

Handbook for Practice Managers

Version 2.1
June 2021

Approved for external use



My Health Record

aapm

Australian Association of
Practice Management

Contents

About My Health Record for practice managers	4
Glossary of terms	5
Understanding the Healthcare Identifiers (HI) Service	7
My Health Record registration	9
Understanding PRODA	10
Register for a PRODA account	10
Ensure at least one of your healthcare providers has a HPI-I before registering	10
Ensure the right person registers	10
Determine your organisation structure	11
Understanding the seed and network organisation structures	11
Network organisations	12
Access flags	12
Roles and responsibilities	13
Other digital health roles and responsibilities	14
How the roles might be set up in your organisation	15
Register for My Health Record access	16
Digital health certificates	16
Connecting to and using My Health Record	17
Access to the My Health Record system	17
Conformant clinical software	17
Linking healthcare providers to your organisation	17
Using the My Health Record system	17
National Provider Portal	17
Using PRODA To Access My Health Record through the National Provider Portal	18
Managing compliance	19
My Health Record security and access policy	19
NASH PKI Certificates Policy	19
Privacy and security compliance	20
Ongoing participation obligations	20
Strengthened privacy regulations	21

Patient consent	22
Limiting access	22
Refusal of consent to upload	22
Emergency access	22
Appendix A: Readiness checklist	23
Appendix B: Policies and procedures for the use of NASH PKI Certificate for Healthcare Organisations	28
Purpose	28
Policies and procedures	28
Staff responsibility	28
Related resources	28

About My Health Record for practice managers

This handbook is designed to assist practice managers to understand the overall process for registration of their practice (organisation) to access the My Health Record system. It is supported by the My Health Record Registration Guide for Practice Managers, a step-by-step guide to the registration process.

The handbook is supported with links to more detailed information, including a step-by-step checklist to take you through the process that is included in [Appendix A](#).

Need help?

If you need help at any time during the registration process, you can contact one of the help desks listed below.

My Health Record Support Centre

1800 723 471

Provider Digital Access (PRODA)

Help Desk: 1800 700 199

Healthcare Identifiers Service (HI)

Help Desk: 1300 361 457 for help registering an organisation in the My Health Record and the HI Service.

eBusiness Service Centre

1800 700 199 for help relating to progress a NASH PKI Certificate request and for support with HPOS & PRODA enquiries

NASH PKI Operations Team

1300 721 780

Online Technical Support

for software vendors

Glossary of terms

TERMS	DEFINITIONS
conformant software	Conformant software products have been assessed for conformance with national digital health requirements. This includes the ability to view a My Health Record, upload a shared health summary, upload prescriptions, provide assisted registration, and more.
CSP contracted service provider	A contracted service provider (CSP) in the My Health Record system is an organisation that provides technology services or health information management services relating to the My Health Record system to a healthcare provider organisation, under contract to that organisation. CSPs must be registered with the Healthcare Identifiers Service.
EOI evidence of identity	Evidence of identity is needed as part of the registration for a PRODA account.
HI healthcare identifier	A healthcare identifier is a unique number that has been assigned to individuals, and to healthcare providers and organisations that provide health services. The identifiers are assigned and administered through the HI Service which was established to undertake this task (see HPI-O and HPI-I).
HPI-I Healthcare Provider Identifier – Individual	This is the unique identifier number given to an individual healthcare provider. Any healthcare provider registered with Australian Health Practitioner Registration Authority (Ahpra) will have a number automatically issued to them. This number begins with 800361 and is 16 digits long. Health practitioners not registered by Ahpra can apply for a HPI-I from the Healthcare Identifiers Service.
HPI-O Healthcare Provider Identifier – Organisation	A healthcare provider identifier – organisation, is a number that is assigned to eligible healthcare organisations once they have registered with the HI Service, to support their unique identification. The HPI-O number begins with 800362, is 16 digits long and is required to register for the digital health record system.
HPOS Health Professionals Online Services	Health Professionals Online Services is a web-based service provided by Medicare that allows providers to send and retrieve various types of information to/from Medicare.
IHI individual healthcare identifier	An individual healthcare identifier is a 16-digit unique number used to identify individuals who receive care in the Australian healthcare system.
NASH National Authentication Service for Health	An individual healthcare identifier is 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.

TERMS	DEFINITIONS
network organisation	Network organisations stem from the seed organisation. They commonly represent different departments or divisions within a larger complex organisation (e.g. a hospital or multi-disciplinary healthcare practice). They can be separate legal entities from the seed organisation, but do not need to be legal entities.
OMO organisation maintenance 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 (if any) 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. In general practice, 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. Alternatively, the RO may take on the OMO role as well.
PRODA Provider Digital Access	Provider Digital Access is 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.
RO responsible officer	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. For large organisations, the RO may be the chief executive officer or chief operations officer. For small organisations (such as a general practice), the RO may be a practice manager or business owner.
seed organisation	Healthcare provider organisations participate in the My Health Record system either as a seed organisation only 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. A seed organisation could be, for example, a local general practice, pharmacy or private medical specialist.
Services Australia	Services Australia is an executive agency of the Australian Government, responsible for services such as Centrelink and Medicare.
System Operator	The System Operator for the My Health Record system is the Australian Digital Health Agency.

Understanding the Healthcare Identifiers (HI) Service

The purpose of the HI Service is to assign a unique national healthcare identifier for each patient, practitioner and healthcare organisation, to establish and maintain accurate records to support the communication and management of health information.

WHY DO I NEED TO USE THE HI SERVICE?

The HI Service is the fundamental building block for secure digital communication of health information between practitioners and the creation of a My Health Record. The HI Service allows healthcare providers to associate health information about an individual in a secure, consistent and accurate manner. Healthcare identifiers, one of the digital health foundations, are used in electronic documents such as discharge summaries, prescriptions and shared health summaries to correctly identify the patient, the healthcare provider and the organisation.

TYPES OF HEALTHCARE IDENTIFIERS

The HI Service operated by Services Australia allocates a unique 16-digit healthcare identifier number to patients, healthcare providers and organisations. The HI Service will give patients and healthcare providers confidence that the right health information is associated with the right patient at the point of care.

THERE ARE FOUR TYPES OF HEALTHCARE IDENTIFIERS:

1

IHI

Individual Healthcare Identifier:

Allocated to all individuals enrolled in the Medicare program or those who are issued with a Department of Veterans' Affairs card and others who seek healthcare in Australia.

2

HPI-I

Healthcare Provider Identifier – Individual:

Allocated to healthcare providers involved in providing patient care. A healthcare provider will only be issued with one HPI-I, which will uniquely identify them, does not expire and belongs to them as an individual.

3

HPI-O

Healthcare Provider Identifier – Organisation:

Allocated to organisations (such as a hospital or medical clinic) where healthcare is provided.

