**My Health Record Security and Access Policy**

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

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

1. **PURPOSE**

* To provide guidance for staff and contractors about access to, and use of, the My Health Record system.
* To provide guidance in the use of information technology in [name of organisation] as it relates to the My Health Record system.
* To outline the roles and responsibilities of the Responsible Officer and the Organisation Maintenance Officer in relation to the My Health Record system.

1. **SCOPE OF POLICY**

This policy applies to all staff (including its employees and any healthcare provider to whom [name of organisation] supplies services under contract) with access to the My Health Record system.

1. **RELATED DOCUMENTS/LINKS**

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

[*My Health Records Act 2012*](https://www.comlaw.gov.au/Details/C2015C00602/Html/Text)

[*My Health Records Rule 2016*](https://www.comlaw.gov.au/Details/F2016L00095)

[*My Health Records Regulation 2012*](https://www.comlaw.gov.au/Details/F2016C00093)

[*My Health Records (Assisted Registration) Rule 2015*](https://www.comlaw.gov.au/Details/F2015L02055)

[*Healthcare Identifiers Act 2010*](https://www.comlaw.gov.au/Details/C2016C00091/Html/Text)

1. **DEFINITIONS**

* ***Access flag*** means an information technology mechanism made available by the System Operator to define access to a consumer’s digital health record.
* ***HI Service*** is the ‘Healthcare Identifiers Service’, a national system for uniquely identifying healthcare providers and individuals, which makes sure the right health information is associated with the right individual.
* ***Information Commissioner*** is the Office of the Australian Information Commissioner (OAIC).
* ***Network*** means a network of healthcare provider organisations created and managed in accordance with subsections 9A (3) to (6) of the *Healthcare Identifiers Act 2010*.
* ***Network organisation*** is a healthcare provider organisation which is part of a Network and is subordinate to a Seed Organisation; it can be used to represent different departments, sections or divisions within an organisation or can be separate legal entities from the Seed Organisation.
* ***Organisation maintenance officer (OMO)*** has the same meaning as in the *Healthcare Identifiers Act 2010*.
* ***Provider portal*** means the portal provided by the System Operator that allows for identified healthcare providers from participating healthcare provider organisations to access the My Health Record system without having to use a conformant clinical information system.
* ***Responsible officer (RO)*** has the same meaning as in the *Healthcare Identifiers Act 2010*.
* ***Seed organisation*** is a healthcare provider organisation which provides or controls the delivery of healthcare services; in a Network, the Seed Organisation is the principal entity in the Network.
* ***System Operator*** is the Australian Digital Health Agency.

1. **ORGANISATION STRUCTURE, ROLES AND RESPONSIBILITIES**

**ORGANISATION STRUCTURE**

All healthcare providers and organisations wishing to participate in the My Health Record system must first be registered with the HI Service. Healthcare provider organisations will usually participate in the My Health Record system as a ‘Seed Organisation’ only. However, in large or complex organisations, there may be a network made up of a Seed Organisation and one or more ‘Network Organisations’ that is part of or subordinate to the Seed Organisation.

[name of organisation] is registered in the HI Service as a: [insert ‘Seed Organisation’ or ‘Network Organisation’]

**MY HEALTH RECORD SYSTEM ROLES**

The My Health Record system requires people to be assigned to key roles, which authorises them to carry out certain actions in relation to [name of organisation]’s access to, and use of, the system. These roles are set out below:

* *Responsible Officer (RO)*: the RO is an employee of the Seed Organisation and has the authority to act on behalf of the Seed Organisation (and any Network Organisations) in its dealings with the System Operator. The RO has primary responsibility for an organisation’s compliance with participation requirements in the My Health Record system.  
    
  The RO for [name of organisation] is: [name of RO]
* *Organisation Maintenance Officer (OMO)*: the OMO is an employee of a healthcare provider organisation that is a Seed Organisation, or a Network Organisation. The OMO’s primary role is to undertake the day to day administrative tasks in relation to the My Health Record system. A healthcare provider organisation can have multiple OMOs.   
    
