the clinician discussing with the patient details about the event that is summarised in information being uploaded
  - using a print-out of the patient health summary to allow the patient to verify its accuracy and suggest amendments between or prior to visits with the clinician.

Uploading a record to the MHR does not relieve WA health system staff of their obligations to maintain their healthcare organisation's own health records and other local obligations.

5.1 Document Versions

A patient's MHR document uploaded by the WA health system or contracted service provider 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.

5.2 Removing Documents from the MHR

If a clinical document is loaded in error or posted to the wrong patient, the WA health system or contracted service provider will remove the document from the MHR. Where identified within the WA health system a service call must be raised with the HSS HIH who will be responsible to action the removal of incorrect or wrongly posted MHR documents. The process to remove the MHR 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.

6. System Security

The WA health system will audit access logs for potential information security incidents.

The System Operator can request to see the WA health system's MHR Policies and records of access of the MHR System by the WA health system staff.

6.1 Reporting Security Incidents and Data Breaches

If any person/staff member becomes aware of a security incident or data breach in relation to the MHR, it is their responsibility to follow the reporting procedure outlined in the WA health system My Health Record (MHR) Policy MP0094/18 and below.

A security incident/data breach is

- When any unauthorised person accesses the MHR or
- When an officer with access to the MHR 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 MHR.

The following information should be provided:

- Description of the data breach
- Date and time of the data breach
- Cause of the data breach
- Type of information involved
- How many healthcare consumers were or may have been affected
- Whether the data breach has been contained
- What action has been taken to mitigate the effects of the data breach and/or prevent further data breaches
- Name and contact details for the appropriate contact person within your organisation
- Any other relevant information.

Contact the ADHA's My Health Record Enquiry Line 1800 723 471 (option 2 for providers) and be ready to supply the above information. The Senior Analyst, Digital Health, Health Support Service (HSS) should also be notified.

The relevant user account may be suspended until the extent and severity of the security incident is determined.

6.2 Assessing/Auditing/Investigating Breaches

Steps for the WA health system once the System Operator has been notified include:
Assess the data breach:

- Evaluate: assess whether there is a reasonable likelihood that a data breach may have occurred and the effects of the potential data breach may be serious for at least one or more healthcare consumers.
- Contain: if a data breach has or is likely to have, occurred, identify risks related to the breach and take steps to prevent additional breaches or system compromise.

Request notification:

- Assess the seriousness of the effects of each data breach on a case by case basis, taking all relevant circumstances into account.
- Ask the ADHA to notify all healthcare consumers that may be affected; or the general public if a significant number of people are impacted (Note: healthcare providers should not contact consumers directly).

Continue investigation

- Conduct an extensive investigation to determine the extent of the breach (there is an expectation that this occurs within days, not weeks).
- Depending on the data breach, staff may require the assistance of HSS, Human Resources or the Integrity Unit.
- Notify the relevant parties of any additional findings and take actions to prevent any other potential breaches of a similar nature.

6.3 Timing of notifications

The obligation to notify the relevant patients of a data breach is triggered the moment the healthcare entity becomes aware it has, or may have, occurred. This is necessary regardless of whether only preliminary investigation has been undertaken and the data breach is yet to be confirmed.

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

7. My Health Record Training

The WA health system will maintain records of staff training as it relates to the MHR.

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

7.1 Levels of Competency

Awareness

All staff are required to:

1. know what a MHR is and what information may be available within a MHR
2. be able to refer queries to the ADHA website or national hotline.

Consent Management

Patient Administration/Clerical staff are required to:

1. know what a MHR is and what information may be available within a MHR
2. understand the Consent Management Protocol and direct patients to the appropriate form to complete if they wish to withdraw or reinstate their consent and upload the consent to the patient administration system
3. be able to refer queries to the ADHA website or national hotline.

Capable

Clinical staff including but not limited to Doctors, Nurses & Midwives, Pharmacists, Aboriginal Liaison Officers, Allied Health Staff (including Assistants) should be able to:

1. explain what the MHR is, including the benefits
2. access a MHR from relevant software

3. understand the Consent Management Protocol and direct patients to the appropriate form to complete if they wish to withdraw or reinstate their consent
4. address or appropriately refer patient queries
5. be cognisant that patents will have access to information written into discharge summaries and other summaries loaded to the MHR

All staff with authorisation to access the MHR system and upload to it on behalf of the WA health system will be required to undertake training on the MHR system before they first access the systems and upload documents. This training will consist of information security and security incident management procedures including the reporting of events.

The MHR training will provide information about how to use the WA health system's clinical information software in order to access the MHR system accurately and responsibly, the legal obligations on healthcare provider organisations and individuals using the MHR system and the consequences of breaching these obligations. Training will consist of a combination of materials provided by the System Operator through the learning centre, training specific to the clinical software used by the WA health system to access the MHR, the Consent Management Protocol for Publishing to the MHR and specific material in relation to uploading information.

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

8. Responding to Consumer Requests / Complaints

In compliance with the WA Health Complaint Management Policy OD0589/15 WACHS staff will make patients aware of the WACHS consumer compliments and feedback process. The WACHS Consumer compliments and feedback website may be used for raising issues or complaints with regard to their WA Country Health MHR transactions or WACHS staff will log any issues of which they are made aware as per processes set out on the WACHS intranet Consumer Feedback page.

Where a patient asks the WA health system to amend a MHR document created, and the organisation agrees, an amended version of the document will be uploaded. Any document loaded to the MHR by the WA health system is a copy of a document held in a WA health system repository; therefore the WA health system will not amend a MHR 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 their MHR.