4

CSP

Contracted Service Provider: Organisation (most likely a software provider) that acts on behalf of a healthcare provider organisation supporting the secure delivery and management of health information.

A CSP can obtain healthcare identifiers from the HI Service, and use or disclose healthcare identifiers on behalf of the healthcare organisation. A CSP must apply to the HI Service for a registration number and cannot interact with the HI Service until a healthcare organisation has authorised it to do so. While this registration number appears similar to healthcare identifiers it is simply a registration number

There are two types of HPI-Os:

1

Seed HPI-O

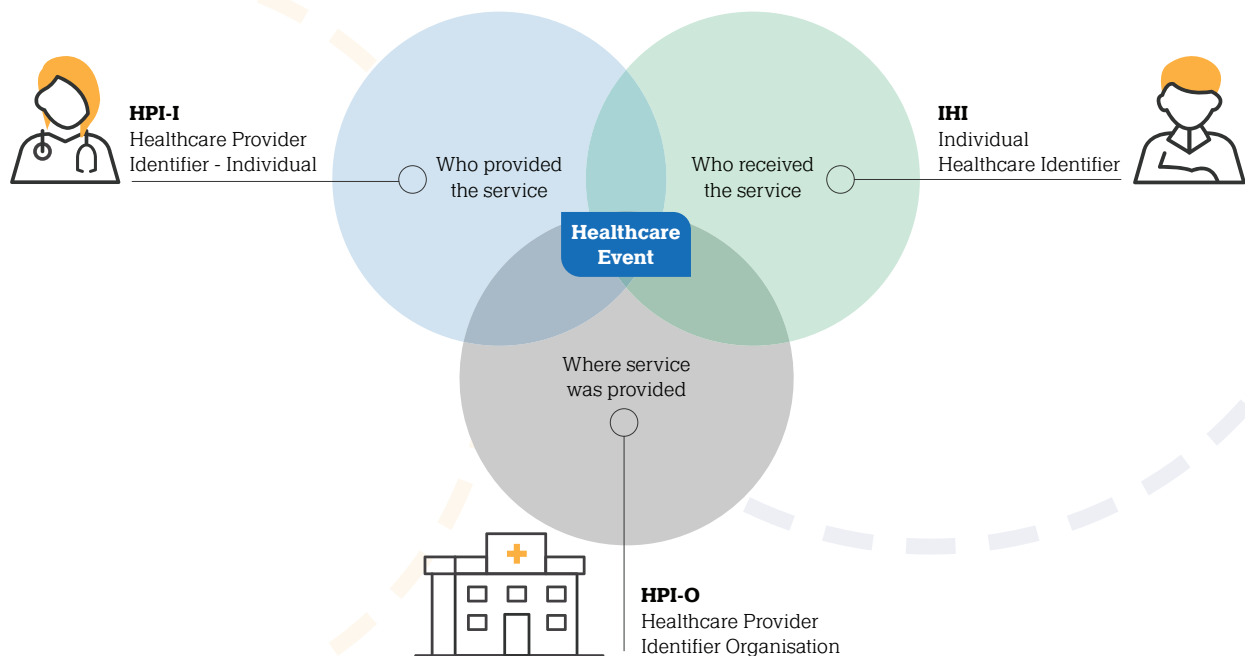
Seed HPI-O is any legal entity that delivers healthcare services within Australia, e.g. medical practices, community healthcare or hospitals.

2

Network HPI-O

Network HPI-O is a sub-entity of a seed HPI-O that provides healthcare services. For example, practices with multiple locations or hospital departments (such as a maternity ward, emergency department).

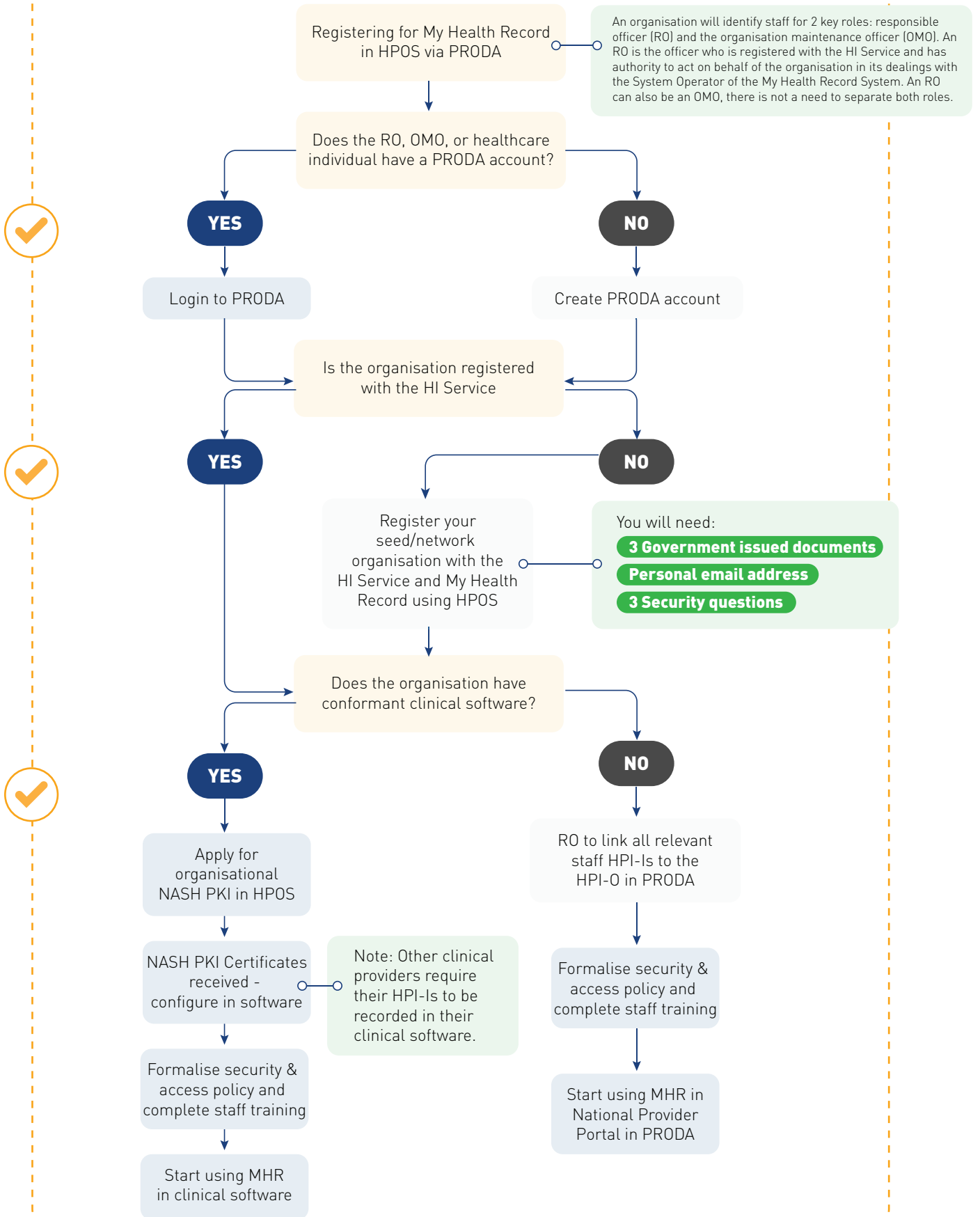
The illustration below shows the role of the three main healthcare identifiers in a healthcare event such as a consultation:



