PROCEDURE DOCUMENT

ACT Government | ACT Health

Access and use of the National My Health Record System – Procedure

Document number	AHDPD-83:2021
Effective date	1/06/2022
Review date	1/06/2024
Author branch	Technology and Operations, Digital Solutions Division
Endorsed by	Executive Board
Audience	ACT Health Directorate
Version number	2.2

Contents

Purpose

This procedure provides information for Staff[1] accessing, using and uploading documents to the My Health Record (MHR) system in order that their actions comply with national legislative requirements, ACT legislative requirements, ACT Government and ACT Health Directorate (ACTHD) policy and best practice standards. This procedure describes the operating procedures required through the *Access and use of the My Health Record System Policy* (Policy).

The MHR contains clinical information contributed by healthcare provider organisations and individuals. Individuals and their registered healthcare providers can view and upload information in the MHR. The MHR supplements but does not replace detailed medical records and clinical records held and maintained by healthcare organisations and practitioners.

As more people use the MHR, Australia's national health system will become better connected. The result will be safer, faster, and more efficient care for healthcare consumers and their families.

Health care consumers can choose to share their information with the healthcare providers involved in their care. The uploading, viewing, and sharing of documents in the MHR will provide the treating team with a more detailed picture with which to make decisions, diagnoses and provide treatment.

Scope

This procedure applies to all staff using information systems managed and maintained by the ACTHD. This includes, but is not limited to, Canberra Health Services (CHS), Calvary Public Hospital Bruce (CPHB), Clare Holland House, Tresillian Queen Elizabeth II Family Centre, Digital and Data Technology Services (DDTS), students, contractors, and volunteers who, in their roles of delivering healthcare services, may access or upload documents to the MHR.

Only authorised and approved staff will have access to the MHR for the delivery and support of health care services.

ACT Health will comply with the My Health Record Act 2012 (MHR Act) in order to:

- Upload clinical documents to the MHR system; and
- Facilitate access to the MHR system through ACTHD managed information systems for the provision of healthcare to patients.

[1] This includes, but is not limited to the ACTHD, Canberra Health Services (CHS), Calvary Public Hospital Bruce (CPHB), Clare Holland House, Tresillian Queen Elizabeth II Family Centre, Digital and Data Technology Services (DDTS), students, contractors, and volunteers.

Roles and Responsibilities

Responsible Officer (RO)

In accordance with the MHR Act 2012 and the Healthcare Identifiers Act 2010 the ACTHD Chief Information Officer (CIO), as the RO, is responsible for:

- Compliance with the MHR legislation including the requirements of the MHR Act 2012, My Health Records Rules 2012, My Health Records Regulation 2012, 2015, 2016 Healthcare Identifiers Act 2010 and ACT Health Records (Privacy and Access) Act 1997;
- Acting on the behalf of the ACTHD in dealings with the MHR operator;
- Reporting all MHR access breaches, or possible access breaches, to the MHR system operator; and
- Ensuring the provision of appropriate resources to maintain policies, procedures supporting the ACTHD interaction and continued interactions with the MHR.

Organisation Maintenance Officer (OMO)

In accordance with the MHR Act 2012 and the Healthcare Identifiers Act 2010 the RO appoints Organisation Maintenance Officers (OMOs) that are responsible for the following interactions with the MHR system:

- Ensuring the accuracy and currency of the organisation's MHR policy and procedure and its compliance with MHR system legislation.
- Establishing and maintaining an accurate and up-to-date list of all staff who are authorised to access the MHR system on behalf of ACT Health via the Clinical Portal system;
- Establishing and maintaining an accurate and up-to-date list of all requests made by ACT Health to withhold information from a healthcare recipient's MHR;
- Co-ordination of all requests for amendment and removal of clinical documents submitted to the MHR system on behalf of the ACTHD;
- Co-ordinating responses to consumer queries, complaints, and requests in relation to access to the MHR and clinical documents uploaded by information systems operated by the ACTHD; and
- Investigating any unauthorised access to the MHR system and reporting to the Responsible Officer.

