Guide to My Health Record for Australian Surgeons

Royal Australasian College of Surgeons

Australian Government
Australian Digital Health Agency

Contents

Further information

Royal Australasian College of Surgeons
250-290 Spring Street
East Melbourne VIC 3002 Australia

Telephone: +61 3 9249 1200
Web: surgeons.org

3rd edition, February 2020

Committed to Indigenous health

Service | Integrity | Respect | Compassion | Collaboration

Dear colleagues

As the Chair of the Younger Fellows Committee, I am always keen to learn about how our Fellows are innovating their day-to-day practice, particularly with regards to digital health.

The committee has been conducting research into digital health and we have found that although there is an interest in using the Australian Government's My Health Record, many of our Fellows are not sure where to begin.

The College supports the use of My Health Record as a central repository of information that saves time for practitioners and ultimately improves patient care. In a time of innovation in digital health, maintaining a reliable source of data to improve patient care is a step in the right direction.

We have produced this booklet as a way of supporting our colleagues in connecting to and using My Health Record in day-to-day practice.

Pecky De Silva,
Chair, Younger Fellows Committee

Glossary of terms

Terms	Definitions
HI Service	Healthcare Identifier Service A national system for uniquely identifying individuals and healthcare providers.
HPI-I	Healthcare Provider Identifier – Individual A unique 16-digit number used to identify individual healthcare providers. Health practitioners registered with AHPRA are automatically assigned an HPI-I while those not registered with AHPRA can apply for a HPI-I from the HI Service.
HPI-O	Healthcare Provider Identifier – Organisation A unique 16-digit number used to identify eligible healthcare organisations. Organisations can apply for an HPI-O from the HI Service.
HPOS	Health Professional Online Services A web-based service provided by Services Australia that allows providers to send and retrieve various types of information to/from Services Australia.
IHI	Individual Healthcare Identifier A unique 16-digit number used to identify individuals who receive care in the Australian healthcare system. IHIs are automatically assigned to everyone enrolled in Medicare or with a DVA treatment card; anyone else can apply to the HI Service.
LDAC	Limited document access code A code that an individual can provide to healthcare providers. The 4-8 alphanumeric code is provided to a healthcare provider so that they can access documents marked as 'restricted' in a patient's My Health Record.
NASH	National Authentication Service for Health A NASH Certificate is required by organisations seeking to interact with the My Health Record system using conformant software. It can also be used for secure messaging.
NPP	National Provider Portal An interface through which healthcare providers can access the My Health Record system without the need for conformant clinical software.
OMO	Organisation Maintenance Officer A staff member of a healthcare organisation who is registered with the HI Service and is authorised to interact on behalf of the organisation in its day-to-day administrative dealings with the My Health Record System Operator and HI Service.
PRODA	Provider Digital Access An online authentication system used to securely access Government online services. Using a two-step verification process, you only need a username and password to access multiple online services.
RAC	Record Access Code A code that an individual can use to restrict access to their My Health Record. The code is provided to a healthcare provider so that the healthcare organisation is granted access to a person's My Health Record.
RO	Responsible Officer A staff member of a healthcare organisation who is registered with the HI Service and has authority to act on behalf of the seed or network organisation in its dealings with the My Health Record System Operator and the HI Service. The RO is often the business owner in a small practice, or the CEO of large organisations like hospitals.

My Health Record

My Health Record – a guide for specialist practitioners

This guide has been designed to assist RACS Fellows in implementing and utilising My Health Record as part of their practice

How to use this guide

This guide has been designed to assist RACS Fellows in implementing and using My Health Record as part of their practice. Whether you use it regularly, have explored it once or twice, or are yet to come across it, this guide will prove useful to Fellows who work in private practice and in larger organisations.

This guide:

- provides an overview of My Health Record
- outlines its features and benefits outlines practical tips on registering, implementing and using My Health Record in your practice.

Thank you to RACS Fellows who took the time to share their insights, case studies and thoughts while we were researching this guide.

About My Health Record

Launched in 2012 as the Personally Controlled Electronic Health Record (PCEHR), My Health Record is Australia's national digital health record system. It is a secure online summary of an individual's health information and is available to all Australians. Healthcare providers and other staff members authorised by their healthcare organisation can access My Health Record to view and add patient health information.

My Health Record lets you access timely information about your patients such as shared health summaries, discharge summaries, prescription and dispense records, pathology and diagnostic imaging reports and immunisation information. It does not replace existing health records. Rather, it supplements these with a high-value, shared source of patient information that can improve care planning and decision making.

While there is no requirement for healthcare professionals or patients to use My Health Record, the more it is used, the more useful it becomes for both patients and healthcare providers.

Why use My Health Record?

By using My Health Record, healthcare providers (e.g. surgeons) have access to key patient information that may otherwise not be directly received or accessed easily. By uploading key clinical information, surgeons are contributing to more informed care and decision-making. By using My Health Record, surgeons can provide a vital source of information for other healthcare professionals and patients by enabling continuity of care between the hospital system and community care. Information in a patient's record may also be useful in an emergency when a patient may be unconscious, or if a patient is unable to recall or communicate specific information.

More than 23 million Australians have a My Health Record, making it a vast and useful repository of knowledge for healthcare professionals. Ultimately, its use means surgeons can spend more time with their patients and less on administrative tasks such as sourcing information and

"I think it would be a good thing if take-up increased. The old system is very archaic, and results in a lot of duplication, and time is money".

– Melbourne-based Paediatric surgeon, RACS Fellow

documentation from other healthcare providers.