Find out more about registering your practice with the Healthcare Identifiers Service [here](#)

Healthcare providers such as GPs, allied health professionals and nurses registered with the [Australian Health Practitioner Regulation Agency \(Ahpra\)](#) are automatically registered with the HI Service and assigned a HPI-I number. Health professionals that are employed in a profession not regulated by Ahpra will need to apply for a HPI-I.

My Health Record registration



Understanding PRODA

If no one in your organisation has a [PRODA](#) account, it will be necessary to register for one in order to access HPOS (see below) and manage your practice's healthcare identifiers and access to the HI Service.

PRODA is an online authentication system to securely access government online services such as Health Professional Online Services [HPOS](#) and National Disability Insurance Scheme. It replaces Medicare PKI certificates, CDs and tokens.

Using a two-step verification process, you only need a username and password and access to a personal mobile phone or email account.

Anyone who works in healthcare services, whether you're a healthcare professional, practice manager or working within the administration team, is eligible to apply for a PRODA account.

Your PRODA account does not expire, it belongs to you as an individual. You can only register one PRODA account in your name. You must keep your PRODA account details secure and do not share the information with others. You should use your own personal information to set up your account (Services Australia need this to verify your identity) and to comply with the PRODA terms and conditions.

Register for a PRODA account

Ensure at least one of your healthcare providers has a HPI-I before registering

As long as at least one of your healthcare providers is registered with [Ahpra](#) you can continue to the next step. If your organisation does not have any Ahpra registered healthcare providers, at least one healthcare provider will need to apply for a HPI-I prior to your organisation registering for My Health Record. They can apply for a HPI-I via their HPOS account. See more information on [applying for a HPI-I](#). See [Ensure the right person registers below](#).

Ensure the right person registers

The person who makes decisions on behalf of the organisation, usually the owner or CEO, needs to be the person who applies for a PRODA account and subsequently for My Health Record access unless another person is given this authority. The applicant will need to provide [documentation](#) to verify their identity during the application process.

The applicant will become the organisation's responsible officer (RO) who has primary responsibility for the organisation's compliance with participation requirements in the My Health Record system. More information about the role of the responsible officer may be found below in the section [Roles and responsibilities](#).

The following will help you to understand these requirements:

- [System participation obligations](#)
- [Security practices and policies checklist](#)
- [Register your organisation](#)
- [Penalties for misuse of health information](#)

PRODA account details must match details on the Australian Business Register, otherwise evidence of their authority to act on behalf of the organisation must be provided. When there is a trust or a trading name, evidence will always be required.

Determine how you will access My Health Record

There are two options to access patients' My Health Records; via [conformant software](#) which allows healthcare providers to view and upload to their patient's My Health Record. For those without conformant software, the [National Provider Portal](#) allows healthcare providers access to view and download or print their patient's My Health Record information. There is no ability to upload patient information through the National Provider Portal. More information is available below in [Connecting to and using My Health Record](#).

More information can be found in the [My Health Record Practice Manager Registration Guide](#).

Establish a security and access policy

Understand the compliance requirements for accessing the My Health Record system and formalise a security and access policy for your organisation. [Further information and sample policy templates](#) can be found on the My Health Record website. [Read more about participation obligations](#).

Determine your organisation structure

When an organisation is registering with the HI Service, it is necessary to determine the appropriate structure, either as a seed organisation or a network organisation (see below). Most practices will register as a seed organisation. If there is any uncertainty, it is always best to register first as a seed organisation and change to a network organisation if necessary.

Understanding the seed and network organisation structures

Healthcare provider organisations participate in the My Health Record system either as a seed organisation only 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. A seed organisation could be, for example, a local GP practice, pharmacy or private medical specialist.

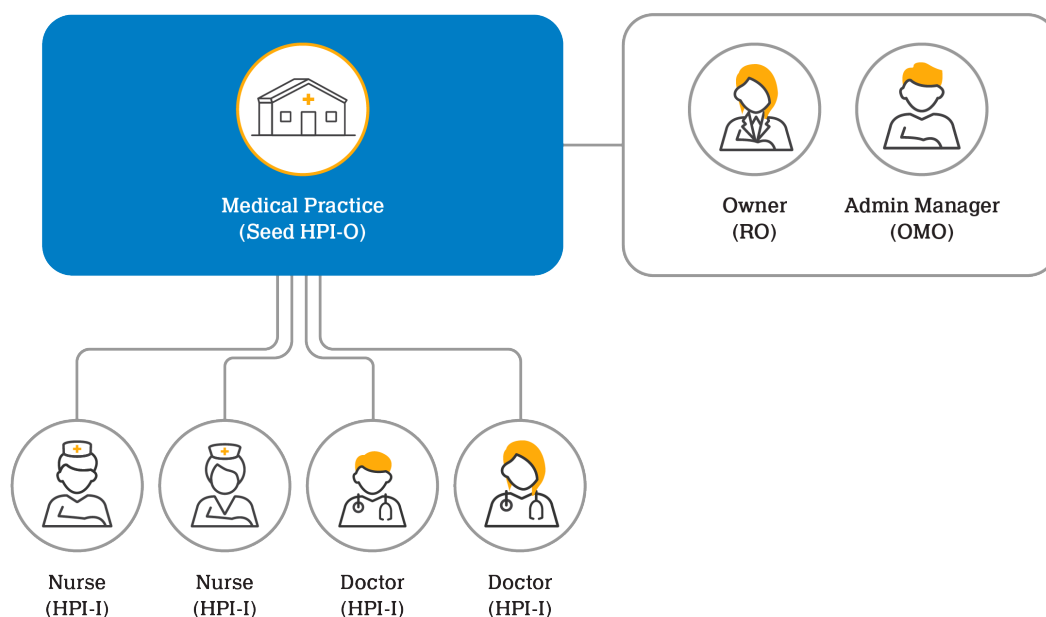
An example of a network organisation could be an individual department (e.g. pathology or radiology)

within a wider metropolitan hospital. A network hierarchy operating in the My Health Record system consists of one seed organisation and one or more network organisations.