  The OMO for [name of organisation] is: [name/s of OMO]

**KEEPING INFORMATION ABOUT THE ORGANISATION UP-TO-DATE**

If [name of organisation] becomes aware that information held by the HI Service or the My Health Record system in relation to [name of organisation] is not accurate, up-to-date and complete, the RO or OMO must provide an update to the HI Service and/or System Operator in writing of the correct information. This shall be provided within 20 days of [name of organisation] becoming aware that the information held is not accurate, up-to-date and complete.

**NETWORK OBLIGATIONS: ACCESS FLAGS/LINKAGES**

*ACCESS FLAGS*

Where [name of organisation] is part of a Network, it is a requirement that appropriate Access Flags are set and maintained. Access Flags must be set in a way that balances:

* reasonable expectations of patients about the sharing of their healthcare information; and
* existing arrangements within the Network for the collection and sharing of healthcare information.

It is the responsibility of the RO and/or the OMO of the Seed Organisation to set appropriate Access Flags. The RO and/or the OMO of the Seed Organisation will undertake reviews of the Network 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. [name of organisation] commits to making reasonable changes in line with requests from the System Operator.

*LINKAGES*

Where [name of organisation] is part of a Network, the RO and/or the OMO of the Seed Organisation will establish and maintain an up-to-date record with the System Operator, which details the linkages between organisations in the Network.

1. **ACCESS AND USE OF THE MY HEALTH RECORD SYSTEM**

**AUTHORISING ACCESS TO THE MY HEALTH RECORD SYSTEM**

Organisational staff must only access the My Health Record system if this access is required by the duties of their role.

All staff members whose role requires them to access the My Health Record system will be provided a unique user account with individual login name. [name of organisation] will maintain records linking user accounts to individual staff so that these can be matched in the case of an audit by the System Operator. [name of organisation] will maintain records (for example staff rostering records) to allow it to determine which user accessed the My Health Record system on a particular day. These records must be maintained to allow audits to be conducted by the System Operator.

User accounts will not be used by multiple staff members.

It is the responsibility of the OMO to:

* Provide a unique user account with individual login name for each authorised user; and
* Immediately suspend or deactivate individual user accounts in cases where a user:
* leaves [name of organisation]
* has the security of their account compromised
* has a change of duties so that they no longer require access to the My Health Record system

**STAFF PASSWORDS/LOGGING OUT**

Staff will ensure that they assign a secure password to their user account and keep their password secret. Staff must regularly review and change their password.

All staff who have access to the My Health Record system will ensure that they log out of the system when they are not using it to prevent unauthorised access.

**IDENTIFYING STAFF WHO ACCESS THE MY HEALTH RECORD SYSTEM**

*Provider Portal*

Where healthcare providers in [name of organisation] access the My Health Record system on behalf of [name of organisation] via the national Provider Portal, the OMO will establish and maintain an accurate and up-to-date list of healthcare providers with the System Operator who are authorised to access the Provider Portal. If an individual healthcare provider is no longer authorised to access the provider portal on behalf of [name of organisation], the OMO will ensure the System Operator is informed and the individual removed from the list of authorised users.

*Conformant Software*

Where healthcare providers in [name of organisation] access the My Health Record system on behalf of [name of organisation] via conformant clinical software, the OMO will maintain a record of authorised Healthcare Provider Identifier – Individual (HPI-I) numbers in the clinical software and in [name of organisation]’s internal records.

The clinical software will be used to assign and record unique internal staff member identification codes. This unique identification code will be recorded by the clinical software against any My Health Record system access.

**STAFF TRAINING**[name of organisation] has a formal training program where all staff with authorisation to access the My Health Record system on behalf of [name of organisation] are required to undertake regular and ongoing privacy and My Health Record system training.

Existing staff will undertake My Health Record system training before they first access the system, while new staff will be required to undertake training, if appropriate to their role, as part of their orientation to [name of organisation]. If any new functionality is introduced into the system, additional training will be provided to all staff with authorised access to the My Health Record system.

Staff training will provide information about how to use [name of organisation]’s clinical software, and/or the national Provider Portal, in order to access the My Health Record system accurately and responsibly. Staff training will consist of training materials made available by the System Operator or other materials that [name of organisation] deems relevant, and training specific to the clinical software used by [name of organisation]. Training will also cover the legal obligations on healthcare provider organisations and individuals using the My Health Record system and the consequences of breaching these obligations.

