# Appendix 1 – ‘My Health Record policy’ template for general practices

The RACGP has developed a *My Health Record policy template for general practices* to address the requirements of Rule 42 of the My Health Records Rule 2016 (the Rule): health provider organisations need to have a written policy that reasonably addresses a range of matters, including how they authorise people to access My Health Record.

The following policy template provides guidance on meeting the legislative requirements for the content of a My Health Record policy. It is recommended that your practice use this guidance template to assist in documenting your written policy. You can adapt the sections in red text and other areas of the template as required to suit the specific procedures of your individual general practice. The explanatory notes provide additional information and context on why a particular requirement of the policy is important. Your final policy does not necessarily need to include these explanatory notes.

**Your practice’s My Health Record policy is required to cover matters specified in Subrule 4 (see 42 (4) of the Rule) which states:**

(4) Without limiting the matters a healthcare provider organisation’s policy must reasonably address, the policy is, subject to subrule (5), to address the following:

(a) the manner of authorising persons accessing the My Health Record system via or on behalf of the healthcare provider organisation, including the manner of suspending and deactivating the user account of any authorised person:

(i) who leaves the healthcare provider organisation;

(ii) whose security has been compromised; or

(iii) whose duties no longer require them to access the My Health Record system;

(b) the training that will be provided to healthcare provider organisation employees before they are authorised to access the My Health Record system, including in relation to how to use the My Health Record system accurately and responsibly, the legal obligations on healthcare provider organisations and individuals using the My Health Record system and the consequences of breaching those obligations;

(c) the process for identifying a person who requests access to a healthcare recipient’s My Health Record and communicating the person’s identity to the System Operator so that the healthcare provider organisation is able to meet its obligations under section 74 of the Act;

(d) the physical and information security measures that are to be established and adhered to by the healthcare provider organisation and people accessing the My Health Record system via or on behalf of the healthcare provider organisation, including the user account management measures that must be implemented under rule 44;

(e) mitigation strategies to ensure My Health Record system-related security risks can be promptly identified, acted upon and reported to the healthcare provider organisation’s management; and

(f) where the healthcare provider organisation provides assisted registration:

(i) the manner of authorising employees of the organisation to provide assisted registration;

(ii) the training that will be provided before a person is authorised to provide assisted registration;

(iii) the manner of confirming a healthcare recipient’s consent for the purposes of rule 9 of the My Health Records (Assisted Registration) Rule 2015; and

(iv) the process and criteria for identifying a healthcare recipient for the purposes of assisted registration.

**Please note that My Health Records Rule 2016 Subrule 5 states:**

(5) If in the reasonable opinion of a healthcare provider organisation, a requirement in subrule (4) is not applicable to the organisation due to the limited size of the organisation, the organisation’s policy need not address that requirement.

*Explanatory notes:* If you believe that a requirement in Subrule 4 is not applicable to your practice due to the limited size of your organisation, you do not need to address that requirement; however, you should state this explicitly in your practice’s My Health Record policy.

**Your practice’s My Health Record policy is required to comply with My Health Records Rule 2016 Subrule 6 which states:**

(6) Healthcare provider organisations must ensure that:

(a) the policy mentioned in subrule (1) is:

(i) drafted in such a manner that the organisation’s performance can be audited against the policy to determine if the organisation has complied with the policy; and

(ii) kept up-to-date;

(b) each iteration of the policy contains a unique version number and the date when that iteration came into effect;

(c) without limiting paragraph (6)(a)(ii) – the policy is reviewed at least annually and when any material new or changed risks are identified. The review must include consideration of:

(i) factors that might result in:

(A) unauthorised access to the My Health Record system using the healthcare provider organisation’s information systems;

(B) the misuse or unauthorised disclosure of information from a healthcare recipient’s My Health Record by persons authorised to access the My Health Record system via or on behalf of the healthcare provider organisation; and

(C) the accidental disclosure of information contained in a healthcare recipient’s My Health Record;

(ii) any changes to the My Health Record system that may affect the healthcare provider organisation; and

(iii) any relevant legal or regulatory changes that have occurred since the last review; and

(d) a record of each iteration of the policy mentioned in subrule (1) is retained in accordance with the record keeping obligations (if any) applicable to the healthcare provider organisation.

.

[insert practice name] My Health Record policy

Current as of: [insert date of last revision]

Version no: [insert version number]

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

* Our RO, [insert name of person assigned to the role of RO, and their position], oversees our practice’s legal compliance and sets up procedures to facilitate compliance with My Health Record legislation.
* Our OMO, [insert name of person assigned to the role of OMO, and their position], is responsible for implementation and compliance monitoring of My Health Record policy, and for maintenance of the policy within our practice.

How My Health Record is accessed in this practice

[Describe how individuals in your practice are authorised to access My Health Record, including how access is suspended or deactivated when they leave the healthcare provider organisation, when their security has been compromised, or when their duties no longer require them to access My Health Record.]

At our practice we access My Health Record via the [insert which software you use to access the system (eg your practice clinical information system) and/or the National Provider Portal. If you allow access via the National Provider Portal, your practice must establish and maintain with the System Operator an accurate and up-to-date list of all identified healthcare providers who are authorised to access the My Health Record system via or on behalf of the organisation using the portal under Section 27 of My Health Record Rules].

Registration for individuals authorised access to My Health Record is [describe how individuals at the practice become authorised to access My Health Record (eg they may have had to complete specific training or sign specific agreements)] and is a responsibility of [insert user (eg the practice manager)].