The majority of healthcare provider organisations in Australia are independent – for example, general practices, pharmacies, private health specialists, or allied health care organisations. These will most likely participate in the My Health Record system as an independent seed organisation, rather than part of a network hierarchy.

Your seed organisation will identify staff for two key roles – the responsible officer (RO) and the organisation maintenance officer (OMO). An OMO can also be identified for a network organisation.

A Medical Practice – Example of a Seed Structure



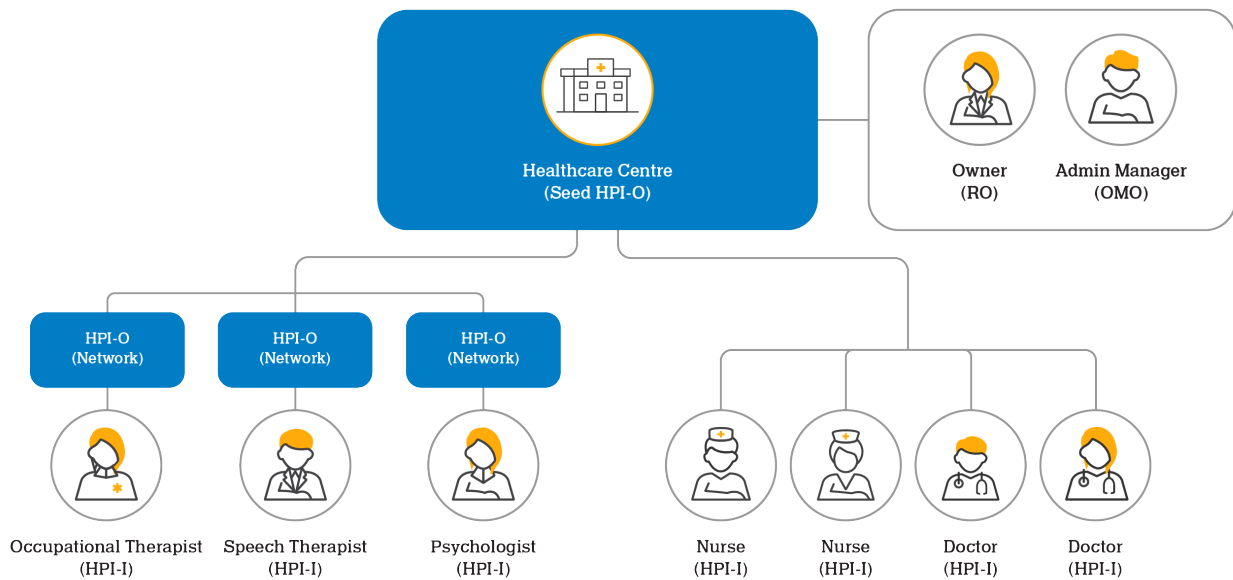
Network organisations

Whilst most healthcare organisations will register as a seed, some larger and more complex organisations may need to register as a network organisation.

If you want to add subordinate organisations under your parent organisation and ensure authority of those organisations, you may want to consider registering the other organisations as network organisations under the seed organisation you have just registered. Follow these steps: Select 'Manage Healthcare

Identifiers' > select the seed organisation that you are placing the network organisation under > select 'Add Organisation' > then follow the prompts. This will create a network organisation underneath the seed. You should be instantly provided with the new HPI-Os of the network organisations created. Then follow these steps to link these to My Health Record. Each network organisation will need their own NASH certificate.

A Healthcare Centre – Example of Seed & Network Structure



Access flags

Network organisations will need to set access flags when registering the organisation for My Health Record. Access flags are a key component of the My Health Record system's access control mechanisms, supporting the individual's capability to restrict the healthcare organisations that can access their My Health Record.

The level of detail for this capability is established when a healthcare organisation sets access flags.

Access flags are set by healthcare organisations in the My Health Record system, not in local systems. When a healthcare organisation is involved in the care of an individual and, as a result, is added to the access list for the individual's My Health Record, access flags determine if any other associated healthcare organisations are also added to the access list for the individual's My Health Record.



For more up-to-date information on [access flags](#), go to the Services Australia website.

Roles and responsibilities

The Healthcare Identifiers (HI) Service and the My Health Record system require certain people working in healthcare organisations to be assigned roles which authorise them to carry out certain actions on behalf of the organisation. The table below outlines the different responsibilities for each role in an organisation.



QUICK TIP:

Learn about how to manage RO/OMO in HPOS through the [Services Australia website](#).

Responsible officer (RO)

- The person 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 My Health Record System Operator (Australian Digital Health Agency). For large organisations, the RO may be the chief executive officer or chief operations officer. For small healthcare organisations, the RO may be a practice manager or business owner.
- The RO is also an OMO by default.

Organisation maintenance officer (OMO)

- The person who is registered with the HI Service and acts on behalf of a seed organisation and/or network organisations (if any) 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.
- In a healthcare organisation, this role may be assigned to the practice manager, or other senior staff who are familiar with the practice's clinical and administrative systems. Alternatively, the RO may also take on the OMO role.

HI Service

- Register a seed organisation
- Request a PKI certificate (or link an existing one) for the organisation
- Maintain the HPI-O details with the HI Service
- Maintain their own RO details with the HI Service (add or remove RO)
- Maintain OMO details with the HI Service (add or remove OMO) for seed and network levels
- Retire, deactivate and reactivate the HPI-O
- Maintain links between the seed organisation (and any network organisation/s) and any contracted service provider

- Maintain their own OMO details
- Validate, link or remove linked HPI-Is to HPI-O(s) they are linked to
- Request PKI certificate(s) (or link existing one) for organisation(s) they are linked to
- If required, maintain a list of authorised employees within the organisation who access the HI Service.
- Register a network HPI-O for lower network levels
- Register OMO details for lower network levels

My Health Record system

- Authorise the addition/removal of HPI-Os
- Adjust the My Health Record system access flags for participating organisations within their hierarchy (OMO at seed level can also do this)
- Set HPI-O/HPI-I authorisation links

- Set and maintain access flags according to the organisational network hierarchy, in accordance with meeting the principles outlined in the My Health Record Rules
- Set HPI-O/HPI-I authorisation links
- Act on behalf of the seed and network organisation(s) (that they are linked to) according to the hierarchy
- Maintain accurate and up-to-date records of the linkages between organisations within their network hierarchy



Find out more information about roles and responsibilities [here](#).

