# **My Health Record Security and Access Policy**

Please note that the following policy template is intended as a guide only. Please tailor this template to meet the needs of your organisation and remove any type of guiding instructions. This policy template must be kept up to date.

The template addresses the requirements for health provider organisations to have a written policy as further detailed in [Rule 42 of the My Health Records Rule 2016.](https://www.legislation.gov.au/Details/F2016C00607) We do not recommend implementing this policy without first considering whether it meets your needs.

You must communicate this policy and ensure it remains readily accessible to all your employees and to any healthcare providers to whom your organisation supplies services under contract.

Each iteration of this policy should contain a unique version number and the date that iteration came into effect.

This Policy is for Click or tap to enter Organisation / Business Name referred to throughout this policy as “the organisation”

Version No. Click or tap to enter version No.

Date: Click or tap to enter a date.

## Purpose

* To provide guidance for staff and contractors on access to, and use of, the My Health Record system.
* To provide guidance in the use of information technology in the organisation as it relates to the My Health Record system.
* To outline the roles and responsibilities of the Responsible Officer (RO) and the Organisation Maintenance Officer (OMO) in relation to the My Health Record system.

## Scope of Policy

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

*This policy should be reviewed at least annually, with any material new or changed risks to be identified in accordance with the review considerations outline in Rule 42 (6) of the My Health Records Rule 2016.*

## Related Documents and Links

This policy is to be read in conjunction with the documents listed below, each of which can be accessed via the [Australian Government Federal Register for Legislation](https://www.legislation.gov.au/Series/C2012A00063).

My Health Records Act 2012 (Cth)

My Health Records Rule 2016

My Health Records Regulation 2012

My Health Records (Assisted Registration) Rule 2015

Healthcare Identifiers Act 2010 (Cth)

Privacy Act 1988

## Definitions

|  |  |
| --- | --- |
| Access Flag | An information technology mechanism made available by the System Operator to define access to a consumer’s My Health Record. |
| Healthcare Identifiers (HI) Service | ‘Healthcare Identifiers Service’, a national system for uniquely identifying healthcare providers, organisations and individuals receiving care. The HI Service is a foundation component of all national digital health products and services, including My Health Record. Healthcare identifiers are used to help ensure individuals and healthcare providers have confidence that the right information is associated with the right individual at a particular point of care. |
| Information Commissioner | The Office of the Australian Information Commissioner (OAIC) is the independent national regulator for privacy and freedom of information. They oversee the privacy aspects of the My Health Record system. |
| Network | Network of healthcare provider organisations created and managed in accordance with subsections 9A(3) to (6) of the *Healthcare Identifiers Act 2010*. |
| Network organisation | The 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. A network organisation within a network has the meaning given by subsection 9A(6) of the *Healthcare Identifiers Act*. |
| Organisation maintenance officer (OMO) | An OMO for a healthcare provider organisation has the meaning given by subsection 9A(8) of the Healthcare Identifiers Act.  For the OMO full roles and responsibilities see section 5 below. |
| Provider portal | A read-only portal provided by the System Operator that allows 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) | An RO for a healthcare provider organisation has the meaning given by subsection 9A(7) of the *Healthcare Identifiers Act*.  For the OMO full roles and responsibilities see section 5 below. |
| Seed organisation | The 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. A seed organisation for a network has the meaning given by subsection 9A(5) of the *Healthcare Identifiers Act*. |
| My Health Record System Operator | Established under the My Health Record Act, the entity responsible for operating the My Health Record system. The System Operator is the Australian Digital Health Agency. |

## Organisation Structure, Roles and Responsibilities

**Organisation Structure**

To participate in the My Health Record system all healthcare providers and organisations 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.

The organisation is registered in the HI Service as at Click or tap to enter a date.

**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 the organisation’s access to, and use of, the system. These roles are set out below:

|  |  |  |
| --- | --- | --- |
| **Role** | **HI Service** | **My Health Record System** |
| RO | * Register a Seed Organisation * Maintain the HPI-O details with the HI Service * Maintain their own RO details with the HI Service (add or remove RO) * Maintain OMO details with the HI Service (add or remove OMO) for seed and network levels * Retire, deactivate and reactivate the HPI-O   Maintain links between the Seed Organisation (and any Network Organisation/s) and any Contracted Service Provider.  See section 9A(7) of the Healthcare Identifiers Act for the full list of RO responsibilities in relation to the HI Service. | * Authorise the addition/removal of HPI-Os * Adjust the My Health Record system Access Flags for participating organisations within their hierarchy (OMO at seed level can also do this) * Set HPI-O/HPI-I authorisation links (OMO can also do this). |
| OMO | * Maintain their own OMO details * Request PKI certificate(s) (or link existing one) for organisation(s) they are linked to (note: only OMO's can request a NASH via HPOS) * Register a network HPI-O for network levels below * Register OMO details for network levels below * Validate, link or remove linked HPI-Is to HPI-O(s) they are linked to * Publish HPI-O details in the Healthcare Provider Directory (HPD) for HPI-Os they are linked to * If required, maintain a list of authorised employees within the organisation who access the HI Service.   See section 9A(8) of the Healthcare Identifiers Act for the full list of OMO responsibilities in relation to the HI Service. | * Set and maintain Access Flags according to the organisational network hierarchy, in accordance with meeting the principles outlined in the My Health Record Rules * Act on behalf of the Seed and Network organisation(s) (that they are linked to) according to the hierarchy * Maintain accurate and up-to-date records of the linkages between organisations within their network hierarchy. |

**Responsible Officer Details**

The RO: Click or tap here to enter Name of Responsible Officer.  
  
