My Health Record Policy

Current as of: November 2018
Version no: 1

This policy provides guidance for staff and independent providers about access to and use of the My Health Record within our practice. It also provides guidance in the use of information technology in our practice as it relates to the My Health Record.

This practice's My Health Record policy is:

- drafted so that our practice can be audited against it to determine that the practice is in compliance with the policy
- kept up to date and reviewed at least annually and also when any new or changed risks are identified
- version-controlled so that each iteration contains a unique version number and the date when it came into effect
- inclusive of definitions of the roles of responsible officer and organisation maintenance officer

Responsible officer (RO) and organisation maintenance officer (OMO)

The following roles are responsible for implementation and compliance monitoring of the My Health Record policy in our practice:

- Our RO, Dr David Millar oversees our practice's legal compliance and sets up procedures to facilitate compliance with the My Health Record legislation
- Our OMO, Karen Millar is responsible for implementation and compliance monitoring of the My Health Record policy, and for maintenance of the policy within our practice

How the My Health Record is accessed in this practice

At our practice the My Health Record is accessed via the Best Practice Software Program. Only specific healthcare providers are authorised to access the My Health record system. Each provider is identifiable via their unique healthcare provider identifiers. The system operator is provided with an accurate and up-to-date list of all authorised healthcare providers. Access is deactivated if they leave the Practice or if their duties no longer require them to access My Health Record. Access is suspended immediately if their security has been compromised.

Registration for individuals authorised access to the My Health Record is a responsibility of Karen Millar (the Practice manager).

Karen Millar maintains the currency of our Health Provider Identifier – Organisation (HPI-O) and our information on the Health Provider Directory (HPD) according to the requirements of the *Health Identifiers Act 2010*.

In our practice we collect and record the Healthcare Provider Identifiers (HPI-Is) of our healthcare providers by keeping a digital and secured physical record of their AHPRA registration and ensure its currency is maintained.

We have a system in place to authorise access for users to access My Health Record by requesting audit logs from our IT provider for our clinical information system to see who has accessed the My Health Record.

The access to My Health Record is audited by administration staff, reviewing the audit log of our clinical information system on a periodic basis and keeping a register of individuals authorised to access the My Health Record for audit trail purposes. Karen Millar is responsible for the register and keeps it accurate and up to date by maintaining and reviewing it against all employee records.

Our practice does not give permission for health practitioners other than Dr David Millar and Dr Yin Min Hew to view the My Health Record via their own National Authentication Service for Health (NASH) certificates under the practice's registration for access of the My Health Record.

When an individual who is authorised to access the My Health Record in our practice leaves our practice, we deactivate their local account by:

- de-activating the user logon to our practice clinical software
- removing the link between our practice and the provider entry in the healthcare provider directory
- revising our register of authorised users

If the access security of one of our individuals authorised to use the My Health Record has been compromised, their account will be de-activated by:

- de-activating local account immediately when the practice becomes aware of the security breach
- de-activating relevant user logon to your clinical software and issuing new user logon to clinical software for the concerned staff member
- keeping record of the details surrounding the event
- discerning who the account belongs to and why the security breach happened
- notifying the My Health Record System Operator of the breach

My Health Record user training

In our practice we ensure that all authorised individuals who access the My Health Record have accessed comprehensive training that is current and provided by a credible source. This training includes how to use the system accurately and responsibly, the legal obligations of healthcare provider organisations and individuals using the system, and the consequences of breaching those obligations. Staff training is provided by the Australian Government Australian Digital Health Service. Training is provided via use of their resources

including: fact sheets, guides and online training. Training is always available to all staff for education and to support the smooth running of the practice with My Health Record.

Assisted registration

Our practice does not provide assisted registration for patients.

Requests to access a patient's My Health Record

Our practice has established processes for identifying a person who requests access to a patient's My Health Record. Users are identified by their unique identification, which is password secured and communicated to the System Operator on request to access a patient's My Health Record. Signed consent from the patient will also be requested and obtained at the time and prior to accessing their record. This consent will be permanently stored on the patient's record.

Physical and information security measures

In our practice we have established the following physical and information security measures. These should be adhered to by everyone accessing our practice system:

- restricting access to only persons who require access as part of their duties
- having a unique identification for each individual using the healthcare provider organisation's information technology systems, and having that unique identity protected by a password or equivalent protection mechanism
- having password and/or other access mechanisms that are sufficiently secure and robust to ensure security and privacy risks associated with unauthorised access to the system are adequately covered
- regularly reviewing passwords to ensure they are regularly changed and sufficiently complex
- implementing screensaver settings on computers so that users are required to enter their username and password to de-activate screensavers
- ensuring that individuals no longer authorised to access the My Health Record via or on behalf of the healthcare provider organisation are not able to do so via their user accounts
- suspending a user account that enables access to the My Health Record as soon as practical after becoming aware that the account has been compromised.

Policy review statement

This privacy policy will be reviewed regularly to ensure it is in accordance with any changes that may occur. We will notify our patients of these changes via our website and a hard copy of our Privacy Policy is available at our practice premises.