Other digital health roles and responsibilities

The following people are permitted to upload, view and download content in a person's My Health Record for the purpose of providing healthcare on behalf of a registered healthcare provider organisation and no other reason:

- Australian Health Practitioner Regulation Agency (Ahpra) registered healthcare providers (general practitioners, pharmacists, nurses etc)
- Healthcare providers issued with a Healthcare Provider Identifier - Individual (HPI-I) not registered with Ahpra (diabetes educators, dietitians, audiologists etc)
- Employees undertaking activities to support the provision of healthcare as part of the duties assigned to them by the organisation and as authorised under the healthcare provider's privacy policy in line with legislation.

A staff member can only access the My Health Record system if:

- they are authorised by the healthcare provider organisation to access the system and
- they are providing healthcare to that individual.

Participating healthcare provider organisations are required to document which employees can access the system as part of their My Health Record policy. This policy should also address the training that is provided to employees around use of the My Health Record system and their legal obligations and the consequences of breaching those obligations. Healthcare provider organisations are required to identify each person who accesses an individual's My Health Record and to provide that information to the System Operator when requested.

The following actions are not permitted:

- Browsing the record out of curiosity – or for any reason other than providing healthcare to an individual.
- Viewing or downloading content for insurance or employment purposes.
- Access by staff who do not have a designated role to support delivery of healthcare.

If a person deliberately accesses an individual's My Health Record without authorisation, criminal penalties could apply, including \$315,000 in fines and up to 5 years' jail time.

The My Health Records rules state healthcare provider organisations must have a policy on who is authorised to access the My Health Record system and that they must educate their staff on how to use the My Health Record system accurately and responsibly, including their legal obligations when using the system and the consequences of breaching those obligations. The My Health Records rules also state healthcare provider organisations must employ reasonable user account management practices around access to MHR, including identifying when staff access records.

Healthcare provider organisations are required by privacy law and confidentiality practice to ensure that health records in their organisation are only accessed by people with a need to access them. This requirement extends to their management of access to the MHR, and legislation specific to the MHR provides additional protections. They are required to ensure that their IT systems and the information they hold is kept safe and secure. Professional associations and colleges such as the AMA and RACGP provide guidance to their members on how to meet these obligations.

Other members of the practice team will hold roles within the organisation's digital health structure and each role will carry responsibilities.

More information about legislation and [penalties for misuse of health information](#) can be accessed via the My Health record website.

Healthcare provider (HPI-I): a healthcare provider with a valid HPI-I is able to perform all functions within the My Health Record system, except the administration functions that are managed by the RO or OMO, unless the healthcare provider holds one of those roles.

They are able to author and upload clinical documents as well as download documents from their patient's My Health Record, where the organisation authorises them to do so.

Healthcare providers who are registered with Ahpra will automatically be issued with a HPI-I when they register. Health professionals in a profession not regulated by Ahpra will need to apply for a HPI-I.

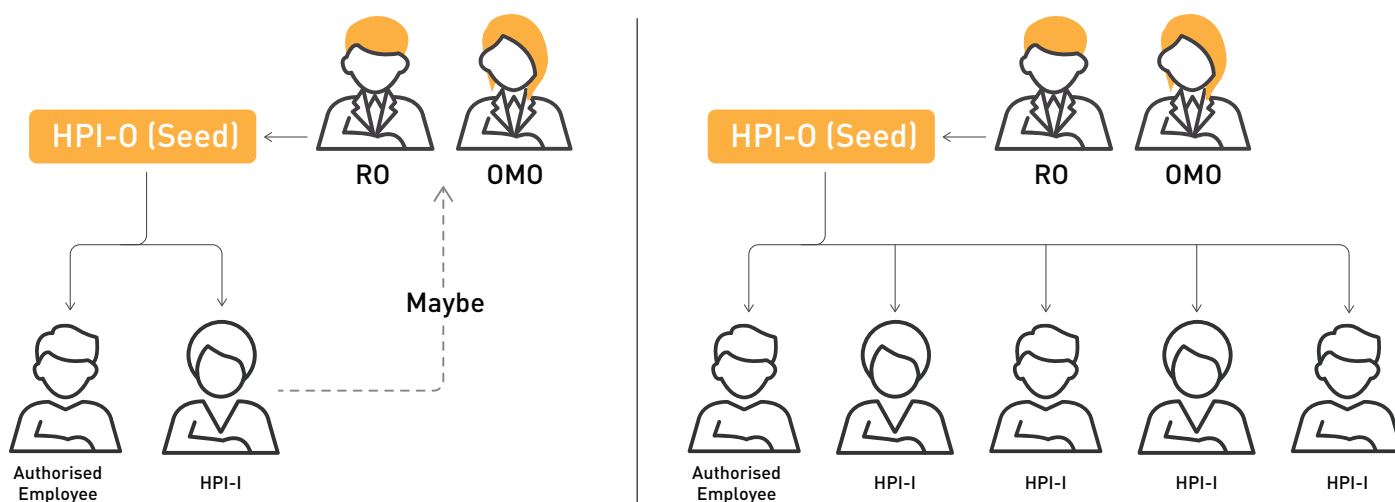
Authorised employee:

- **HI Service:** an individual within an organisation who requires access to provider identifiers and/or IHIs from the HI Service to assist with patient administration.
- **My Health Record system:** a person authorised by a healthcare organisation to access the My Health Record system on behalf of the organisation. Authorised users may be individual healthcare providers and other local users who have a legitimate need to access the My Health Record system as part of their role in healthcare delivery.

How the roles might be set up in your organisation

The diagram below illustrates how these roles might be set up for a seed organisation.

Seed only HPI



Further information about the different roles, examples of employee types, and appropriate actions for each role, can be found [on the My Health Record website](#).

Register for My Health Record access

Once a PRODA account is established, your organisation will need to apply for access to the My Health Record system. Your organisation will need to go through the registration process whether it has [conformant software](#) or will access the My Health Record via the National Provider Portal.

Following My Health Record system registration, your organisation will need to apply for a NASH (National Authentication Service for Health) Certificate to allow secure sharing of patients' health information.

Digital health certificates

Medicare and NASH certificates are used to access the My Health Record and your organisation will need both certificates to configure your software.

Once your organisation has both certificates, the RO or OMO will need to link the NASH certificate to the Medicare Site Certificate through HPOS.

It is a good idea to make a note of certificate expiry dates and set a reminder to check for the renewed certificate. If you downloaded the certificate from HPOS, you can check the expiry date on the HI Service Certificates tab.

See the section Digital health certificates below for more information.

A step-by-step guide for registering for My Health Record system access is available in the [My Health Record Practice Manager Registration Guide](#).

Healthcare organisations accessing the My Health Record system via clinical software require a NASH PKI Certificate for Healthcare Organisations. The NASH PKI Certificate for Healthcare Organisations Terms and Conditions require the healthcare organisation to have a set of policies and procedures in place governing use of the NASH PKI Certificate.