A RACS Fellow, a Paediatric surgeon at a large urban hospital, says: "The main problem is – and this is applicable here at the Children's – is that you get patients come in, and they don't know where they got their X-ray or their MRI, they say they had an X-ray at a place next door to the KFC in Brunswick, and you're googling these places to find it, and ringing around. If surgeons knew that My Health Record was available and knew that was a good spot for all those documents, it would be a win."

Another RACS Fellow, a urologist, says, "If you're in Sydney there are thousands of X-ray providers, and you see someone and you say 'do you have your X-ray' and they say, no they said they'd send a copy. And you go 'yeah right' then you have to go find it. They can't remember where they had it done, so you're ringing up numerous places trying to chase it down. Once again, that single repository, My Health Record, would take all that work out of it. It's a great concept."

Benefits of My Health Record

For practitioners:

- Improved decision making through increased access to patient information.
- Reduced time spent looking for and receiving information about patients from other healthcare providers (e.g. patients with chronic diseases).
- Access to information that was not received directly – i.e. hospital discharge summaries, test results or medication information that may have been forgotten by the patient.
- Avoids duplication of tests, scans and diagnosis, relieving the time burden of ordering tests.
- Ability to access information if patient is unconscious/mentally impaired and can't provide it.

For your patients:

- Healthcare providers have access to important clinical information such as medication and allergies in an emergency or when patients are unable to provide them.
- My Health Record lets patients control their health information securely, in one place.
- Helps patients keep track of their own health history.
- Less reliance on memory and provision of specific information.
- More time is spent with medical practitioners.
- More accurate decision making and better coordination of healthcare.

For practice managers:

- Reduced time spent gathering patient information, e.g. ordering tests.
- Less reliance on paper or faxed records.
- Improved practice efficiency and reduced costs.

What is in My Health Record?

Healthcare providers and other staff authorised by their healthcare organisation can access My Health Record to view and add patient health information via conformant clinical information systems or the National Provider Portal (NPP).

The following information can be accessed. Some document types may not be available, depending on how the consumer configured their privacy settings.

- **Pathology and diagnostic imaging reports** that may be uploaded to a patient's record by the pathology laboratory or diagnostic imaging provider and are viewable to healthcare professionals who have access to that patient's record.
- **Event summary** documents which describe single healthcare events relevant to the patient's ongoing health, such as a treatment beginning or ending, a clinical intervention, or a new medication prescription.
- a **Shared health summary** that represents the patient's health at a specific point in time and is usually created by the patient's regular healthcare provider, such as the patient's GP. This document may contain information about current medications, immunisations, allergies and patient health conditions, including past procedures.
- **Advance care planning** documents that outline the wishes of the patient for future healthcare and treatment. They may also contain details of a nominated contact who holds the details of their advance care plan.
- **Prescription and dispense records** that contain information about medicines prescribed and dispensed by a healthcare provider.
- **Medicines information view** which displays medicines listed in a patient's record, viewable by date or in alphabetical order. Information is gathered from the Pharmaceutical Benefits Scheme (PBS) records, prescription and dispense records, recent shared health and discharge summaries and event summaries. The medicines view also contains information about allergies and adverse reactions and links to the most recent shared heath summary and discharge summary (if available).
- **Discharge summaries** that capture details of a patient's stay in hospital and recommendations for patient care after discharge.
- **Specialist letters** that outline a diagnosis, prescription or recommendation for care.
- **Immunisation view** displays details of a patient's immunisations recorded in the Australian Immunisation Register (AIR). The view shows an immunisation history, including date, disease, vaccine details including batch number and vial serial number, dose, source and a link to the source document.
- **Medicare overview** which includes information about the patient's medical history such as Medicare and Pharmaceutical Benefits Scheme (PBS) information held by Services Australia, Medicare and Repatriation Schedule of Pharmaceutical Benefits (RPBS) information stored by the Department of Veterans' Affairs (DVA), organ donation decisions and immunisations that are included in the Australian Immunisation Register, including childhood immunisations and other immunisations received.
- **Patient-entered information** which includes information about medicines, allergies and adverse reactions, contact details, next of kin, emergency contact, carer information and advance care plans. Patients can add information by logging into their record through the myGov website.

Your patients and My Health Record

Once your organisation is registered for My Health Record and you have been authorised to begin using the system, you can start accessing your patient's records for the purpose of delivering care. Patients can link and log in to their record through the myGov website. Once linked, they can add information such as next of kin, allergies and adverse reactions, advance care plans and emergency contact details. Your patients may also wish to add personal health notes to their record, which are private and cannot be seen by medical organisations. Those with dependent children or adults can view and add information to their child or dependent's My Health Record on their behalf. From age 14, patients will be able to manage their own record. If the patient would prefer their parents to manage their record on their behalf, they can identify them as a nominated representative (more information here).

A key feature of My Health Record is that it is personally controlled. Individuals have a number of mechanisms available

to them to manage the content of, and to control access to, their own and/or their dependent's record(s).

Patients can choose to restrict organisations from accessing their entire record by applying restrict access to particular documents by using a Limited Document Access Code (LDAC). Once set, these codes can be provided by the patient to organisations that they wish to grant access to their record or the hidden documents in their record.

Your patients can apply or remove restrictions to documents or organisations at any time. They can do this by clicking on the 'Privacy & Access' section of their record.

