IMPLEMENTATION GUIDE

FOR SPECIALIST PRACTICES

My Health Record

The following guide provides steps on how to implement My Health Record in your practice, including:

- registering to My Health Record,
- connecting to My Health Record,
- managing compliance, policies and education, and
- informing and supporting patients.

These steps will support you in integrating My Health Record into your practice safely and effectively.

Australian Government
Australian Digital Health Agency

Implementation Checklist

IMPLEMENTATION STEP	STATUS
Prepare for registering with My Health Record	☐
Manage the required compliance processes	☐
Train staff on how to use My Health Record	☐
Complete the registration process	☐
Configure software (for organisations accessing via conformant software)	☐
Inform and support patients	☐
Position your organisation to meet ongoing participation obligations	☐

Step 1: Prepare for registering with My Health Record

UNDERSTANDING SEED AND NETWORK STRUCTURES[1]

Healthcare provider organisations participate in the My Health Record system either as a Seed Organisation or as a Network Organisation that is part of a wider 'network hierarchy' (under the responsibility of a Seed Organisation). A Seed Organisation is a legal entity that provides or controls the delivery of healthcare services (e.g. a private medical specialist practice).

ROLES AND RESPONSIBILITIES

The Healthcare Identifiers (HI) Service and the My Health Record system require people working in healthcare provider organisations to be assigned roles authorising them to carry out certain actions. These roles include the Responsible Officer (RO) and the Organisation Maintenance Officer (OMO). The RO and OMO are explained below:

- **Responsible Officer (RO):** The officer of an organisation who is registered with the HI Service and has authority to act on behalf of the Seed Organisation and relevant Network Organisations (if any) in its dealings with the System Operator of the My Health Record system and Service Operator of HI Service. For private medical specialist practices, the RO may be a business owner. For large organisations like hospitals, the RO may be the Chief Executive Officer.
- **Organisation Maintenance Officer (OMO):** The officer of an organisation who is registered with the HI Service and acts on behalf of a Seed Organisation and/or Network Organisations in its day-to-day administrative dealings with the HI Service and the My Health Record system. Healthcare organisations can have more than one OMO if they wish. This role may be assigned to the Practice Manager and/or other senior staff who are familiar with the practice's clinical and administrative systems. **Note:** the RO may take on the OMO role as well.

More information on the responsibilities of the RO and OMO roles can be viewed on the Australian Digital Health Agency's website.

DECIDE ON TYPE OF MY HEALTH RECORD ACCESS

There are two main options for healthcare organisations to access their patients' My Health Records:

- **Conformant Software**: Healthcare providers can choose to access their patient's My Health Record through conformant software which allows healthcare providers to view, download and upload information to their patients' My Health Records.
- **National Provider Portal**: For those who don't have conformant software, their patients' My Health Record can be accessed through the National Provider Portal which allows read-only access.

To see whether your practice software is conformant, review the list of software providers published on the Australian Digital Health Agency's website.

Step 2: Manage compliance[2]

MY HEALTH RECORD SYSTEM POLICY

In order to meet the legislative requirements for participating in the My Health Record system, organisations need to confirm that they have relevant policies and procedures in place. The required policies are:

- My Health Record security and policy, and
- National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) certificates policy (only for organisations accessing via conformant software).

To help you with this step, please read the overview of digital health policies document which highlights objectives and requirements for both policies. Additionally, consider using the following sample policies:

- RACP My Health Record system security and access policy template, and
- sample NASH PKI certificates policy.

For help with creating My Health Record policies and with managing compliance more broadly, see the Australian Digital Health Agency's contacts for healthcare professionals' page.

PRIVACY AND SECURITY COMPLIANCE CHECKLIST

The following checklist can be used as a guide to implement security practices and policies in your organisation. It covers the requirements that must be incorporated in a My Health Record system security and access policy, as outlined in the *My Health Records Rule 2016* (Cth), together with several sound privacy and security practices.

- **Managing User Accounts** – individual user accounts are used and monitored when accessing your organisation's practice software and the My Health Record system.
- **Identification of Staff** – requirements for staff members using clinical software to access the My Health Record system to view individual My Health Records.
- **Staff Training** – regular training is given to staff members that use the My Health Record system.
- **Handling of Privacy Breaches and Complaints** – reporting procedures and processes are put in place to meet notifications requirements or handle consumer concerns regarding unauthorised access to their My Health Record.
- **Risk Assessments** – are regularly undertaken and security and privacy risks for My Health Record access and the broader Information Communications Technology of your organisation are considered.