For more information and [support with NASH PKI certificates](#), go to the Services Australia website or call the eBusiness Service Centre on 1800 723 471.

Connecting to and using My Health Record

Access to the My Health Record system

There are two ways a registered healthcare organisation can access the My Health Record system:

1. **Conformant clinical** software allows healthcare providers to view, download and upload information and documents.
2. **The National Provider Portal (NPP)** allows healthcare providers only to view and download or print information and documents.

Note: Providers with conformant software may also use the NPP that has been set up on tablets and other mobile devices. For example, a healthcare provider doing a home or hospital visit without access to the practice's conformant software, may look at their patient's My Health Record using the NPP on their mobile device.

Conformant clinical software

Clinical software allows authorised healthcare providers to upload, view and download information from an individual's My Health Record. This type of clinical software is referred to as conformant software.

Contact your software provider for support in configuring your clinical software to enable access to the My Health Record system.

Each conformant software has its own 'look and feel' for how it displays information in an individual's My Health Record. Regardless of the type of software, all clinical documents are uploaded in a standardised format irrespective of the software being used. A list of conformant clinical software products is available [here](#).

Linking healthcare providers to your organisation

You will need to know the HPI-Is for all the healthcare providers in your organisation who will have access to My Health Record. HPI-Is can be obtained from the healthcare provider's Ahpra account or by contacting the HI Service.

When healthcare providers leave your organisation, it will be necessary to remove the link to your organisation using a similar process.

Using the My Health Record system

Once your organisation has completed the registration process, linked the HPI-Is to the organisation (HPI-O) and configured the software, it is technically ready to start using the My Health Record system. There are a few more important steps to ensure that your organisation develops appropriate policies and procedures so that it complies with legislation around use of the My Health Record.

See more information on '[Managing compliance](#)' and '[Ongoing participation obligations](#)'.



QUICK TIP:

Rule 42 of the My Health Records Rule 2016: health provider organisations need to have a [written policy](#) that reasonably addresses a range of matters, including how they authorise people to access the My Health Record.

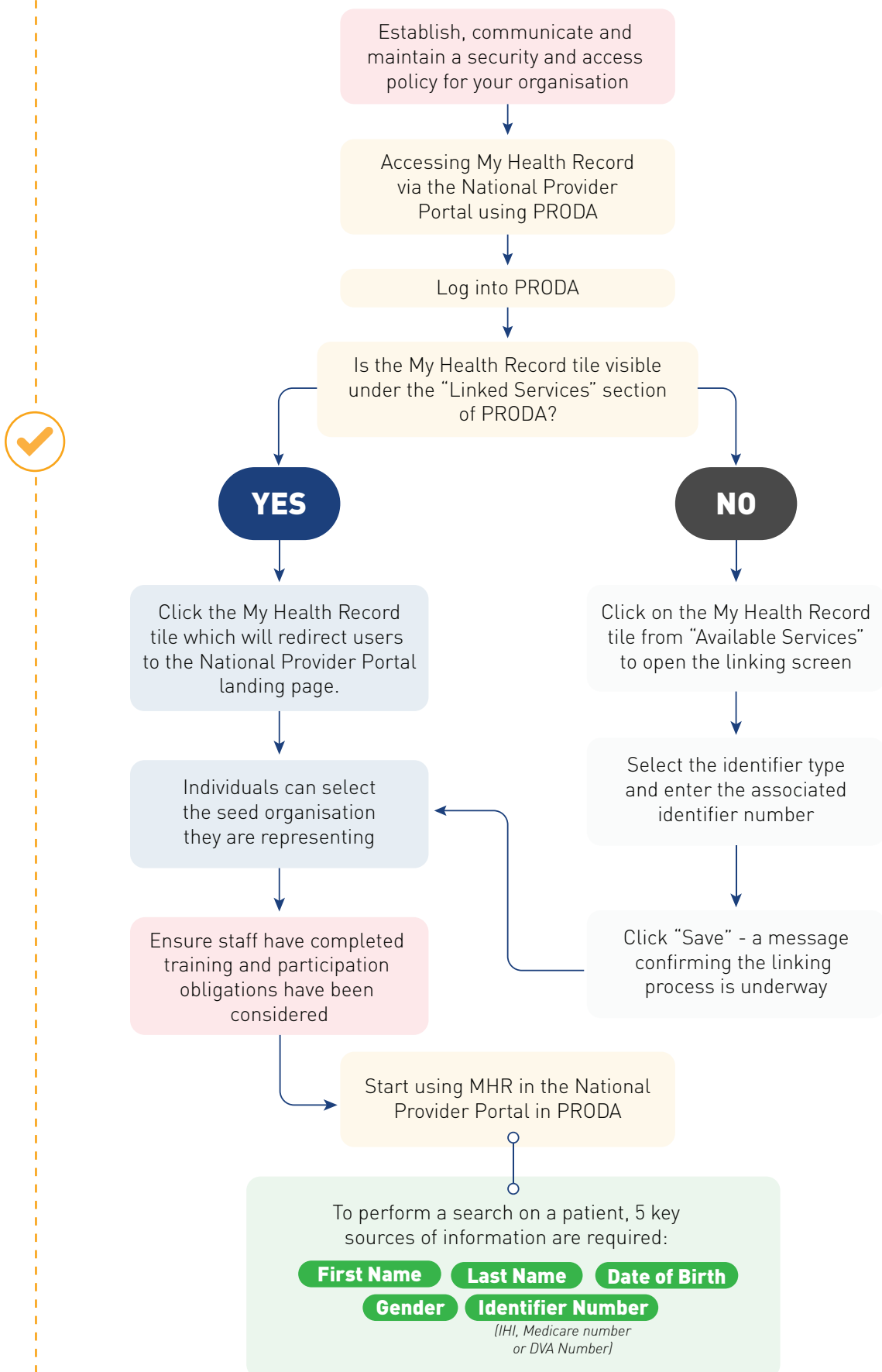
National Provider Portal

The National Provider Portal (NPP) is a **read-only service** that is accessible to registered healthcare providers who do not have access to conformant clinical software. It is also available for use on mobile devices where access to the organisation's clinical information system may not be available.

Healthcare providers may access the NPP using their PRODA account.

The registration process for the My Health Record system, either via conformant clinical software or the NPP, is available through Health Professional Online Services (HPOS), via PRODA. Improving registration time from weeks to hours.

Using PRODA To Access My Health Record through the National Provider Portal



Managing compliance

As part of meeting legislative requirements to participate in the My Health Record system, organisations need to confirm they have a security and access policy which addresses several areas:

1. My Health Record System Security Policy
2. National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) Certificates Policy

Requirements only for general practice eligibility for the PIP eHealth incentive:

1. Secure Message Delivery (SMD) Policy
2. Clinical Coding and Terminology Policy

Organisations must review their policies at least annually and use version control to keep copies of previous versions so that they may be produced if requested.

