ACT Government | ACT Health

POLICY DOCUMENT

Access and Use of the National My Health Record System - Policy

Document number	AHDPD-82:2021
Effective date	2 June 2022
Review date	1 June 2024
Author branch	Technology and Operations, Digital Solutions Division
Endorsed by	Executive Board
Audience	ACT Health Directorate
Version number	2.2

Contents

Policy Statement

Access to the national My Health Record system (MHR) is available through information systems supported and maintained by the ACT Health Directorate (ACTHD). The ACTHD must ensure that users of these information systems are appropriately authorised and comply with relevant Australian Government and Australian Capital Territory legislations and policies.

This policy outlines the requirements, responsibilities, and conditions to access and use the MHR. Included in this policy are the requirements for staff supporting the information systems used to access the MHR. The MHR operator is Australian Digital Health Agency (Agency).

Purpose

Staff[1] using information systems maintained and supported by the ACTHD are authorised under Section 61 of the My Health Record Act 2012 (MHR Act), to access a national MHR record if access is:

- For the purpose of providing healthcare to a patient, and
- In accordance with the access controls set by the patient.

Through participation in the MHR, authorised staff using information systems supported by the ACTHD can invoke emergency access (EA) provisions (under the MHR Act) to override access controls set by the patient, only in circumstances where:

(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.

The purpose of this policy is to ensure that the access and use of the MHR complies with ACT Government policies and relevant legislation while supporting the timely access to health information to support safety and quality in the delivery of health care services.

Access to the MHR by authorised staff is typically for viewing only and where staff print or otherwise capture information from the MHR, staff are to ensure that the information remains secure and confidential in accordance with ACT Government policies and relevant legislation. There is also a responsibility of staff accessing and using the MHR to ensure that information contained in the MHR is accurate and appropriate and that confidentiality and privacy are maintained.

[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, Data and Technology Services (DDTS), students, contractors, and volunteers.

Scope

The Access and Use of the national MHR policy applies to all users of information systems supported and maintained by the ACTHD to access and use the MHR in the performance of their duties. This includes, but is not limited to ACTHD, Canberra Health Services (CHS), Calvary Public Hospital Bruce (CPHB), Clare Holland House, Tresillian Queen Elizabeth II Family Centre, Digital and Data Technical Services (DDTS), students, contractors, and volunteers.

The access and use of the MHR by accredited public hospitals is a requirement under the National Safety and Quality Health Care (NSQHS) Standards (Standard 1).

Roles and Responsibilities

Responsible Officer

In accordance with the MHR Act and the Healthcare Identifiers Act 2010 (HI Act), the Chief Information Officer (CIO), ACTHD Digital Solutions Division as the Responsible Officer is responsible for:

- Compliance with the national MHR legislation including the requirements of the MHR Act, My Health Records Rule 2016 (MHR Rule), My Health Records Regulation 2012(MHR Regulation), HI Act, the ACT legislation, and the Health Records (Privacy and Access) Act 1997.
- Acting on behalf of the ACTHD in dealing with the MHR operator; and the Office of the Australian Information Commissioner (OAIC).
- Reporting all MHR access breaches or possible access breaches to the MHR operator.
- Where required, refer matters relating to the use and access of the MHR to ROs at other organisations such as Calvary Healthcare ACT who provided contracted services to the ACT Government at the CPHB and Clare Holland House.
- Ensuring the provision of appropriate resources to maintain policies, procedures supporting the ACTHD interaction and continued interactions with the MHR.

Organisation Maintenance Officer

The Organisation Maintenance Officer (OMO) is responsible for the management of ACTHD interactions with the MHR. This includes:

- Ensuring the accuracy of the organisation's MHR policies and procedures and their compliance with MHR legislation and ensuring that the policy remains current and reflects any changes to MHR legislation.
- Establishing and maintaining an accurate and up-to-date list of all staff who are authorised to access the MHR via the Clinical Portal system; and
- Investigating any unauthorised access to the MHR and reporting to the RO.

Authorised Staff

All authorised staff are responsible for:

- Keeping and maintaining full and accurate notes in the clinical record on any interaction with the MHR where clinical information within the MHR is used for clinical decision making.
- Reporting all suspected or alleged access breaches to the MHR to their supervisor, the Digital Solutions Service Desk, Responsible Officer or Organisation Maintenance Officer.
- Ensuring that privacy and confidentiality are maintained at all times 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
- Seeking approval through the ACTHD ethics and research approval process for the use of information in MHR for research and quality assurance activities.

Note: ACTHD staff are not permitted to access their own MHR using ACTHD information systems.

Requirements

All Staff accessing patient health records using ACTHD information systems need to complete mandatory training in the use and access of patient clinical records including the use and access of the MHR.

The ACTHD will comply with the My Health Record Act 2012 (MHR Act) in order to;

- Upload clinical documents to the MHR; and
- Facilitate access by ACTHD staff to the MHR in the provision of healthcare to patients.