See expanded guidance on the security practices and policies checklist.

MISUSE OF MY HEALTH RECORD

Misuse of a person's health information is a serious matter. Damage to an individual or healthcare provider organisation is significant and healthcare providers have professional and legal obligations to protect patient information.

The My Health Record system and the Healthcare Identifiers Service are protected by a penalty framework set out in the *My Health Records Act 2012* (Cth) and *Healthcare Identifiers Act 2010* (Cth). Actions subject to penalties include, but is not limited to:

- unauthorised collection, use or disclosure of health information in a My Health Record,
- unauthorised use or disclosure of healthcare identifiers or other information obtained for the purposes of the Healthcare Identifiers Service,
- failing to give written notice within 14 days if the entity ceases to be eligible to be registered, and
- failing to notify an actual or potential data breach in which they were directly involved.

For more information, see the Australian Digital Health Agency's webpage on penalties for misuse of health information. Civil fines can include a maximum of $315,000 and criminal penalties of up to 5 years' jail time.

Step 3: Train staff[3]

Organisations are required to ensure that staff accessing My Health Record as part of their role within the organisation are appropriately trained before accessing the system. Consider the following recommended training checklist and declaration form, which provides a list of recommended training topics with links to relevant content, as well as a declaration section.

Several training options are available for staff, some of which are linked to in the above form, including:

- Australian Digital Health Agency online eLearning Modules.
- On Demand Software Training simulators and demonstrations. Username: OnDemandTrainingUser and password: TrainMe.
- Access to software Summary Sheets or My Health Record manuals requested from your software vendor.
- Presentations/educations sessions by Australian Digital Health staff.

See also the Australian Digital Health Agency's list of My Health Record training and resource options available for healthcare providers.

Step 4: Complete the My Health Record registration process[4]

Separate processes exist to enable access to My Health Record through the National Provider Portal or through conformant software. See the information and resources below to enable your chosen access route.

REGISTRATION FOR ACCESS VIA THE NATIONAL PROVIDER PORTAL (NPP)

Enabling My Health Record access via the NPP requires you to:

- register for your PRODA account,
- register your practice, and
- link your healthcare provider individuals to your organisation.

The Australian Digital Health Agency has provided a simple one-page guide on how to enable access via the NPP.

REGISTRATION FOR ACCESS VIA CONFORMANT SOFTWARE

Enabling My Health Record access via conformant software requires you to:

- register for your PRODA account,
- select HPOS service,
- link existing identifiers,
- register your practice,
- check with your software vendor if they have been registered as a contracted service provider (CSP)
- (if they are not a CSP), request a NASH PKI certificate, and
- link your existing Medicare PKI certificate.

The Australian Digital Health Agency has provided simple one-page guides on how to enable access via conformant software / CSP.

NEED HELP WITH THE MY HEALTH RECORD REGISTRATION PROCESS?

- **PRODA**: 1800 700 199 (Mon-Fri 8am to 5pm, Australian Western Standard Time)
- **HI Service Enquiry Line:** 1300 361 457 (Monday to Friday, 8:30am – 5:00pm AEST)
- **HPOS**: 13 21 50 (Mon-Fri 8am to 5pm, Australian Western Standard Time)
- **My Health Record Help line**: 1800 723 471 (24 hours, 7 days a week)

NEED HELP WITH LOCATING YOUR HEALTHCARE IDENTIFIER?

- **AHPRA registration number**: use the AHPRA website's search function
- **Healthcare Provider Identifier – Individual (HPI-I):** call the HI Service enquiry line on 1300 361 457 (Monday to Friday, 8:30am – 5:00pm AEST)
- **Healthcare Provider Identifier – Organisation (HPI-O):** call the HI Service enquiry line on 1300 361 457 (Monday to Friday, 8:30am – 5:00pm AEST)

Step 5: Configure software

This step is only relevant if you DO have conformant software and are accessing My Health Record via conformant software.

If you are accessing My Health Record via the National Provider Portal (NPP)
skip step 5 and continue from step 6.