My Health Record security and access policy

This governs the use of My Health Record within your organisation and must address the following:

- How members of the organisation's team are authorised to access the My Health Record system on behalf of the organisation. This must include:
 - › How access is suspended or deactivated for someone who leaves the organisation or whose security has been compromised or whose role has changed so that they no longer require access to the My Health Record to perform their duties.
- The training that will be given to anyone on the practice team before the person is authorised to access the My Health Record system. Training must cover:
 - › How to use the My Health Record system responsibly and accurately;
 - › Legal obligations on the organisation and individuals using the My Health Record system;
 - › The consequences of breaching those obligations.
- The process for identifying a person who requests access to a patient's My Health Record and how this information is communicated to the System Operator when requested.

- The physical and information security measures that are to be established and adhered to by the organisation and those accessing the My Health Record system on behalf of the organisation:
 - › Restricting My Health Record access to only those members of the practice team who require access as part of their duties;
 - › Uniquely identifying individuals using the organisation's IT 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 given the security and privacy risks associated with unauthorised access to the My Health Record system;
 - › Ensuring that the user accounts of those who are no longer authorised to access the My Health Record system to prevent access to the My Health Record system;
 - › Suspending a user account that enables access to the My Health Record system as soon as practicable after becoming aware that the account or its password or access mechanism has been compromised.
- Mitigation strategies to ensure My Health Record-related security risks can be promptly identified, acted upon and reported to the organisation's management.

[Sample security and access policies](#) are available for download via the My Health Record website.

NASH PKI Certificates Policy

Healthcare organisations accessing the My Health Record system via a conformant clinical information system require a NASH PKI Certificate for Healthcare Organisations. The NASH PKI Certificate for Healthcare Organisations Terms and Conditions require the healthcare organisation to have a set of policies and procedures in place governing use of the NASH PKI Certificate.

A sample NASH PKI Certificates Policy is included in [Appendix B](#).

Privacy and security compliance

The following checklist can be used as a guide to implementing security practices and policies in your organisation.

It covers the requirements that must be incorporated in a My Health Record security and access policy, as outlined in the *My Health Records Rule 2016*, together with a number of sound privacy and security practices.

This checklist is a guide only and should be individualised to meet the needs of your organisation:

1. [My Health Record security and access policy](#) – meeting your obligations to publish, distribute and regularly review your organisation's security policy
2. [Managing user accounts](#) – individual user accounts are used and monitored when accessing your organisation's practice software and the My Health Record system
3. [Identification of staff](#) – requirements for staff members using clinical software to access the My Health Record system to view individual My Health Records
4. [Staff training](#) – regular training is given to staff members who use the My Health Record system
5. [Handling of privacy breaches and complaints](#) – reporting procedures and processes are put in place to meet notifications requirements or handle health consumer concerns regarding unauthorised access to their My Health Record
6. [Risk assessments](#) – are regularly undertaken and take into account security and privacy risks for My Health Record access and the broader information communications technology of your organisation.

Ongoing participation obligations

There are several ongoing obligations on a participating organisation. Please note, this is not an exhaustive list of obligations. If in doubt of your organisation's obligations, you should contact the System Operator.

To participate in the My Health Record system, your healthcare organisation must:

- Not discriminate against an individual because they do not have a digital 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 that 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.



QUICK TIP:

Staff training of the My Health Record system is an important part of compliance. A number of [training checklists](#) and [training resources](#) can be accessed on the My Health Record website.

Strengthened privacy regulations

In November 2018, the Australian Parliament passed new laws to strengthen My Health Record privacy specifically relating to the following areas:

1. Access by insurers and employers
2. Access by law enforcement and government agencies
3. Permanent deletion of a cancelled My Health Record
4. Greater privacy for teenagers aged 14 and over
5. Increased penalties for misuse of information
6. Strengthening protections for victims of domestic and family violence
7. Operation of the My Health Record system
8. Use of My Health Record data for research purposes
9. No commercial use of My Health Record data

More information is available about these changes is available [here](#).

Patient consent

“Under the *My Health Records Act 2012*, healthcare provider organisations are authorised to view information in the My Health Record System and upload information to the system. Individuals can choose to add access controls to their record to restrict access to specific documents (using a limited document access code), or to their whole record (using a record access code).”

Limiting access

Limiting access to the whole of their record and having a record access code that needs to be given to healthcare provider organisations to whom they wish to grant access and/or;

- Limiting access to specific documents in their My Health Record, and having a limited document access code to give to select healthcare provider organisations for them to gain access to the restricted documents;
- Turning off automatic checking for a My Health Record, which will prevent a healthcare provider organisation being automatically notified via their local clinical software if a person has a record.

Refusal of consent to upload

Individuals may expressly inform a healthcare provider organisation that they do not want certain information to be uploaded to their My Health Record during a consultation, and the healthcare provider must comply with this request.

Emergency access

There are certain urgent situations, defined in the *My Health Records Act 2012* (section 64), where it may be permissible for a healthcare provider to bypass the access code(s) using an emergency access function available through your clinical information system. This is sometimes 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 if:

- there is a serious threat to the individual’s life, health or safety and their 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). In addition, individuals can choose to receive an SMS or email notification each time the emergency access function is used to view their My Health Record.

With emergency access, any access controls that the individual has set will be overridden. This means you will have full access to their record. However, information that has been entered in the consumer-only notes section of the record, and any documents that the person has previously removed will not be visible.

For more information, go to the [My Health Record website](#).

Appendix A: Readiness checklist

This checklist aims to support healthcare organisations get ready for using My Health Record. It contains hyperlinks for guidance and further information for each step.



Australian Government
Australian Digital Health Agency



Organisation Readiness Checklist

This checklist supports healthcare organisations to register and use My Health Record

About My Health Record

What is My Health Record and what are the benefits?	My Health Record website , benefits for providers , YouTube case studies , webinars . Information on uploading , viewing and organisation registration .
Online education about PRODA and HPOS	Provider Digital Access (PRODA) provides secure access to online government services. Access online PRODA education . Health Professional Online Services (HPOS) is a fast and secure way for health professionals and administrators to do business with Services Australia . Access online HPOS education .

Information required to register an organisation for My Health Record

Business ABN/ACN		Responsible officer (RO)	
Trading name		Organisation maintenance officer/s (OMO)	
Street address Postal address		Mobile phone (to receive PIC code via SMS for NASH PKI Certificate)	
Email		Organisation type Check options on the Services Australia website	

Important numbers

Healthcare Provider Identifier – Organisation (HPI-O)	The HPI-O identifies the healthcare provider organisation where healthcare is provided. It is available once the organisation has completed the online registration process for the Healthcare Identifiers Service (HI Service) .
Healthcare Provider Identifier – Individual (HPI-I)	An HPI-I identifies an individual healthcare provider. Ahpra-registered health professionals can locate their HPI-I by accessing their account via the Ahpra website or by calling HI Service (1300 419 495). Non-Ahpra registered health professionals can apply for a HPI-I online via Health Professional Online Service (HPOS) .