Managers and Supervisors

Managers and Supervisors at all levels are responsible for ensuring that the procedure for ACT Health's interactions with the MHR system is implemented in their area of responsibility.

This includes:

- Training new and existing personnel on their individual responsibilities to comply with the requirements of legislation, policies, and procedures; and

- Ensuring that access to the MHR system via the Clinical Portal is deactivated when a staff member leaves the organisation or has a change of role that no longer requires access to the MHR system.

All Staff

Are responsible for:

- Assisting consumers by answering general questions relating to the MHR;
- Ensuring that withdrawal of consent to upload information to the MHR is promptly recorded in ACTPAS by authorised users of ACTPAS;
- Promptly notifying the OMO or Digital Solutions Support where a request to withdraw consent for an individual has been notified;
- Access the MHR only if the access is required by the duties of their role;
- Keeping and maintaining full and accurate notes in the clinical record on any interaction with the MHR and where clinical information within the MHR is used for clinical decision making in the treatment of a patient;
- Ensure that privacy and confidentiality are always maintained by observing relevant policies and adhering to the requirements of the Public Sector Management Act 1994 and the ACT Health Records (Privacy and Access) Act 1997; and
- Report any unauthorised access breaches of the MHR system to an ACTHD OMO.

Digital Solutions Division Staff (DSD)

Are responsible for:

- Providing support and training to ACTHD, CHS and CPHB in the use of the MHR system via the Clinical Portal;
- Providing access to the Clinical Portal for staff to view the MHR for the purpose of providing healthcare services and revoking access where a staff member leaves the organisation or has moved to a role that no longer requires access;
- Providing level 1 help desk support for any application issues experienced by users relating to the use and access of the MHR;
- Ensure that the recording of the withdrawal of consent by a health care recipient is only recorded at the request of the health care recipient or their authorised representative;
- Promptly manage requests to assist with the withdrawal of consent to upload information to the MHR;
- Promptly notifying the Digital Solutions Service Desk or an ACTHD OMO where notification to withdraw consent, or to re-instate consent to upload to the MHR system for an individual has been received.

Procedure

All Staff accessing health records via ACTHD information systems need to familiarise themselves and undertake training in the use and access to clinical records that includes access and use of information held in the MHR system.

Patient Identification

The identity of the patient is to be established upon admission, referral, appointment booking or attendance. This will ensure that the patient's identity has been verified to enable the uploading of clinical documents to the MHR and the access and use of the MHR by staff directly involved in the delivery of health care services. The accurate identification of the healthcare recipient enables the retrieval and validation of the national Individual Healthcare Identifier (IHI) from the national Healthcare Identifiers Service.

Uploading Clinical Documents to the MHR

Clinical documents are uploaded to the MHR system where the patient has a MHR and has not withdrawn consent for ACTHD managed information systems to submit their information to the MHR. The upload of information is a fully automated process requiring no action from clinical or administrative staff.

Individuals may request at any time that they do not wish information uploaded to their MHR. This is required under the MHR Act 2012.

Where an individual does not want information uploaded to the MHR, staff are required to inform the individual that:

1. Withdrawal of consent will prevent the individual from having documents or reports uploaded to the MHR system created after the change has been made from ACT Health services.
2. At present it is not possible to restrict individual documents or document types from being uploaded to the MHR. Withdrawal of consent will prevent the uploading of ***all*** information from ACTHD information systems to the MHR.
3. The withdrawal of consent will only prevent the information systems operated and managed by ACTHD from uploading documents from the point that consent is updated in ACTPAS. Withdrawal of consent will not remove documents previously uploaded to the MHR.
4. Withdrawal of consent in ACTPAS will not prevent other healthcare providers or organisations from uploading clinical information to their MHR; and
5. Healthcare recipients may set individual controls to restrict who can access their information in their MHR. Individual controls include setting a record access code or flagging specific documents in their MHR as 'limited access' and controlling which health care organisations can view these documents.