There are four document settings patients can apply to restrict healthcare providers from seeing information in their record:

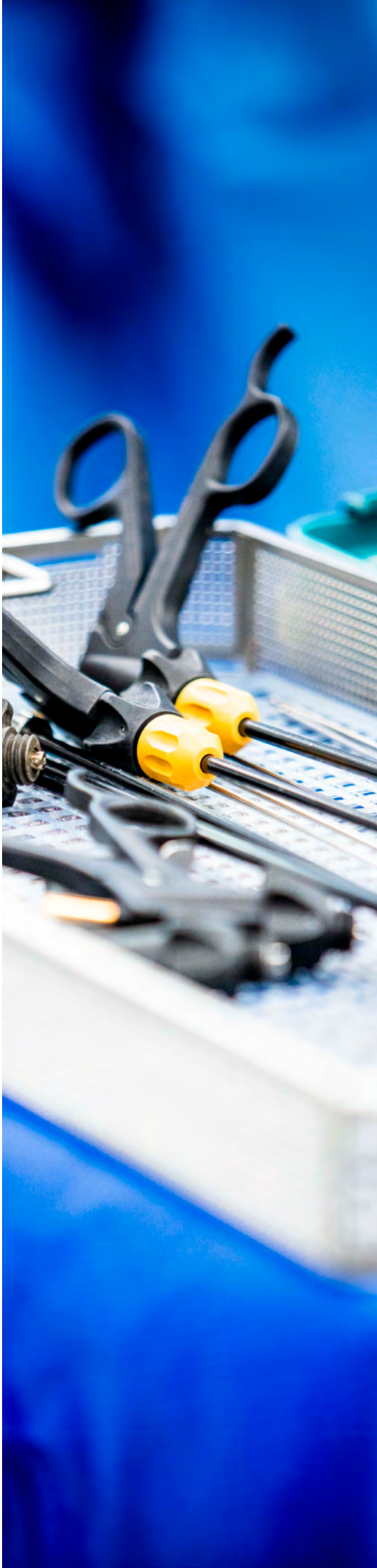
- **General access:** Allows healthcare providers and the patient's representatives to view a document.
- **Restricted:** Allows only healthcare providers and the patient's representatives with 'restricted access' to view a clinical document. There are certain types of documents that cannot have 'restricted access' such as a shared health summary, personal health summary and an advance care plan.
- **Hidden:** Patients, their healthcare providers and their representatives cannot view this document in the patient's record. To view this document, patients or their representatives need to reinstate the document.
- **Removed:** Patients, their healthcare providers and representatives cannot view this document in the patient's record, even in a medical emergency.

During a consultation or healthcare event, patients can also request that certain documents are withheld from My Health Record. However, a healthcare organisation or specialist is under no obligation to offer patients the opportunity to review every document uploaded to their record.

By default, documents in an individual's record are set to general access for healthcare providers. This means you can view all documents within an individual's record, except for information that has been entered in the consumer-only notes section of the record, and any documents that the person has previously removed.

The My Health Records Act generally overrides specific state or territory requirements relating to patient consent. However, in the Australian Capital Territory, New South Wales and Queensland, consent is still required to upload certain types of sensitive information. These consent requirements are listed in clause 3.1.1 of the *My Health Records Regulation 2012*.

The Agency has a range of step-by-step guides available to support your patients when interacting with My Health Record, including uploading a personal health summary, setting privacy controls and a range of other functions.



How to implement My Health Record

In a hospital setting

Use of My Health Record in a hospital setting allows a continuity of information between the hospital system and community care. You will be able to view all the document types outlined in the descriptions above. If the hospital utilizes My Health Record compliant software, you will be able to upload information to patients' My Health Records, which can then be used by other healthcare providers involved in their care. When the hospital uses My Health Record through the web-based National Provider Portal (more information on this below), you can view documents but cannot upload documents yourself.

Hospitals that wish to register for the My Health Record system should contact their local health department eHealth team or the Australian Digital Health Agency Provider Readiness team.

You can find the list of public hospitals connected to My Health Record here and a list of private hospitals connected here.

In private practice

Whether your practice has conformant clinical software or not, every organisation using My Health Record will need to register before linking it to their practice.

Determine registration type

There are two types of registration:

- **A seed organisation** is a legal entity that delivers healthcare services such as a local GP practice, pharmacy, or private medical specialist.
- **A network organisation** is part of a wider 'network hierarchy' (under the responsibility of a seed organisation). Network organisations more commonly represent different departments or divisions within a larger complex organisation, such as a hospital, multi-disciplinary healthcare practice; or different branches of a larger health organisation.

Most private practices will register as a seed organisation.

Establish roles and responsibilities

As part of the registration process, each organisation must nominate individuals to carry out certain activities to do with My Health Record.

These roles are:

- **Responsible officer** (RO) must be registered with the HI Service and have authority to act on behalf of the organisation in its dealings with the My Health Record System Operator and the HI Service. The RO is often the business owner in a small practice, or the CEO of large organisations like hospitals.
- **Organisation maintenance officer** (OMO) is registered with the HI Service and is authorised to interact on behalf of the organisation in its day-to-day administrative dealings with the My Health Record System Operator and HI Service. Your organisation can have more than one OMO.

Manage compliance

Use of healthcare identifiers and access to My Health Record are governed by the:

- *Healthcare Identifiers Act 2010* (Cth) (HI Act)
- *Healthcare Identifiers Regulations 2010*
- *My Health Records Act 2012* (Cth)
- *My Health Records Rule 2016* (Cth)
- *My Health Records Regulation 2012* (Cth)

My Health Record system policy

As part of your organisation's legislative requirements to participate in My Health Record, your practice will need to have the relevant policies and procedures in place including:

- My Health Record system and access policy; and
- National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) Certificate policy if your practice is accessing My Health Record via conformant clinical software.