[Insert the person responsible – this will be either the RO or the OMO] maintains the currency or our Health Provider Identifier – Organisation (HPI-O) and our information on the National Health Services Directory 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 [describe how your practice collects and records, registers and generally manages HPI-Is].

*Explanatory notes:* Under the My Health Records Rule 2016, healthcare provider organisations must ensure that their Organisation Maintenance Officers establish and maintain with the System Operator an accurate and up-to-date list of all identified healthcare providers – individuals who are authorised to access My Health Record via or on behalf of the organisation using the provider portal.

We have a system in place to authorise access for users to access My Health Record by [describe how your practice keeps track of individuals who are authorised to access My Health Record. For example, how would you access the audit logs for your clinical information system to see who has accessed My Health Record and what assistance, if any, you may need from your IT provider or other external organisations to provide this information].

*Explanatory notes:* Only healthcare providers with a Health Provider Identifier–Individual (HPI-I) linked to the practices Health Provider Identifier–Organisation (HPI-O) are authorised to access a patients My Health Record. Practices may keep a list of individual users authorised to access My Health Record and will need a process to ensure this list is reviewed and updated frequently to remove authorised individuals who no longer require access to My Health Record. These processes could be included as part of the practice’s induction and termination policies. There is a potential risk of unauthorised access if your practice uses shared terminals and logons. Given the risks to practices it is unwise not to implement and enforce individual logons.

Access to My Health Record is audited by [describe the process for audit access to My Health Record by your staff (eg viewing the audit log of your clinical information system on a periodic basis or keeping a register of individuals authorised to access My Health Record for audit trail purposes) and who within your practice is responsible for the register. You will need to consider how this register is kept accurate and up to date. Practices might consider attaching a register to this policy].

*Explanatory notes:* Some practices may not understand how to monitor log files and may be unable to provide an internal audit facility. These practices may wish to document that the healthcare providers they authorise to access My Health Record through their clinical information system can be identified and audited through that clinical information system. The practice does not have the skills to manage this internally, but the practice will provide reasonable assistance to the System Operator or the Office of the Australian Information Commissioner (OAIC) to obtain this information should it be required.

Our practice does not give permission for health practitioners other than [insert users with access] to view My Health Record via their own National Authentication Service for Health (NASH) certificates or Provider Digital Access (PRODA) credentials, under the practice’s registration for access of My Health Record.

*Explanatory notes:* You may decide to restrict access for health practitioners to access My Health Record using their own NASH certificate or PRODA credentials as part of your access controls. Practices may not have the same ability to monitor provider usage through the National Provider Portal as they may through the practice’s clinical information system.

When an individual who is authorised to access My Health Record in our practice leaves our general practice, we deactivate their local account by [describe the process for de-activating the staff member’s access; for example:

* de-activating the user logon to your practice clinical software
* removing the link between your practice and the provider entry in the healthcare provider directory via the Healthcare Identifier (HI) service on the Health Professional Online Service (clinical staff only) where you provide access to the provider portal
* revising your register of authorised users if have one].

If the access security of one of our individuals authorised to use My Health Record has been compromised, their account will be de-activated by [describe the process of de-activating the local account of a staff member whose security has been compromised; for example:

* 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 My Health Record System Operator of the breach].

My Health Record user training

In our practice we ensure that all authorised individuals who access 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.

[Describe the process of staff training, when it is run and who it is run by, and whether you run it in the practice, use online resources or access training from a Primary Health Network (PHN). Describe any written certification that you provide to staff who receive training, and whether you require written verification from staff that they have completed other external training. Practices may also find it useful to keep a record of all training that has been undertaken by all staff. A document detailing the name of the staff member, purpose of training and the date training was completed could be attached to the policy.]

Assisted registration

Our practice [does/does not] provide assisted registration for patients.

*Explanatory notes:* Assisted registration may still be used by practices to create a My Health Record for patients who initially opted-out from having a record created but who now want a record. Providing assisted registration is optional for practices. If you do provide assisted registration, you should have a policy in place outlining how the requirements outlined in Section 42 Subrule 4(f) are met.

Practices performing assisted registration take responsibility for informing patients and gaining their consent for My Health Record. This creates a potential risk and practices should consider the risks and benefits when deciding to offer assisted registration.

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.

[Describe how you identify users accessing My Health Record and how you communicate this information to the System Operator.]

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.

[Describe the security measures within your practice. Essential user account management measures to be implemented could include:

* 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 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 My Health Record as soon as practical after becoming aware that the account has been compromised).]

Mitigation strategies

To ensure that My Health Record system-related security risks can be promptly identified, acted upon and reported to the relevant authority, our practice will:

[Describe strategies for risk mitigation. This could include regular reviews of security and procedures for accessing My Health Record and revision of those procedures as required, development of a risk reporting procedure to allow staff to inform management of any suspected security issue or breach of the system, and/or risk assessment audits of IT systems to examine privacy and security risks.]

**Disclaimer**

The template policy is intended for use as a guide of a general nature only and may or may not be relevant to particular practices or circumstances. The RACGP has used its best endeavours to ensure the template is adapted for general practice to address current and anticipated future privacy requirements. Persons adopting or implementing its procedures or recommendations should exercise their own independent skill or judgement, or seek appropriate professional advice. While the template is directed to general practice, it does not ensure compliance with any privacy laws, and cannot of itself guarantee discharge of the duty of care owed to patients. Accordingly, the RACGP disclaims all liability (including negligence) to any users of the information contained in this template for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of reliance on the template in any manner.