Withdrawal of Consent to Send Health Information to the MHR System

Where a patient, or their authorised representative, advises they wish to withdraw consent to upload to the MHR, staff are required to:

1. Immediately update the individual's MHR consent status via the 'My Heath Record Consent' tab in ACTPAS;
2. Staff who do not have access to ACTPAS must immediately notify the ward clerk and request for the consent status to be amended. If a staff member with ACTPAS is not available to update the record in ACTPAS, staff should immediately contact Digital Solutions Support by calling x45000;
3. The patient is to be advised that their decision to withdraw consent can be revoked at any time by notifying ACT Health, CHS, or CPHB.
4. Where a patient advises that they wish to revoke previous advice to withdraw consent, staff are to follow the same procedure as above but leaving the status as "*Send documents to National My Health record*".

Amendment of a Clinical Record within the MHR

A clinical document uploaded to the MHR system will only be amended if the patient, their nominated representative, or a healthcare provider reports that information in a clinical document is incorrect.

The following steps must be followed to amend a document in the MHR:

1. Make a written request to amend a document in a healthcare recipient's MHR to the OMO and provide the document name, document number and patient's record number (URN) along with any supporting evidence that this document contains incorrect information.
2. The OMO will forward requests for the amendment of clinical records for investigation by the Health Information Service (HIS) at CHS and CPHB.
3. Where appropriate, the OMO will notify the document author and document approver and request that the document be amended based on advice supplied by the CHS HIS or CPHB HIS team.
4. The clinician who authored the original document will amend the document and inform both the responsible HIS and the OMO upon completion of the amendment.
5. The OMO will inform the person making the request in writing or email of the outcome of request.
6. The OMO will confirm with the version of the document has been successfully uploaded to the MHR.

Note: The MHR system does not accept amendments to a clinical document that has been uploaded. A new version of the clinical document must be created and submitted to the MHR system. The new version will be assigned a new version number to clearly denote that it is an amended version of the original document. Clinicians will have access to all versions of a document stored in a patient's MHR.

Removal of a Clinical Record from the MHR

Where it is identified that a record in the MHR needs to be removed this should be notified to the OMO. The OMO will gather the required information and contact the MHR operator to arrange the removal of the MHR document. Patients and their nominated representatives can also be advised to contact the MHR operator directly to have the document removed.

Accessing the MHR - Prerequisites

1. Staff members who access the MHR system must have completed Clinical Portal training and MHR system training prior to accessing the system. Training materials and reference guides are available on the ACTHD Digital Solutions Division intranet site. Training is also available to all staff through the HRIMS staff learning and development system.
2. Staff directly involved in the provision of health care to patients are authorised under Section 61 of the MHR Act 2012, to access a patient's MHR if:
    - The access is for the purpose of providing healthcare to the patient; and
    - Access is in accordance with the access controls set by the patient.
3. Access to a patient's MHR is through the Clinical Portal.
4. MHR information viewed from clinical information systems is not retained to ensure that viewing only occurs on current information held in the MHR.
5. Healthcare providers and other participants in the system are authorised to collect, use and disclose information in an individual's MHR for the purpose of providing an individual with healthcare. This must be done in line with the access controls the individual has set on their MHR.
6. There are some other specific circumstances where healthcare providers and other participants can collect, use, and disclose information in an individual's MHR.

    These circumstances are where it is:
    - For the management and operation of the MHR system;
    - To lessen or prevent a serious threat to an individual's life, health or safety or for public health and safety;
    - As required or authorised by law;
    - For purposes relating to the provision of indemnity cover to a healthcare provider;
    - As ordered by a court or tribunal;
    - Where deemed reasonably necessary for certain law enforcement purposes; and
    - Ethics Committee approval has allowed for the secondary use of de-identified MHR data for research or public health purposes.
7. Staff are authorised to access an individual's MHR for the purposes of providing healthcare. If no access controls are established, access to the MHR is unrestricted.
8. Access to a MHR can be restricted by access controls established by the healthcare recipient or an authorised representative. Where an individual has restricted access to their MHR, the healthcare recipient, or their authorised representative, will provide a clinician with the access code if they wish to allow the clinician to view their MHR.
9. Where an individual does not or cannot provide an access code to their MHR, access can be only be gained through invoking emergency access (EA).