The RACS My Health Record security and access policy template has been developed to support specialists in private practice. The template is available to download from the College website and you can also find it in the appendix below. This policy must be in place before your organisation can register to participate in My Health Record. It must address the specific matters specified in the template, and must be provided to the System Operator on request and reviewed at least annually.

Recognise privacy and security obligations

Establishing and maintaining information security practices is an essential professional and legal requirement when using digital health systems in the delivery of healthcare services.

The My Health Records Rule 2016 sets out the security requirements that participating organisations must comply with to be eligible to be registered and remain registered in the My Health Record system. Non-compliance with the My Health Records Rule can result in cancellation of participation and other penalties.

Your organisation must document and implement the internal practices and procedures that it uses to protect personal information when using My Health Record. These include:

- **Managing user accounts** – this must list all staff (including names and positions) who have access to My Health Record, and must be regularly updated. It must also outline the ways in which passwords are kept up to date and sufficiently complex, and the processes regarding suspending and terminating user accounts when staff depart the organisation or when their role no longer requires access to My Health Record.
- **Identification of staff** – Clinical software is used to assign and record unique internal staff member identification codes, including a Healthcare Provider Identifier-Individual (HPI-I), when applicable.
- **Handling of privacy breaches and complaints** – your organisation must show the reporting procedure to allow staff to inform management regarding any suspected security or privacy issues or breaches of the My Health Record system. Your organisation must also keep a log of any suspected breach, including time and date, the user account associated with the breach, and whose patient information was accessed (if known).
- **Risk assessments** – your organisation must show processes for undertaking periodic risk assessments of how staff use My Health Record, the organisational ICT system, and create improvements as needed.

Organisations must put in place a yearly audit to ensure all policies remain relevant to My Health Record access permissions.

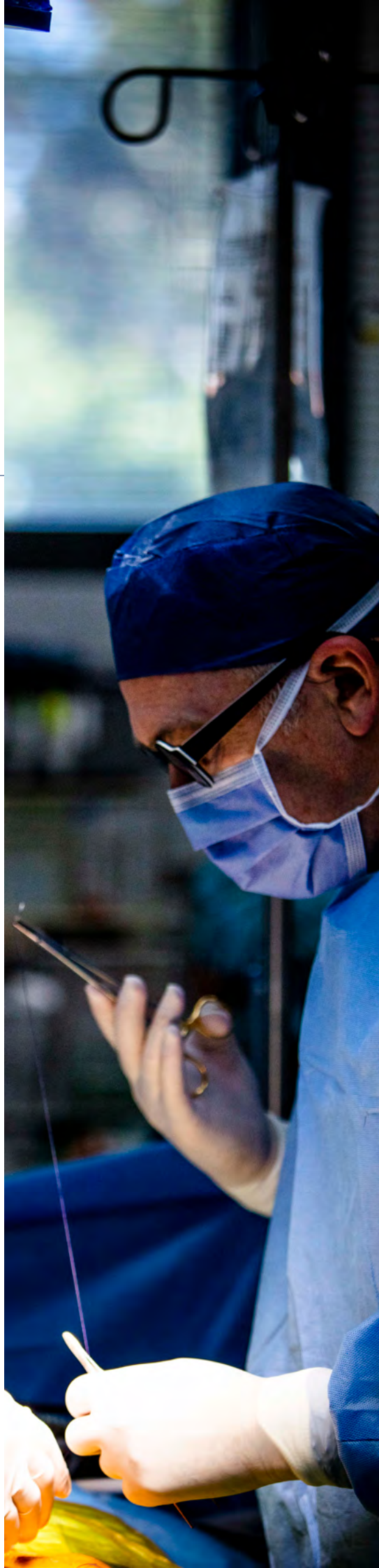
For more information about the above please refer to the Australian Digital Health Agency's My Health Record Security and access policy checklist webpage.

Implement staff training

All staff requiring access to My Health Record, as part of their role in healthcare delivery, will need to undergo training before accessing the system. Training will include accurate and responsible use of My Health Record, legal obligations of users and consequences for breaching obligations (see paragraph 42(4)(b) of the My Health Records Rule).

The Australian Digital Health Agency (can provide training for you and your practice staff, including CPD eLearning modules.

For more information, go to the 'support' section of this guide.



How to register for My Health Record

Every healthcare organisation needs to be registered with the Healthcare Identifiers (HI) Service before they can connect to My Health Record. Most small private practices will need to register as a seed organisation.

Once your registration is confirmed, the healthcare organisation will receive a unique, 16-digit number called a Healthcare Provider Identifier – Organisation (HPI-O). If you believe you already have the 16-digit number but are unsure what it is, contact the HI Service enquiry line on 1300 361 457.

Register to access via conformant clinical software

1. The RO must register for a Provider Digital Access (PRODA) account. This requires three forms of identification. https://proda.humanservices.gov.au/
2. Register with the Healthcare Identifiers (HI) Service. To find out how to register, visit https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/register-your-organisation
3. Check if your clinical information system (CIS) Is conformant. A list of conformant software can be found here: https://www.myhealthrecord.gov.au/for-healthcare-professionals/conformant-clinical-software-products
4. If your CIS is conformant, apply for a NASH PKI certificate. For information about how to apply, visit this webpage https://www.servicesaustralia.gov.au/organisations/health-professionals/services/medicare/national-authentication-service-health
5. Contact your software vendor to setup and configure.

Register to access via the National Provider Portal

If your organisation does not use conformant clinical software, you can access My Health Record through the National Provider Portal (NPP). The NPP is a view-only platform that allows healthcare providers to view and download their patient's records.

