**My Health Record Security and Access Policy**

Version X; <Date>

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 <Practice Name> 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 <Practice Name> 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)

[*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. <Practice Name> is registered in the HI Service as a Seed 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 <Practice Name>’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 <Practice Name> is: <Name of Responsible Officer>.
* *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 <Practice Name> is: <Name of Organisation Maintenance Officer>.

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

If <Practice Name> becomes aware that information held by the HI Service or the My Health Record system in relation to <Practice Name> 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 <Practice Name> becoming aware that the information held is not accurate, up-to-date and complete.

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. <Practice Name> 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. <Practice Name> 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 <Practice Name>
* 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**

*Conformant Software*

Where healthcare providers in <Practice Name> access the My Health Record system on behalf of <Practice Name> via conformant clinical software (*Genie Solutions*), the OMO will maintain a record of authorised Healthcare Provider Identifier – Individual (HPI-I) numbers in the clinical software and in <Practice Name>’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**<Practice Name> has a formal training program where all staff with authorisation to access the My Health Record system on behalf of <Practice Name> 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 <Practice Name>. 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 <Practice Name>’s clinical software 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 <Practice Name> deems relevant, and training specific to the clinical software used by <Practice Name>. 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 <Practice Name>, <Practice Name> 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 <Practice Name> 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**<Practice Name> 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, <Practice Name> shall take steps to investigate the issue. Unauthorised access should be managed through <Practice Name>’s existing privacy complaint management processes and privacy policy.

Where a patient asks <Practice Name> 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 pracititoner 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.

1. **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 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 <Practice Name>’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: <Insert Name>Tel: <Insert Telephone>Email: <Insert Email> |
| **Approval Authority**(person responsible for content and updates as set out in the *‘Policy Implementation and Maintenance’* section above) | Name: <Insert Name>Tel: <Insert Telephone>Email: <Insert Email> |
| **Next Review Date** | <Insert Date> (must be within 12 months from date of approval) |

**DOCUMENT VERSION HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document version #** | **Approved/amended/rescinded** | **Date** | **Approved by** |
| 1 | Approved <Insert Date> | <Insert Date> | <Insert Name> |
|  |  |  |  |