10. Where there is a mismatch in demographic data between data sourced from a MHR and data stored locally, the clinician is alerted by the Clinical Portal. The clinician is required to clarify the mismatched information and content of the record with the patient to confirm that the information on the clinical document sourced from a MHR is associated with the patient.
11. Any breach of the Policy or this procedure, could constitute alleged misconduct. The relevant Enterprise Agreements and misconduct policies and procedures contain the processes for managing these instances.

Accessing MHR at CPHB and CHS

CPHB is registered as a separate organisation to CHS in the national Health Identifier service.

A clinician who works for CPHB will access the MHR in the following manner:

- Where the clinician is providing clinical treatment to a patient on behalf of CPHB, they must logon to the Clinical Portal with their defined CPHB username and password in order to access the MHR from the CPHB location.

- Where the clinician is providing clinical treatment to a patient on behalf of CHS, they must logon to the Clinical Portal with their defined CHS username and password in order to access the MHR on behalf of CHS.

Access Controls

Default Setting

The default state upon creation of an individual's MHR is that there are no access controls restricting access to the entire record, documents within the record, or any healthcare organisations attempting to access the record. The vast majority of individual MHRs will have no access controls set. A health care recipient, or their nominated representative can set access restrictions on their MHR.

No Access Request

Where a healthcare recipient or a nominated representative requests that a MHR should not be accessed, the healthcare recipient or nominated representative is to be advised that they will need to set access controls via the MHR Consumer Portal through their MyGov (https://my.gov.au) portal access. If the healthcare recipient or nominated representative has not set access controls the record will be available for access via the Clinical Portal without any restrictions.

Accessing a Record with Access Controls

A healthcare recipient can choose to restrict access to their MHR by applying access controls to the entire record, to particular documents in their record, or prevent specified healthcare organisations from accessing their record. Access controls are managed directly by the patient or nominated representative via the MHR Consumer Portal system. Access to a MHR with secured access controls is in accordance with the access controls established by the patient.

A clinician can access a patient's MHR secured by access controls if the patient provides the access code. Once access has been granted by the patient the record will continue to be viewable by Staff without further need to enter access codes for five days.

There are provisions under the MHR Act 2021 to override access controls by invoking EA under very specific conditions.

Types of Access Controls and their Use

Record Access Code (RAC)

A patient can secure access to their MHR by placing a RAC on their record (effectively a PIN or a password) with which they can control which providers are able to access their record. A patient can provide the RAC to a clinician in order to access and view the patient's MHR.

When a patient provides a RAC to a healthcare provider, the provider is only required to enter the RAC the first time they access the patient's MHR. It is not necessary to re-enter the RAC each time the provider accesses the MHR. The providers' organisation will be added to the approved provider access list on the patient's MHR. The patient may subsequently remove the organisation from the access list by revoking permission if they wish.

Limited Document Access Code (LDAC)

A patient can secure documents in their MHR by placing a code on specified documents (effectively a PIN or a password) with which they can control access to specified documents. A patient may provide the access code to a clinician in order to access and view any documents secured by a document code. A clinician will only know if a patient has documents secured by document codes if the patient informs the clinician of their existence as these documents will be hidden from view until the code is entered.

Revoked Access

A patient can prevent access to their MHR for one or many healthcare organisations. A provider acting on behalf of an organisation that has had their access revoked will not be able to access a patient's MHR unless EA provisions are invoked.

Access Codes Not Provided

Where a patient does not or cannot provide an access code to their MHR, access can only be gained through invoking EA.

Emergency Access

The MHR Act 2012 makes provision for access to an individual's MHR that is secured by access controls by overriding those access controls using EA where CHS and CPHB are participants in the MHR system, reasonably believes that:

i. The collection, use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety; or

ii. The collection, use or disclosure is necessary to lessen or prevent a serious threat to public health or public safety; and

iii. It is unreasonable or impracticable to obtain patient consent to the collection, use or disclosure; and

iv. The collection, use or disclosure occurs no later than 5 days after that advice is given.