The OMO will oversee a register of staff training as it relates to the My Health Record system, including the names or those who have completed training and the date on which training was completed.

1. **SECURITY AND PRIVACY PROCEDURES**

**MITIGATION STRATEGIES**

To ensure that My Health Record system related security risks can be promptly identified, acted upon and reported to [name of organisation], [name of organisation] will:

* Regularly review its security and procedures for accessing the My Health Record system, and report the findings to management and revise procedures accordingly;
* Establish a risk reporting procedure to allow staff to inform management regarding any suspected security issue or breach of the system; and
* Consider, and where appropriate, conduct a risk assessment into its ICT systems that examine privacy and security risks, and to conduct this assessment on a regular basis.

**REPORTING SECURITY BREACHES**

A security breach is when there is an unauthorised collection, use or disclosure of health information included in a patient’s digital health record, an example of which is when a staff member with access to the My Health Record system discovers that someone else may have gained access to their user account.

If any staff member becomes aware of a security breach, including where their user account has been compromised or that someone has used their computer to gain unauthorised access to the My Health Record system, they are immediately to inform their manager, who in turn is required to inform the RO or OMO. If only the OMO is informed, it is the OMO’s responsibility to ensure that the RO is made aware of the issue.

The RO or OMO will create a log entry of the breach including details of the date and time of the breach, the user account that was involved in the unauthorised access, and which patient’s information was accessed (where known).

The OMO will also undertake appropriate mitigation strategies, including, but not limited to:

* Suspending/deactivating the user account
* Changing the password information for the account

The RO or OMO is required to report a data breach to the System Operator (ph. 1800 723 471) and the Information Commissioner (ph. 1300 363 992) as soon as practicable after becoming aware that the following has, or may have, occurred:

* an unauthorised collection, use or disclosure of health information included in a healthcare recipient’s My Health Record, or
* the security or integrity of the My Health Record system has, or may have, been compromised by an event or circumstance.

**PATIENT DOCUMENT AND RECORD CODES**

Patients have the ability to set a number of privacy controls on their digital health record. A patient can set a code that restricts access to providers for certain documents contained within their record, they can also set a different code that restricts access to providers to their entire record.

Where a patient of [name of organisation] provides a My Health Record document or record code to unlock their record, the code must not be retained or recorded in the local patient record by staff, and must be disposed of (if for example it is written on paper) securely.

**RESPONDING TO PATIENT COMPLAINTS**[name of organisation] will make patients aware of the process for raising issues or complaints and will log any issues of which they are made aware.

If a patient raises an issue in relation to unauthorised access to their digital health record, [name of organisation] shall take steps to investigate the issue. Unauthorised access should be managed through [name of organisation]’s existing privacy complaint management processes and privacy policy.

Where a patient asks [name of organisation] to remove or amend a clinical document, and the medical practitioner agrees, the healthcare provider shall take steps to amend or remove the document as soon as possible.

In cases where there is disagreement between the medical practitioner and the patient about amendments to a clinical document, and the provider does not consider an amendment to be appropriate, then the provider may choose to remove the document. If the provider does not consider the removal of the document to be appropriate, then the provider should discuss this with the patient and where relevant direct the consumer to exercise their personal controls over the document.

**\*\*\* *Assisted Registration is voluntary for organisations. If your organisation does not provide Assisted Registration, please delete this note as well as the below section 8 and Appendix A before finalising this policy*.\*\*\***

1. **ASSISTED REGISTRATION**

Assisted Registration is a way for organisations to help patients register for the My Health Record system at the point of care. Assisted Registration is voluntary for organisations. Where [name of organisation] provides Assisted Registration, it will follow the below policy and procedures in registering a patient for the My Health Record system.

**AUTHORISING EMPLOYEES TO UNDERTAKE ASSISTED REGISTRATION**Only staff who have undergone training in Assisted Registration, and who have been authorised to perform Assisted Registration, may assist a patient to register for the My Health Record system.

The OMO will maintain an up-to-date list of staff who are authorised to undertake Assisted Registration on behalf of [name of organisation].