The OMO: Click or tap here to enter Name of Organisation Maintenance Officer

*Please note you can assign multiple OMO’s, simply add any additional OMO names above****.***

**Keeping Organisation Information Up-To-Date**

If the organisation becomes aware that information held by the HI Service in relation to the organisation is not accurate, up-to-date and complete, the RO or OMO must provide an update to the HI Service in writing of the correct information. This shall be provided within **20 days** of the organisation becoming aware that the information held is not accurate, up-to-date and complete.

If the organisation undergoes a material change, the RO or OMO must give the System Operator, in writing, details of the material change within two business days.

A material change may be:

* a change in the financial administration status of the organisation;
* a change in the organisation’s legal name;
* a change in the organisation’s legal structure; or
* the organisation is involved in a merger or acquisition.

**Network Obligations: Access Flags/Linkages**

*Please note this section is only relevant if the organisation has a network structure.*

***Access Flags***

Where the 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 the System Operator or a consumer query reveals potential structural issues. The organisation commits to making reasonable changes in line with requests from the System Operator.

***Linkages***

Where the 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.

## Access and Use of the My Health Record System

**Authorising Access to the My Health Record System**

Practice staff access to the My Health Record system is required as part of your role and responsibility.

All staff members required to access the My Health Record system will be provided with a unique user account with individual login name.

The organisation will maintain records linking user accounts to individual staff so that these can be matched in the case of an audit or investigation by the System Operator.

The 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.

* A user account must only be used by the individual to whom it was assigned. 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 the 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
* is no longer authorised to access 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 review and change their password every 30 days.

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.

In some instances, 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.

**Identifying Staff Who Access the My Health Record System**

***Provider Portal***

Where a healthcare provider in the organisation accesses the My Health Record system on behalf of the organisation via the National Provider Portal, the OMO will establish and maintain accurate and up-to-date authorisation links via HPOS (Health Professional Online Services) to ensure only those healthcare providers who are authorised can access the Provider Portal. If an individual healthcare provider is no longer authorised to access the provider portal on behalf of the organisation, the OMO will need to ensure the System Operator is informed and the individual is removed as an authorised user.

***Conformant Software***

Where healthcare providers in the organisation access the My Health Record system on behalf of the 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 the organisation’s internal records.

As mentioned above, 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**

The organisation has a formal training program where all staff with authorisation to access the My Health Record system on behalf of the organisation are required to undertake regular and ongoing privacy and My Health Record system training. Access to the My Health Record system will not be authorised to staff members until this training program is completed. Where any ongoing training requirements are not met, staff members authorisation will be revoked until training is completed.

*It is recommended that you put in place a timeframe around re-training / refresher training of staff (e.g. yearly / every 6 months and as required (e.g. when functionality or legislation changes).*

The organisation requires staff to complete re-training or refresher training on the My Health Record every Click or tap to enter timeframe i.e., 6 months. the organisation, and as required.

*Please describe in the below paragraph how your organisation keeps track of staff training. For example:*

The organisation keeps a central register of staff training. This register captures: what the training was about, who received the training, when it was provided, and who or how the training was provided.

Staff training will be provided with training around how 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 the organisation deems relevant, and training specific to the clinical software used by the 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.

## 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 the organisation, the 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 Data Breaches**

Under section 73 of the *My Health Record Act* and *Privacy Act 1988*, 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:

* a person has, or may have, contravened this Act in a manner involving an unauthorised collection, use or disclosure of health information included in a healthcare recipient’s My Health Record; or
* an event has, or may have, occurred (whether or not involving a contravention of this Act) that compromises, may compromise, has compromised or may have compromised, the security or integrity of the My Health Record system; or
* circumstances have, or may have, arisen (whether or not involving a contravention of this Act) that compromise, may compromise, have compromised or may have compromised, the security or integrity of the My Health Record system; and
* the contravention, event or circumstances directly involved, may have involved or may involve the entity.

If any staff member becomes aware of a data 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

**Patient Document and Record Codes**

Patients have the ability to set a number of privacy controls on their My 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 the 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, and you must ensure the practice’s IT system does not retain a copy of the record or document code.

**Responding to Patient Complaints**

The 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 My Health Record, the organisation shall take steps to investigate the issue. Unauthorised access should be managed through the organisation’s existing privacy complaint management processes and privacy policy.

Where a patient asks the organisation to remove or amend a clinical document, and the treating medical practitioner agrees, the medical practitioner or his/her delegate shall take steps to amend or remove the document as soon as possible.

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

Note: Where a patient requests for their information not be uploaded to their My Health Record, the healthcare provider organisation is legally required to comply.

## Policy Implementation and Maintenance

**Maintaining this Policy**

The implementation and maintenance of this policy is the responsibility of the 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 My Health Record system or relevant 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 the 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: Click or tap to enter name.  Tel: Click or tap enter telephone.  Email: Click or tap to enter email. |
| **Approval Authority**  (person responsible for content and updates as set out in the *‘Policy Implementation and Maintenance’* section above) | Name: Click or tap to enter name.  Tel: Click or tap enter telephone.  Email: Click or tap to enter email. |
| **Next Review Date** | Click or tap to enter a date. (must be within 12 months from date of approval) |

**Document Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document version #** | **Approved/amended/rescinded** | **Date** | **Approved by** |
| 1 | Approved  Click or tap to enter a date. | Click or tap to enter a date. | Click or tap to enter a date. |
|  |  |  |  |