Invoking Emergency Access

EA to a MHR that is secured by access controls can only be invoked for the purpose of providing healthcare where:

1. The patient is unwilling or unable to provide the access code and the clinician determines that access to the patient's record is required to lessen or prevent a serious threat to an individual's life, health or safety or a serious threat to public health or public safety;
2. The patient provides consent for the clinician to invoke EA because the individual cannot provide the access code at the time that access is required to lessen or prevent a serious threat to the individual's life, health or safety or a serious threat to public health or public safety.

The system automatically provides privacy warnings and informs the person invoking EA that the healthcare recipient will be informed that EA has been invoked. The clinical staff member invoking EA will have to enter a reason and the MHR system log will retain an audit trail of all EA requests; and

Where EA has been invoked access an individual's MHR will continue to be available for five days.

Documenting Emergency Access

The clinician invoking EA to a MHR must:

- Record the EA reason in the Clinical Portal system from the drop-down menu when EA is invoked; and

- Record in the progress notes of the patient's clinical record relevant details of the threat to public health or safety or threat to an individual's life, health or safety that has required the clinician to invoke EA.

Records Management

The records generated from the requirements for the OMOs to investigate, report and audit the access and use of the MHR by staff as described in this procedure are to be documented and sent to the RO for review and endorsement. All records must be managed in accordance with the *Territory Records Act 2002* and relevant policies and procedures.

Implementation Principles

1. All Australian citizens have a MHR unless they have withdrawn or cancelled their MHR with the MHR system operator. It is implied that a citizen agrees to their information being uploaded to the MHR system as part of the delivery of health services.

2. Clinical information is uploaded to the MHR system as an automated process based on healthcare recipient consent. Examples of patient information presently uploaded to the MHR are discharge summaries, pathology reports and diagnostic imaging reports.

3. Unless a healthcare recipient has advised that they do not wish information to be uploaded to the MHR system, their documents will be uploaded to the MHR system.

4. When a healthcare recipient advises the ACTHD, CHS or CPHB that they do not wish information to be sent to the MHR, the decision is to be recorded in the ACTPAS to ensure that information is no longer uploaded to the MHR system.

5. Where a healthcare recipient requests that information is to be sent to the MHR system, the automatic upload process will involve confirmation that consent to upload is recorded in the ACTPAS.

6. Historical clinical documents are not uploaded to the MHR.

7. Where a clinical document has failed to upload, ACTHD will make reasonable attempts to resend/upload that document to the MHR system.

   Finalised documents cannot be uploaded to the MHR system where:

   a. The healthcare recipient has withdrawn consent for clinical information to be uploaded to their MHR; or

   b. The healthcare recipient was not registered for a MHR at the time the clinical document was finalised; or

   c. The healthcare recipient identification does not match the identification of the individual in the national Healthcare Identifiers service.

References and Related Documents

Legislation

- *My Health Records Act 2012*
- *My Health Records Rules 2012, 2015, 2016*
- *My Health Records Regulation 2012*
- *Healthcare Identifier Act 2010*
- ACT *Health Records (Privacy and Access) Act* 1997
- *Territory Records Act 2002*

Relevant Policies and Procedures

- *ACT Government Acceptable Use Policy*
- *Clinical Records Management Policy*
- *Patient Identification Policy*
- *Access and use of the My Health Record System Policy*
- *National Safety and Quality Health Care (NSQHS) Standards*