**EMPLOYEE TRAINING**Training will be provided to all staff who will be involved in Assisted Registration prior to undertaking Assisted Registration of a patient. The date of completion of the training will be recorded by the OMO in the staff training register.

Training will include information on:

* The process of undertaking Assisted Registration;
* The software that is used to undertake Assisted Registration (i.e. the Assisted Registration Tool or equivalent software);
* The handling of Identity Verification Codes (IVC); and
* How a patient will be identified.

**CONFIRMING THE CONSENT OF THE PATIENT**

[name of organisation] is required to obtain the consent of the patient to:

* register with the My Health Record system; and
* healthcare organisations uploading to the My Health Record system any record that includes health information about the patient.

*\*\*\* The organisation must choose one of the following options below on how the organisation will obtain the patient’s consent. Please delete this note and whichever option below is irrelevant before finalising this policy\*\*\**

[**OPTION 1**]  
[name of organisation] will first provide the patient with the *Assisted Registration Essential Information* and then obtain the consent of the patient by seeking verbal agreement from the patient that they consent to be registered with the My Health Record system and to upload documents to the My Health Record system. This agreement will be recorded in the patient’s electronic medical record in the clinical information system at the time when Assisted Registration takes place.

[**OPTION 2**]

[name of organisation] will first provide the patient with the *Assisted Registration Essential Information* and then obtain the consent of the patient by having the patient complete the *Assisted Registration – Application to Register for a My Health Record* which records the consumer’s consent to register with the My Health Record system and to upload documents to the My Health Record system. The signed Application should be securely disposed of, or where [name of organisation] chooses to retain a copy of the Application it will be:

* scanned and attached to the patient’s electronic medical record in the clinical information system (and then the original paper form will be securely disposed of); OR
* stored in a secure location and in line with [name of organisation]’s record retention polices.

**PATIENT IDENTIFICATION**

The following are the processes to be used in identifying a patient for the purpose of Assisted Registration, and the types of matters to be considered by staff before being satisfied of the patient’s identity.

It is essential that the patient is correctly identified. [name of organisation] will do this by one of the following:

* patient presents for a consultation and has presented on at least three occasions (inclusive of the presentation at which Assisted Registration is being provided) and the Medicare or DVA card is sighted;
* by meeting another of the ‘Known Customer Models’ (see Appendix A); or
* by providing 100 points of Documentary Evidence of Identity (see Appendix A).

[name of organisation] must ensure that the details of the patient as contained in their identity document(s) correspond with the individual’s details as recorded by [name of organisation]’s system. [name of organisation] should sight the relevant documents, and note in the local records which documents were sighted, but should not take copies of the documents or record the document numbers.

The authorised employee who is conducting Assisted Registration shall not register a patient if the employee is not satisfied about the identity of the patient.

**PATIENT IDENTIFICATION VERIFICATION (IVC) CODES**

When a patient registers for the My Health Record, the patient is given an IVC to allow them to access their record online for the first time. In Assisted Registration, the patient can elect to receive their IVC by text message, email or through [name of organisation].

If the patient has elected to receive their IVC through [name of organisation], the authorised employee must print this out for the patient, or may write down the IVC and provide it to the patient. IVCs must not be retained by [name of organisation] and must be destroyed securely as per [name of organisation] policies on destruction of confidential records.

1. **POLICY IMPLEMENTATION AND MAINTENANCE**

**MAINTAINING THIS POLICY**The implementation and maintenance of this policy is the responsibility of the [insert the role – ‘OMO’ or ‘RO’], including that:

* the policy has a version number;
* each time the policy is updated, the new version contains a unique version number and the date when that iteration came into effect;
* a copy of each version of the policy is retained;
* this policy will be reviewed when material is updated, changed, or risks are identified and at least annually; this review will include identification of new risks and consideration of anything that may result in unauthorised access, misuse or unauthorised disclosure of information or accidental disclosure of information, and of any changes to the National eHealth record system or relevant My Health Record system legislative framework since the last review; and
* a copy of this policy is made available to the System Operator within 7 days of receiving a request from the System Operator for a copy of the policy, and the copy provided is the version of [name of organisation]’s policy that was in force on the day requested by the System Operator.