To access, you will need to:

1. Register for your individual PRODA account
2. Register your organisation/practice with the HI Service and My Health Record
3. Link your healthcare provider individuals to your organisation.

More about how to access via the National Provider Portal: https://www.myhealthrecord.gov.au/sites/default/files/accessing_my_health_record_via_the_national_provider_portal_factsheet.pdf?v=1592533765

My Health Record registration flowchart

Register for My Health Record in Health Professional Online Services (HPOS) via Provider Digital Access (PRODA)

Does the RO, OMO or Healthcare individual have a PRODA account

YES

NO

Login to PRODA

Create a PRODA Account

For PRODA support contact Services Australia: 1800 700 199 or proda@servicesaustralia.gov.au or find support information online

Is the organisation registered with the HI Service

For HI Service support contact the HI Service Enquiry line: 1300 361 457 or find support information online

YES

NO

Register your seed/network organisation with the My Health Record using HPOS

Register your seed/network organisation with the HI Service and My Health Record using HPOS

You will need:

- 3 Government issued documents
- Personal email address
- 3 Security questions

Does the organisation have conformant clinical software

YES

NO

For PKI Certificate support contact the Services Australia eBusiness Service Centre for Medicare certificates: 1800 700 199 or ebusiness@servicesaustralia.gov.au or find support infor

Apply for organisational National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) in HPOS

NASH PKI Certificate received – configure in software

Start accessing My Health Record through clinical software

RRO to link all relevant HPI-Is to the HPI-O in PRODA

Start accessing My Health Record through the National Provider Portal

Note: Other clinical providers require their HPI-Is to be recorded in their clinical software

How to use My Health Record

Being able to view important clinical information from other healthcare providers is the primary purpose of My Health Record. Each clinical software has its own 'look and feel' for how it displays information in the My Health Record.

Healthcare providers are under no legal obligation to use My Health Record. It is up to the healthcare provider and their clinical judgement as to when and how they use the system.

Examples of when to use My Health Record include:

- At a first consultation – a patient's My Health Record might be useful for information on medication, existing medical conditions or hospital visits.
- After hospital discharge – this may be useful for information about patients' clinical synopsis, interventions, diagnosis, and medications.
- The referral is missing information and/or the patient cannot recall their medical history – a patient's My Health Record could provide missing information if the patient cannot recall their medical history.
- After an after-hours GP visit – the GP may have uploaded information about any new medications and/or an event summary describing the visit.
- After an incident on holiday – The GP or practitioner may have uploaded an event summary, or medication and prescription details may have changed.
- In an emergency – a patient's My Health Record could provide information on allergies, immunisations, medications and medical conditions in the case of an emergency where the patient is unable to provide information. The patient may have recorded information about an adverse reaction or a new complementary medicine they are taking.

Authority to view

Any person involved in an individual's healthcare who is authorised by the healthcare organisation can access their My Health Record. Access is not limited to clinicians with a Healthcare Provider Identifier - Individual (HPI-I).

Healthcare providers are also authorised to:

- disclose the health information to the individual, or their authorised or nominated representative
- collect, use or disclose the health information for any purpose with the consent of the individual
- collect, use or disclose the health information for purposes relating to the provision of indemnity cover for a health care provider.

Viewing information on My Health Record

Under the *My Health Records Act 2012* (Cth), healthcare providers working in registered healthcare provider organisations can:

- Access an individual's My Health Record at any time as part of providing healthcare to the patient (e.g. during, prior and after a consultation, or a clinical event involving the individual);
- View all documents in the My Health record, unless the patient has restricted access.

In addition to clinicians, a healthcare organisation may authorise other staff to access My Health Record as part of their role in healthcare delivery. This must be noted in the organisation's My Health Record access policy.

If your organisation does not use conformant clinical software, you can still view a patient's My Health Record through the NPP. Watch this video to learn how to navigate a patient's record through the NPP.

Uploading information on My Health Record

If your practice is authorised and registered with My Health Record, you may upload information to the My Health Record under the *My Health Records Act.*

When uploading information to My Health Record, you should consider whether the information will benefit other healthcare providers and your patient. Ensure the information you are uploading is accurate, up to date, complete and relevant, having regard to the purpose of the disclosure in accordance with your obligations under Australian Privacy Principle (APP) 10 of the *Privacy Act 1988* (Cth) (Privacy Act). Any information being uploaded must be authored by someone with an HPI-I, i.e. admin staff may upload but only if the information was prepared by a healthcare provider.

When not to upload information on My Health Record

Your organisation must comply with the patient's request if they ask you not to upload a particular document or information to My Health Record. This is a condition of your organisation's registration with My Health Record. You can advise the patient about the potential risks of excluding information from their record and explain the benefits of ensuring all information is included. However, you must comply with their final decision, and not upload the information if this is requested.

The *My Health Records Act* recognises that under some state and territory laws consent

must be given expressly, or in a particular way, before information related to specific areas of health is disclosed.

Authority to upload

Under the *My Health Records Act*, there is no requirement for a healthcare provider to obtain consent on each occasion before uploading clinical information. There is also no requirement for a patient to review clinical information prior to it being uploaded.

It may be considered good clinical practice to advise a patient that you will be uploading information to My Health Record, particularly if this information might be considered sensitive.

Further, advising the patient you will be uploading the clinical information to their record aligns with your obligations under the APPs and the Privacy Act.

Emergency access

The emergency access function only applies to those My Health Records where a patient has put an access code in place. There are certain urgent situations where it may be permissible for a healthcare provider to override any restrictions a patient has placed on their record by using an emergency access function available through your clinical information system. This is referred to as a 'break glass' function.