Key Principles

Uploading Clinical Documents to the MHR

- All Australian citizens have an MHR unless they have withdrawn or cancelled their MHR with the System operator (the Agency). It is implied that a citizen agrees to their information being uploaded to the MHR as part of the delivery of health services.
- ACTHD managed information systems will upload patient information to the MHR as an automated process based on patient consent as agreed and required by health services. Patient information currently uploaded to the MHR includes discharge summaries, pathology reports and diagnostic imaging reports.
- Unless a patient has advised that they do not wish information to be uploaded to the MHR, documents will be uploaded to the MHR.
- When a patient advises that they do not wish information to be sent to the MHR that decision is to be updated through the My Health Record Consent tab in the ACT Patient Administration System (ACTPAS) to ensure that information is no longer uploaded to the MHR.
- Where a patient requests that information to be sent to the MHR, staff are to confirm that the setting of consent is set correctly within the My Health Record Consent tab in ACTPAS.
- Historical clinical documents are not uploaded to the MHR.
- Where a clinical document has failed to upload, ACTHD will make reasonable attempts to resend/upload that document to the MHR.
- Finalised documents cannot be uploaded to the MHR where:

- The patient has withdrawn consent for clinical information to be uploaded to their MHR; or
- A patient was not registered for a national MHR at the time the clinical document was finalised; or
- The patient identification does not match the identification of the patient in the national Healthcare Identifiers service (HI Service).

Accessing the MHR system

Healthcare providers and other participants in the MHR system are authorised to collect, use and disclose information in a patient's MHR for the purpose of providing the individual with healthcare. This must be done in line with the access controls the patient has set.

Other specific circumstances where healthcare providers and other participants can collect, use and disclose information in an individual's MHR are:

- For the management and operation of the MHR;
- 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.

Accessing a MHR where no access control is set by a patient

Staff are authorised to access a patient's MHR via the Clinical Portal for the purposes of providing healthcare. If no access controls are established, access to an MHR is unrestricted.

Accessing a MHR where access controls have been set

Access to a MHR can be restricted by access controls established by a patient. Where a patient has restricted access to their MHR, the patient or their authorised representative will provide a clinician with the access code if they wish to allow the clinician to view their MHR.

Where an individual does not or cannot provide an access code to their MHR, access can only be gained through invoking Emergency Access (EA).

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 patient cannot provide the access code at the time that access is required.
3. Use of the EA function that is not authorised by section 64 of the My Health Records Act 2012 (MHR Act) is subject to civil and/or criminal penalties under the MHR Act.
4. Once granted, EA to a record is available for a maximum of five days. When this period ends, the MHR reverts to the previous settings. If the emergency situation continues beyond the initial five-day period, the treating healthcare provider will need to request EA again.
5. Use of the EA function is recorded in the access history of the MHR, which can be viewed by the patient and their authorised or nominated representative(s). In addition, patients can choose to receive an SMS or email notification each time the EA function is used to view their MHR.
6. With EA, any access controls that the individual has set will be overridden. The healthcare provider who uses the EA function will have full access to the patient's MHR, except for information that has been entered in the personal health notes section of the record, and any documents the patient (or their authorised representative(s) has previously removed or hidden.

Documenting Emergency Access

Staff invoking EA are required to record details in patient notes that EA to the MHR has been gained and document the reason for access.

It is important to note that registered healthcare provider organisations are subject to reporting obligations under Section 75 of the Act. Consequently, unauthorised use of the EA function may be reportable to the OAIC Australian Digital Health Agency (Agency), as System Operator.

The ACTHD OMOs conduct audits for all instances of EA and report finding to the ACTHD Responsible Officer and, when indicated, to the OAIC and the Agency, as System Operator.

Validating individual information in the national MHR

Where there is a mismatch in demographic data between data sourced from a national 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 national MHR is associated with the patient.

When it is identified that information in the MHR is incorrect this should be reported to the OMO or the System Operator for amendment or removal as indicated.

Breach of policy

Any breach of this policy or the Access and use of the MHR Procedure (Procedure), could constitute alleged misconduct. The relevant Enterprise Agreements and misconduct policies and procedures contain the processes for managing these instances.

Records Management

The records generated through this policy and associated procedure as a result of audit and investigations by the RO, OMOs and ACTHD Staff are to be actioned and endorsed by the RO and managed in accordance with the *Territory Records Act 2002* and ACTHD policy and procedures.

Evaluation

Outcome Measures	Method	Responsibility
What will be measured to determine achievement – has the policy purpose occurred?	**How will this be done?**	**Who is responsible for evaluation?**
Staff must only access national MHR for the purpose of providing health care.	All enquiries regarding staff access to national MHR by patients or the system operator will be investigated by the OMO to ensure compliance with this policy.	OMOs or others as requested by the RO.
Clinical information uploaded to the national MHR is uploaded based on patient consent.	All enquiries regarding the upload of information to the national MHR through ACTHD managed applications will be investigated by the OMO to ensure compliance with this policy.	OMOs others as requested by the RO.
Access and use figures for the MHR are regularly monitored.	Access and usage data is provided to the ACTHD on the number of uploads and views by CHS, CPHB. Data includes the numbers of uploads for each document type uploaded in the reporting period	The Australian Digital Health Agency provides monthly reports to the ACTHD.
ACTHD will audit every instance where emergency access (EA) is invoked.	ACTHD OMO conducts and audit of each instance and report finding to the RO.	ACTHD OMOs

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 Procedure
- 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 national 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.