|  |  |
| --- | --- |
| **Policy Manager**  (person nominated to implement and maintain the policy) | Name:  Tel:  Email: |
| **Approval Authority**  (person responsible for content and updates as set out in the *‘Policy Implementation and Maintenance’* section above) | Name:  Tel:  Email: |
| **Next Review Date** | DD/MM/YY (must be within 12 months from date of approval) |

**DOCUMENT VERSION HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document version #** | **Approved/amended/rescinded** | **Date** | **Approved by** |
| 001 |  |  |  |
|  |  |  |  |

**Appendix A**

|  |
| --- |
| **Known Customer Model** |
| **POINTS**   |  |  | | --- | --- | | 1. The individual has presented at the healthcare provider organisation on at least three occasions (inclusive of presentation at which Assisted Registration is being provided) and the individual’s Medicare or DVA card (with the individual’s name) has been sighted  OR 2. The individual is attending a hospital with a clinical referral in the individual’s name, at which time Assisted Registration is being provided, and the individual’s Medicare or DVA card (with the individual’s name) has been sighted OR 3. The individual is attending an emergency department, at which time Assisted Registration is being provided, and the individual’s photographic identification and Medicare or DVA card (with the individual’s name) has been sighted OR 4. The individual has had at least three prescriptions in their name filled at the pharmacy on three separate occasions within the last 12 months (inclusive of occasion at which Assisted Registration is being provided) and the individual’s Medicare or DVA card (with the individual’s name) has been sighted OR 5. The individual is enrolled with an Aboriginal Medical Service and Assisted Registration is occurring in conjunction with a consultation at the facility, and the individual’s Medicare or DVA card (with the individual’s name) has been sighted OR 6. The individual has presented at a healthcare service on at least three occasions (inclusive of presentation at which Assisted Registration is being provided) and the individual is enrolled in the My eHealth Record program OR 7. The individual is a resident of an aged care facility at which the Assisted Registration is being provided and the individual’s Medicare or DVA card (with the individual’s name) has been sighted OR 8. The individual is a customer or patient of the Healthcare Provider Organisation and has undergone a 100 point documentary check (see Part B) with the organisation either as part of becoming a patient or customer or as part of the Assisted Registration process OR 9. The individual is supported by a referee in accordance with the process used by the My eHealth Record (as operated by the Northern Territory Department of Health) OR 10. Other method approved by the System Operator | 100 | |

|  |
| --- |
| **Documentary Evidence of Identity** |
| |  |  | | --- | --- | |  | **POINTS** | | **Primary Documents – you can use only one of these** | | | Birth Certificate | 70 | | Birth Card issued by a Registry of Births, Deaths and Marriages | 70 | | Citizenship Certificate | 70 | | Current Passport | 70 | | Expired passport which has not been cancelled and was current within the preceding two years | 70 | | Other document of identity having the same characteristics as a passport including diplomatic documents and some documents issued to refugees | 70 | | **Secondary documents** | | | Any of the following, which must contain a photograph and a name. Additional documents from this category are awarded 35 points.   * Driver licence issued by an Australian state or territory * Licence or permit issued under a law of the Commonwealth, a state or territory government - (e.g. a boat licence) * Identification card issued to a public employee * Identification card issued by the Commonwealth, a state or territory government as evidence of the person's entitlement to a financial benefit * An identification card issued to a student at a tertiary education institution | 70 | | Must have name and address on:   * A mortgage or other instrument of security held by a financial body * Local government (council) land tax or rates notice * Land Titles Office record | 40 | | Must have name and signature on:   * Marriage certificate (for maiden name only) * Credit card * Foreign driver licence * Medicare card (signature not required on Medicare card) * DVA treatment card (signature not required on DVA card) * Membership to a registered club * Automobile Association of the Northern Territory (AANT) or equivalent membership * EFTPOS card | 35 | | Only one from each document type may be used - must have name and address on:   * Records of a public utility - phone, water, gas or electricity bill * Records of a financial institution * Lease/rent agreement * Rent receipt from a licensed real estate agent | 35 | | Must have name and date of birth on:   * Record of a primary, secondary or tertiary educational institution attended by the applicant within the last 10 years * Record of professional or trade association of which the applicant is a member | 25 | |