The following section provides a view of the tasks involved with configuring your software with My Health Record. The listed tasks should be completed with guidance and support from your software vendor.

1	Check whether a list of HPI-Is is required for configuring the software.
2	Install NASH PKI and Medicare PKI certificates within conformant software.
3	Confirm HPI-O and HPI-I numbers have been configured into software.
4	Update permission settings for staff accessing My Health Record. Staff will require relevant viewing/uploading permissions for My Health Record and for the electronic transfer of prescriptions, if enabled.
5	Check that My Health Record can now be accessed via your clinical software. Inform your software vendor if there are connection errors or Individual Healthcare Identifier (IHI) errors.

Step 6: Inform and support patients

INFORM PATIENTS YOU OFFER MY HEALTH RECORD

Add information to your website and privacy policy and inform consumers that your healthcare organisation uses My Health Record. To aid this process, consider displaying brochures and posters in your organisation – contact your local Primary Health Network to request additional My Health Record resources and collateral.

SHARE MY HEALTH RECORD RESOURCES WITH PATIENTS

A range of online resources and fact sheets exist to help you communicate to your patients the benefits and methods of using My Health Record. These include, but are not limited to:

- introductory information sheets,
- information on how to keep your My Health Record safe,
- 'how to' guides,
- Frequently Asked Question sheets, and
- cancelling a My Health Record guide.

Step 7: Meet ongoing participation obligations[5]

There are several ongoing obligations for a participating organisation - the following is not an exhaustive list of obligations. If in doubt about your organisation's obligations, you should contact the Australian Digital Health Agency as the System Operator of My Health Record. See the Australian Digital Health Agency's 'contact us' page.

To participate in the My Health Record system your practice must:

- not discriminate against an individual because they do not have a My Health Record or because of their My Health Record's access control settings.
- take reasonable steps to ensure that their employees exercise due care and skill so that any record uploaded to the My Health Record system is, at the time it is uploaded, accurate, up to date, not misleading and not defamatory.
- not upload clinical information or a clinical document to the My Health Record system where an individual has requested that it not be uploaded.
- only upload a clinical document to the My Health Record system if you know that it has been prepared by a person who is a registered healthcare provider (i.e. has an HPI-I) and whose registration is not conditional, suspended, cancelled or lapsed.
- tell the System Operator as soon as practicable after becoming aware of a potential or actual data breach, that is:
  - There has been an unauthorised collection, use or disclosure of health information included in an individual's My Health Record; or
  - An event has, or may have, occurred that compromises, or may compromise, the security or integrity of the My Health Record system.
- tell the System Operator, within two business days of becoming aware, of a non-clinical My Health Record system-related error in a record, or when your organisation undergoes a material change.
- tell the System Operator within 14 days if your organisation has ceased to be eligible to be registered (for example, the organisation has cancelled its HPI-O).
- give the System Operator necessary assistance in relation to any inquiry, audit, review, assessment, investigation or complaint regarding the My Health Record system.
- develop, maintain, enforce and communicate to staff written policies relevant to the My Health Record system to ensure that interaction with the My Health Record system is secure, responsible and accountable, and to provide a copy of your policy to the System Operator on request.

For more information and context on participation obligations, see the Australian Digital Health Agency's overview. Additionally, see the penalties for misuse of health information for information on the consequences for not meeting participation obligations.

Additional My Health Record Implementation Resources

- Handbook for Practice Managers | Australian Digital Health Agency & AAPM
- Practice Manager Registration Guide | Australian Digital Health Agency & AAPM
- My Health Record: Healthcare Provider Registration Access – NPP | Australian Digital Health Agency
- My Health Record: Healthcare Provider Registration Access – conformant software | AD Australian Digital Health Agency HA
- Example My Health Record Policy | Australian Digital Health Agency
- Help Centre | Australian Digital Health Agency

[1] ADHA, 'Roles and responsibilities', n.d., accessed 10 September 2020.
[2] ADHA, 'Handbook for Practice Managers', 2019, accessed 10 September 2020.
[3] ADHA, 'Handbook for Practice Managers', 2019, accessed 10 September 2020.
[4] ADHA, 'My Health Record – Healthcare provider Registration', n.d., accessed 10 September 2020.
[5] ADHA, 'Handbook for Practice Managers', 2019, accessed 10 September 2020.