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

If the issue is not able to be resolved by the WA health system to the patient's satisfaction, the patient has the ability to lodge a complaint with the ADHA or the Office of the Australian Information Commissioner. Where a MHR document is a copy of the local document, the patient must also be made aware of the processes for access to patient records via the Access my WA Health medical records internet site and making complaints per processes set out on the WACHS intranet Consumer Feedback page.

Complaint processes involving contracted service providers will be as per the contract agreement.

9. Definitions

Access control mechanisms	Includes default access controls and advanced access controls.
Access flag	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 MHR. Seed organisations are assigned an access flag by default.
Access list	The record associated with a consumer's MHR that specifies the registered healthcare provider organisations permitted to access a consumer's MHR.
Advanced access controls	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 MHR, and the records within the MHR.
Contracted Service Provider	A contracted service provider of a healthcare provider organisation means an entity that provides (a) information technology services relating to the MHR system; or (b) health information management services relating to the MHR system; to the healthcare provider organisation under a contract with the healthcare provider organisation.
Consumer-entered health summary	Summary of information, including medications and allergies, which a registered consumer may enter into his or her MHR and which is available to anyone with access to the consumer's MHR.
Default access controls	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 MHR.

Document code	A code which may be used to restrict access to individual records within a consumer's MHR.
Healthcare identifier	Has the same meaning as in section 9 of the Healthcare Identifiers Act 2010.
MHR	My Health Record
Network hierarchy	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.
Record code	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	Organisation Maintenance Officer in a seed organisation. Has primary responsibility for OMO roles and coordination of OMO activities in network organisations. Is the Senior Analyst, Digital Health, Health Support Service (HSS)
Service Operator	Is the Commonwealth Department of Human Services.
System Operator	Is the Australian Digital Health Agency.

10. Roles and Responsibilities

All Staff are required to work within policy documents to make sure that WACHS meets the legislative requirements of the *My Health Record Act 2012* and meet the expectations of the consumers utilising WACHS services.

The WACHS Chief Executive, Regional Directors, Executive Directors and Program Leads are responsible for ensuring that all staff and contractors within their areas of responsibility adhere to this manual and identify and manage system related security risks including those to be escalated.

Regional Directors of Business Services are responsible for ensuring each site has relevant information available for patients to be aware of the Consent Management Protocol for Publishing to the MHR and the use of the appropriate form as well as the consent management protocol of any external contractor system uploading documents to the MHR.

The Responsible Officer (RO) has legal responsibility for WA health system compliance with the MHR legislation.

The Seed OMO with support of HSS is responsible for the implementation and compliance monitoring of the MHR requirements and for its maintenance including undertaking periodic privacy and security risk assessments of staff use of the MHR system and the organisation's ICT systems generally. The Seed OMO implements relevant improvements as required. HSS is responsible for all risk assessments being documented appropriately.

- The Seed OMO will maintain a copy of the authorised current and all previous versions of this manual and make them available on request by the System Operator.
- The Seed OMO is responsible for ensuring the accuracy of this MHR manual and its compliance with MHR legislation.
- The Seed OMO will ensure that the manual remains current and reflects changes in MHR legislation and in the structure of the organisation.
- The Seed OMO/RO will ensure that a copy of the organisation's MHR manual is made available to the System Operator within 7 days of receiving the request where this request has been made in writing.
- The Seed OMO/RO will ensure that the version of the MHR manual provided is the version of the organisation's manual that was in force on the dates specified by the System Operator in its written request.

11. Compliance

This manual is a mandatory requirement as part of the My Health Record Act 2012. Failure to comply with this policy document may constitute a breach of the WA Health Code of Conduct (Code). The Code is part of the Employment Policy Framework issued pursuant to section 26 of the *Health Services Act 2016* (HSA) and is binding on all WACHS staff which for this purpose includes trainees, students, volunteers, researchers, contractors for service (including all visiting health professionals and agency staff) and persons delivering training or education within WACHS.

WACHS staff are reminded that compliance with all policy documents is mandatory.

12. Records Management

Clinical/Health Record Management is directed by the Health Record Management Policy.

13. Evaluation

This manual is to be reviewed by the Program Manager, Health Information Management and Seed OMO every two (2) years.

14. Standards

National Safety and Quality Health Service Standards – 1.16, 1.17, 1.18

15. Legislation

My Health Records Act 2012 (MHR Act)
- My Health Records Regulation 2012
- My Health Records Rule 2016 and Explanatory Statement

Healthcare Identifiers Act 2010
- Healthcare Identifiers Regulation 2010

State Records Act 2000
Freedom of Information Act 1992 *(FOI Act)*

16. References

Health Identifier (HI) Service (Medicare)
My Health Record (MHR) System
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.

17. Related WA Health System Policies

MP 0094/18 My Health Record (MHR) Policy
- OD 0463/13 Personally Controlled Electronic Health Record (System) Policy (superseded)

MP 0066/17 Acceptable Use of Information and Communications Technology Policy
MP 0067/17 Information Security Policy
MP 015/16 Information Use and Disclosure Policy
OD 0589/15 WA Health Complaint Management Policy
MP 0031/16 WA Health Code of Conduct
MP 0040/16 Discipline Policy with Explanatory Notes and Template Letters

18. Policy Framework

Information and Communications Technology Policy Framework
Information Management Policy Framework

This document can be made available in alternative formats on request for a person with a disability

Contact:	Katherine Ivey		
Directorate:	Information Management and Technology	**EDRMS Record #**	ED-CO-19-50874
Version:	1.00	**Date Published:**	5 July 2019

This information is available in alternative formats for a person with a disability.