It is expected that the need to use the emergency access function will be rare, as emergency access is only authorised under the *My Health Records Act 2012 (Cth)* if:

- there is a serious threat to an individual's life, health or safety and the record holder's consent cannot be obtained (for example, due to being unconscious), or
- there are reasonable grounds to believe that access to the My Health Record of that person is necessary to lessen or prevent a serious threat to public health or safety. For example, to identify the source of a serious infection and prevent its spread.

Use of the emergency access function is recorded in the access history of the My Health Record, which can be viewed by the individual and their authorised or nominated representative(s). Any access controls that the individual has set will be overridden when emergency access is activated. This means that you will have full access to the individual's record except for information that has been entered in the consumer-only notes section, and any documents that the person has previously removed. The emergency access period lasts for five days, after which the organisation may use this function again if the emergency remains.

Emergency access is audited, and practitioners will be required to provide a justification for its use.

How specialists use My Health Record – case study

Jill Tomlinson, a Melbourne based plastic and reconstructive surgeon, uses My Health Record in her practice. She provided a recent example of how she used My Health Record when treating a patient:

"Earlier this week I saw an elderly patient via video consultation. She had been referred to me by another surgeon for a hand problem and she hadn't completed her patient registration forms so I didn't have a list of the patient's usual medications or medical problems. Her daughter was able to prompt her for the name of two important immunosuppressive medications that she was taking, and they were able to describe in general terms (without the disease name) the medical problem that she takes them for. They are highly relevant for the problem that she was seeing me about. I was able to use My Health Record to look up what medications she has had dispensed in the last 12 months. I had hoped that she would have a sShared hHealth sSummary that would allow me to see a list of her previous medical problems, and her usual GP's details (again, these were not included on the referral from the surgeon she had seen once about the hand problem she'd been referred to me about), so that I could easily copy her GP in my correspondence, and keep her GP informed via a letter that I send via secure messaging."

Jill describes another situation in which My Health Record was useful for accurate information about medication and information relevant to other practitioners involved in the patient's care:

"Today I saw a patient who requires minor hospital surgery. The referral from his GP listed one medication for gout, and the presenting complaint (the condition requiring minor hospital surgery), and nothing under "past history". The patient has an organ transplant so is on multiple immune suppressing medications, is on insulin for diabetes and takes blood thinners following cardiac stenting. My Health Record has a full list of his medications. It also lists attendances and therefore the name of the treating renal physician who I will, with the patient's permission, copy into correspondence."


KLS martin
PROPERTY

Support

Resources

The Agency has a range of resources available to support you and your practice staff with My Health Record:

- *Digital Health Specialist Toolkit*

  Launched in February 2021, the Digital Health Specialist Toolkit is designed to support the adoption of digital health by specialists. The toolkit includes fact sheets, user and implementation guides, FAQ sheets and continuing professional development (CPD) modules on a range of topics including electronic prescriptions, telehealth, secure messaging, and My Health Record. It is available here: https://specialist-toolkit.digitalhealth.gov.au/.

- *eLearning modules*

  Each training course provides an introduction to My Health Record and outlines the benefits, features and functionalities of the system. Enrolment is free.

  https://training.digitalhealth.gov.au/enrol/index.php?id=24

- *Clinical software simulators and summary sheets*

  Healthcare practitioners can simulate use of My Health Record for a range of clinical software products available via https://onlinetraining.digitalhealth.gov.au/ using the following login details:

  - Username: OnDemandTrainingUser
  - Password: TrainMe

Factsheets and checklists:

Registration overview

https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/register-your-organisation

Using My Health Record in a specialist practice

https://www.myhealthrecord.gov.au/sites/default/files/hd110_providers_factsheets_specialists_20190228_v2.2_wr.pdf?v=1552005426

Accessing My Health Record via conformant software

https://www.myhealthrecord.gov.au/sites/default/files/accessing_my_health_record_via_conformant_software_factsheet.pdf?v=1592533839

Accessing My Health Record via the National Provider Portal

https://www.myhealthrecord.gov.au/sites/default/files/accessing_my_health_record_via_the_national_provider_portal_factsheet.pdf?v=1592533765

Factsheets for your patients

https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/support-your-patients

Security Practices and Policies Checklist

https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/security-practices-and-policies-checklist

All factsheets and guides

https://www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/fact-sheets-and-guides

Education and training sessions

The Agency can provide tailored training sessions for you and your organisation. To request an education or training session, please email: education@digitalhealth.gov.au.

Contact

My Health Record Helpline
(Available 24 hours, 7 days a week)

Phone: 1800 723 471 (select option 2)

Australian Digital Health Agency
(Monday to Friday, 8am – 5pm)

Phone: 1300 901 001

Web: www.digitalhealth.gov.au

Email: help@digitalhealth.gov.au

Healthcare Identifier (HI) Service
(e.g. HPI-Is, HPI-Os and IHIs)

Phone: 1300 361 457

Email: healthcareidentifiers@servicesaustralia.gov.au

PRODA Help
(Monday to Friday, 8am – 5pm)

Phone: 1800 700 199 (select option 1)

Email: proda@servicesaustralia.gov.au

Health Professional Online Services (HPOS) Help

Phone: 132 150

Services Australia eBusiness Service Centre for Medicare Certificates (e.g. NASH PKI)

Phone: 1800 700 199

Email: ebusiness@servicesaustralia.gov.au

Office of the Australian Information Commissioner (OAIC)

Phone: 1300 363 992

Web: www.oaic.gov.au

Appendix A: Checklist for practitioners setting up My Health Record in private practice