Additional References

1. **My Health Record.** https://www.myhealthrecord.gov.au/
2. ***Top 10 tips for effective use of electronic health records***
   Wuerth, Rey ; Campbell, Catherine ; King, W
   Paediatrics & Child Health, Mar 2014, Vol.19(3), p.138
3. ***Best Practices: The Electronic Medical Record Is an Invaluable Clinical Tool: Let's Start Using It***
   Vrieze, Scott I ; Docherty, Anna ; Thuras, Paul ; Arbisi, Paul ; Iacono, William G ; Sponheim, Scott ; Erbes, Christopher R ; Siegel, Wayne ; Leskela, Jennie
   Psychiatric Services, October 2013, Vol.64(10), pp.946-949
4. **Electronic Health Record (EHR) As a Vehicle for Successful Health Care Best Practice**
   Ghazisaeedi, Marjan ; Mohammadzadeh, Niloofar ; Safdari, Reza
   Medical Archives, 2014, Vol.68(6), p.419-421

Definitions

Term	Definition
Access Control	Provides patients with the capability to control access to their My Health Record (MHR). MHR access controls can consist of password protecting the entire record or specified documents within a patient record or excluding specified healthcare organisations from accessing a MHR.
Authorised Staff	Staff that are members of treating teams providing clinical treatments and services to patients. This group includes doctors, nurses, nurse practitioners, midwives, pharmacists, allied health professionals, allied health assistants, students, contractors, and volunteers.
Confidentiality	Is the assurance that written and spoken information is protected from access and use by unauthorised persons. With respect to confidentiality, ACT Health Directorate (ACTHD) staff members are to refer to the Public Sector Management Act 1994 (ACT) and are to note that disclosure or misuse of confidential information held in official records is illegal.
Emergency Access (EA)	Emergency access to a national My Health Record (MHR) is provided in the *My Health Records Act 2012* to allow a healthcare provider to access a record by overriding patient access controls in specific circumstances detailed in the My Health Records Act 2012.
Healthcare Identifier Service (HI Service)	Is the national repository for healthcare organisation and healthcare provider identifiers maintained by Medicare Australia. Healthcare organisations are able to access the Healthcare Identifier service to obtain and validate provider and provider organisation identifiers for use in MHR interactions and in provider-to-provider communication.
Clinical Document	May be one of the following: • Discharge Summary • Dispense Record • Medicare Benefits Scheme Benefits • DVA Benefits • Advanced Care Directives • Advanced Care Custodian Notes • Pathology Reports • Diagnostic Imaging Reports • eHealth Prescription Summary • ePrescription • Prescription Request • Shared Health Summaries • Australian Organ Donor Register • Specialist Letter • eReferral

	• Australian Childhood Immunization Records • HPV Immunization Records • Medicines View • Event Summary • Pharmacist Shared Medicines List (PSML)
Organisation Maintenance Officer (OMO)	One or many employees who act on behalf of a healthcare organisation that have specific defined responsibilities detailed in the Access and Use of the National My Health Record System policy and the Access and use of the My Health Record System procedure.
My Health Record system (MHR)	The MHR is a national electronic health record for all Australian residents that is comprised of clinical information contributed by healthcare providers, Medicare Australia and individuals throughout Australia. The MHR is available for access by healthcare providers for the purpose of providing healthcare services to patients. Access to MHR records is controlled by the individual or their authorised representatives.
Patient	Refers to *patients, consumers, individuals, recipients of healthcare* and *clients* that have been or currently are receiving healthcare services.
Provider Portal	Means the portal system provided by the system operator that permits registered healthcare provider organisations to access the MHR.
Responsible Officer (RO)	A senior officer who acts on behalf of ACT Health Directorate in its dealings with the My Health Record service operator with regards to specific responsibilities detailed in the My Health Records Act 2012.
System Operator	The Australian Digital Health Agency is the System Operator of the My Health Record system

Search Terms

My Health Record, MHR, Responsible Officer, RO, Organisational Maintenance Officer, OMO, Emergency Access, EA.

Version Control

Version	Date	Comments
Draft 0.1	19/09/2020	
Draft 1.0	14/09/2021	
Draft 2.0	20/10/2021	
Draft 2.1	07/02/2022	
Final 2.2	10/05/2022	

Disclaimer: *This document has been developed by the ACT Health Directorate specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at his or her own risk and the ACT Health Directorate assumes no responsibility whatsoever.*