	Prepare for registering with My Health Record
☐	Understand your organisation structure (e.g. seed or network organisation)
☐	Establish roles and responsibilities (e.g. RO and OMO)
	Manage compliance
☐	Implement a My Health Record system policy
☐	Recognise privacy and security obligations
☐	Implement staff training The Recommended Training Checklist and Declaration assists healthcare organisations with guiding and tracking My Health Record training according to the participant obligations.
	Register access via:
☐	a) Conformant software, or • Refer to the step-by-step factsheet for registration to use My Health Record via a conformant clinical information system.
☐	b) the National Provider Portal (NPP) • Refer to the step-by-step factsheet for registration to use My Health Record via NPP.
	Configure software
☐	Contact your software vendor or IT support
☐	Confirm HPI-O and HPI-I numbers have been configured into software
☐	Software settings are updated to ensure permission for staff accessing My Health Record
☐	Check if conformant software can access My Health Record
	Inform and support patients

Appendix B: RACS My Health Record Access and Policy Template

My Health Record security and access policy template

Royal Australasian College of Surgeons, version no. 1, September 2021

This policy has been developed to support surgeons, practice managers and staff with meeting their My Health Record compliance obligations. The Australian Digital Health Agency https://www.digitalhealth.gov.au/ and the College https://www.surgeons.org provide a range of digital health support for Fellows.

My Health Record policy

This policy applies to all fellows, employees and contractors affiliated with ORGANISATION NAME. The policy can be accessed through the ORGANISATIONAL MY HEALTH RECORD OFFICER.

Governance

Responsible Officer (RO):

Organisation Maintenance Officer/s (OMO): [identify the contact person here. If an employee has any questions about this policy or their obligations, who can they talk to?]

Access

Authorised staff will access the My Health Record system via:

An up-to-date list of individual healthcare providers authorised to access the Provider Portal will be provided to the System Operator (SO) by:

Authorised staff will be provided with a unique user account to access the My Health Record system via conformant software by:

The level of access granted to individual staff will be determined and documented by: *[Outline the process by which individual staff will be granted access. Who determines who has access, and how and where is it documented. Is it documented by a different person to the person authorising access? State clearly who occupies each role and what they are responsible for]*

Access flags will be assigned by:

Access records will be maintained by:

Security

User account information and access will be managed by:

Account passwords will be changed by users every:

Staff will report any suspected security breach to: [Identify the staff member to whom breaches will be reported and outline the process for reporting breaches; i.e. a form that might need to be filled out, timelines and explanation of potential outcomes]

Confirmed security breaches will be reported to the relevant authority by: *[Identify the staff member responsible for confirming that a security breach has occurred and identify who will be reporting it to the relevant authority]*

A log of security breaches including date and time of the breach, user account involved, patient information accessed (if known), and mitigation strategies employed will be maintained by: *[Identify the individual responsible for investigating security breaches, and the individual responsible for maintaining records of the details of said breaches]*

A risk assessment of information and communications technology (ICT) systems and physical file storage systems to identify and mitigate potential privacy and security risks associated with My Health Record system access is conducted every:

Training

Training is mandatory for all individuals who will be authorised to access My Health Record. Training will be organised for all authorised staff before they first access the My Health Record system, and to refresh their knowledge with continuing optional training, by:

A register of staff training including the names of those who have completed training and the date training was completed will be maintained by:

Training will be reviewed to ensure currency and updated as required (i.e. if new functionality is introduced into the system) every:

Clinical incidents

Clinical incidents will be reported to the relevant party by:

A log of reported clinical incidents will be maintained by:

Clinical incident management is the responsibility of: *[Identify the individual/s responsible for investigating and maintaining records of incidents]*

If patients have a complain about the handling of their personal information, they should first contact the organisation, who will assist with resolving it. If the response is not satisfactory, patients should contact the My Health Record Helpline on 1800 723 471. *[Explain whether there's a delineation between the types of complains referred to the helpline and the types of complains referred to the named officer, and the process for furthering complaints]*

Notes and definitions

Governance

Responsible officer (RO): has legal responsibility for the understanding of and compliance with this policy and compliance with My Health Record legislation (e.g. practice manager).

Organisation maintenance officer (OMO): undertakes the day-to-day administrative tasks in relation to the Healthcare Identifiers (HI) Service and the My Health Record system. An OMO needs to be familiar with the IT system used by the practice.

- OMO is responsible for understanding, implementing and compliance monitoring of the My Health Record system security and access policy, and for maintenance of the policy on behalf of the practice.
- An organisation can have multiple OMOs and the RO can also take on the role of the OMO.

Access

Authorised staff: Staff are only authorised to access the My Health Record system where access is required for the provision of patient care by the authorised employee or by a healthcare provider employed by the organisation. The authorised employee will maintain a record of authorised Healthcare Provider Identifier – Individual (HPI-I) numbers, and the level of access granted, as well as records of any other individuals who have authorised access, in the clinical software and in the organisation's internal records. In the case of the authorised employee leaving the organisation, relinquishing duties related to maintaining the information, or has their security compromised, access will be removed immediately.

Provider Portal: the 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. Where individual healthcare providers are authorised to access the My Health Record system using the Provider Portal, the OMO will establish and maintain an accurate and up-to-date list of individuals with the System Operator. If an individual healthcare provider is no longer authorised to access the My Health Record system via the Provider Portal on behalf of the organisation, the OMO will ensure the System Operator is informed and the individual removed from the list of authorised users.

System Operator is the Australian Digital Health Agency. To contact the Agency regarding issues with the My Health Record system, phone the My Health Record Helpline (1800 723 471).

Unique user account: The clinical information 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 will use their individual user account to access the My Health Record system at all times.

Level of access: It is a criminal offence for anyone other than a person authorised by the healthcare organisation to access a patient's My Health Record. Staff may be granted full access (i.e. ability to view and upload records) or view-only access as determined by the duties of their role, including practice staff whom may be granted a view access to the My Health Record system to assist clinicians in performing certain tasks.

Access flags: Means an information technology mechanism made available by the System Operator to define access to a consumer's digital health record. Where appropriate to the size and complexity of the healthcare organisation, the RO/OMO will define an appropriate network hierarchy for the organisation and assign access flags appropriately for the structure of the organisation. The network hierarchy will define the seed organisation, the network organisations that fall under that seed organisation, and the network organisations for which access flags are appropriate. In setting and maintaining access flags, the RO/OMO will ensure that:

- Patients are able to determine and control access to their My Health Record in a way that meets reasonable public expectations. Network organisations that would not be expected by patients to be connected will thus have their own access flags.
- The organisation is able to share health information internally in an appropriate manner that prevents security breaches. The RO/OMO will undertake reviews of the network structure and access flag assignments at such times as the structure changes, or in the case that a System Operator or patient query reveals potential structural issues. The organisation commits to making reasonable changes in line with requests from the System Operator.

Access records: Records that identify which user accessed the system via conformant software on a particular day. The OMO will determine whether the practice software keeps a record of the individual staff members assigned to a particular user account. If not, the OMO will create and maintain a separate record which details the links between user accounts and individual staff. These records must be maintained to allow audits to be conducted by the System Operator at their discretion or as part of clinical incident management.

Security

Security breach: Instances of unauthorised collection, use or disclosure of health information included in a patient's My Health Record, e.g. when a staff member with access to the My Health Record system discovers that someone else may have gained access to their user account. Organisations are also required to report events or circumstances that could have resulted in a security breach.

Relevant authority: Where a security breach is confirmed, the breach will be reported to the relevant authority and the System Operator. The police will be notified of all security breaches. If patient data is compromised, the Office of Australian Information Commission will be notified. If the breach involved or may have involved the My Health Record system, the System Operator will be notified.

Mitigation strategies: In the event of a security breach, the RO/OMO will undertake appropriate mitigation strategies including but not limited to:

- suspending/deactivating the user account
- changing the password information for the account

- reporting the breach to the police, and the System Operator and the Office of Australian Information Commission as relevant.

Risk assessment: Includes the assessment of:

- potential for unauthorised access to the My Health Record system using the clinical information system, and associated mitigation strategies if required
- potential for misuse or unauthorised disclosure of information from a patient's My Health Record by persons authorised to access the My Health Record system, and associated mitigation strategies if required
- potential for accidental disclosure of information contained in a patient's My Health Record and associated mitigation strategies if required
- increasing risks and potential impact of the changing threat landscape (e.g. newer types of security threats such as ransomware), and associated mitigation strategies if required
- any relevant legal or regulatory changes that have occurred since the last review, and associated mitigation strategies if required.

Training

My Health Record system training: Staff training will be provided to employees before they are authorised to access the My Health Record system. The training will provide information about how to use the conformant clinical software and/or the National Provider Portal, in order to access the My Health Record system accurately, responsibly, and will include privacy training. Training will incorporate information about the legal obligations of organisations and individuals utilising My Health Record and the consequences of breaching these obligations. Training will utilise materials approved by the Australian Digital Health Agency.

New functionality: As a general rule, when new functionality is introduced into the My Health Record, there is a version upgrade and release to practice management software. Training material produced by the Agency and/or peak organisations will be updated to reflect new functionalities as they become available and published for public use. Additional training for staff with authorised access may need to be provided using the updated training material.

Clinical incidents

Clinical incident: an event or circumstance that resulted, or could have resulted, in unintended and/or unnecessary harm to a patient and/or a complaint, loss or damage. A clinical incident can be related to safety, usability, technical, privacy and/or security issues. The incident may relate to the My Health Record system directly, or the behaviour of clinical software when interacting with the My Health Record system.

Relevant party: Clinical incidents will be reported to the relevant party at the time of occurrence. In the first instance, the relevant party is the System Operator which can be contacted via the My Health Record Helpline (1800 723 471). The System Operator will triage the clinical incident and refer as necessary.

Patient complaints

Patient complaints: Patients will be made aware of the process for raising issues or complaints.

- Patient complaints raised in relation to unauthorised access to their My Health Record will be investigated.
- Unauthorised access will be managed through complaint management and staff performance management processes.
- If the unauthorised access is found to be by someone other than an employee, the patient and the complaint will be referred to the management of that service and/or the Office of the Information Commissioner.
- Where a patient requests a document is removed or amended, the request will be logged with the OMO and the document removed, or a new amended document uploaded, within 7 days. If amendment or removal is not considered appropriate, the patient will be directed to exercise their personal controls over the document.

Assisted registration

Assisted registration will not be provided.

Policy review

This policy will be reviewed annually, or when any new relevant material or risks are identified. An annual review will occur even when no new relevant material or risks are identified. The review will consider factors that could lead to unauthorised access to the My Health Record system; the potential misuse or disclosure of patient records, the accidental disclosure of information from a healthcare recipients' My Health Record. The review will also consider any legal/regulatory changes effecting My Health Record policy and changes to the My Health Record system as listed under My Health Records Rule 2016: https://www.legislation.gov.au/Details/F2016C00607

Royal Australasian
College of Surgeons