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

	Healthcare Provider Identifier –Organisation (HPI-O)	Understand My Health Record roles and responsibilities including RO and OMO. The RO and OMO(s) are responsible for ensuring the steps in this document are reviewed for their organisation. Each organisation can have only one RO but can have multiple OMOs. Make a record of the individuals who are the RO and OMO(s) in the organisation's My Health Record security and access policy or other appropriate place. If a change in RO is required, submit application to replace the RO for an organisation with an existing HPI-O.
	OMO and/or RO registers for a PRODA account and selects HPOS	RO or OMO creates or signs into a PRODA account and clicks on Health Professional Online Services (HPOS) from the list of services.
	Nominating the OMO(s)	Once the organisation is registered for My Health Record, ensure the person responsible for the day-to-day administration of the organisation is nominated as an OMO in HPOS. OMO(s) can be added, removed or changed via HPOS as required.

Policies and education

	My Health Record security and access policy	It is a legislative requirement that a My Health Record security and access policy be implemented as described in the My Health Records Rule 2016 . My Health Record policy templates are published by The Royal Australian College of General Practitioners (RACGP), the Pharmaceutical Society of Australia and on the My Health Record website . RO and OMO ensures that a process is in place for auditing when staff have accessed My Health Record in the event of a breach investigation.
	National Authentication Service for Health Certificate for Healthcare Provider Organisations Public Key Infrastructure (NASH PKI) Certificate Policy	Under the National Authentication Service for Health Public Key Infrastructure Certificate for Healthcare Provider Organisations Terms and Conditions of Use, healthcare organisations using a NASH PKI are required to have policies and procedures in place governing use of the NASH PKI Certificate. Full details are available on the Services Australia website. A template NASH PKI Policy is available on the My Health Record website.
	Recognise privacy and security obligations	Both the My Health Record website and the Australian Digital Health Agency Cyber Security Centre website hold information and resources to optimise privacy and security for My Health Record and other healthcare systems. Information regarding Ongoing participation obligations are available on the My Health Record website .
	Staff completed My Health Record training	Internal My Health Record training is provided to organisation staff and a register of this training is maintained. See Recommended Training Checklist .



Registering the organisation via HPOS

	<p>Register seed organisation for the Healthcare Identifiers Service (HI Service) and My Health Record via HPOS. A seed organisation is a legal entity that provides or controls the delivery of healthcare services within Australia.</p>	<p>My Health Record registration step by step guides are on the My Health Record website and the HPOS website.</p> <p>The RO completes the registration request by accessing HPOS via PRODA.</p> <p>Follow these steps if you have had a change of ownership.</p> <p>To amend organisation details including updating the personal details of an RO or OMO and to deactivate, reactivate and retire an HPI-O use HPOS or these forms.</p> <p>For further advice contact the HI Service on 1300 361 457.</p>
	<p>A network organisation is a sub-entity of a seed organisation that provides healthcare services. If required, register network organisations.</p>	<p>If your organisation decides to register one or more network organisations follow these steps to add organisation(s) to create a network organisation underneath the seed. You will be instantly provided with the new HPI-Os of the network organisations created. Then follow these steps to register these networks to access the My Health Record system. Each network organisation requests a separate NASH PKI certificate. Network organisations are asked to set access flags when registering the network organisation for My Health Record. There is more information about access flags on the My Health Record website and in Division 4 of the My Health Records Rule 2016. Access flags allow networks to either inherit their parent organisation's access (flag set to 'no') or have access separate from their parents organisation's access (flag set to 'yes'). A seed organisation is always set to 'yes'.</p> <p>For further support regarding network organisations, contact the HI Service.</p>
	<p>RO or OMO signs into their HPOS Messages</p>	<p>RO logs into HPOS and checks their HPOS Messages for the message that contains the HPI-O, details of the RO and OMO and how to apply for a NASH PKI Certificate when using conformant software to access My Health Record.</p>
	<p>Applying for a National Authentication Service for Health Public Key Infrastructure (NASH PKI) Certificate for Healthcare Provider Organisations for using conformant software to access My Health Record</p>	<p>RO or OMO logs into HPOS via PRODA and requests a NASH PKI Certificate.</p> <p>Ensure a mobile phone number is entered when prompted, to receive an SMS with the personal identification code (PIC) to download the NASH within 30 days.</p> <p>Once downloaded, the name of the NASH file is 'Site', which can be renamed 'NASH' once downloaded and the NASH PKI can be reused until it expires.</p> <p>RO and OMO should plan for applying for, and installing, a new NASH with the support of the software vendor at the expiry date. If you downloaded the certificate from HPOS, you can check the expiry date on the HI Service Certificates tab.</p> <p>If the NASH PKI has expired or cannot be accessed, revoke the previous NASH PKI Certificate first and then request a new NASH PKI Certificate via HPOS.</p>
	<p>Linking existing Medicare PKI Certificate, if required by software provider</p>	<p>Check with the software provider whether a Medicare PKI Site Certificate is required for the HI Service and My Health Record. RO or OMO logs into HPOS via PRODA and links existing Medicare PKI Certificate.</p> <p>If your organisation does not have a current Medicare PKI Site Certificate but will be using conformant software, request a Medicare PKI Certificate via HPOS or via the HW001 form.</p>



	<p>Linking HPI-Is to HPI-O in HPOS</p> <p>is required for National Provider Portal, and some software</p>	<p>It is a legislative requirement for organisations to maintain a list of employees authorised to access My Health Record. For those organisations using the National Provider Portal, the RO and/or OMO links all HPI-Is to the HPI-O via HPOS to allow appropriate individuals access to the HI Service and My Health Record. If using conformant software, check with the software provider whether this step is required.</p>
	<p>If using software using a contracted service provider (CSP) (e.g. Aquarius, MMEx) then link HPI-O to CSP Number</p>	<p>RO/OMO links HPI-O to CSP number, which is provided by the CSP software vendor, in both the CSP Links tab and added under Manage CSP Links in HPOS.</p>
	<p>Is your software My Health Record Conformant? If not, you can use the National Provider Portal.</p>	<p>Follow these step-by-step instructions to register the organisation and individuals for the National Provider Portal. Click here to access the National Provider Portal online or via PRODA.</p>

Software configuration

	<p>Check with the software vendor on whether a list of HPI-Is is required to be available for configuring the software. e.g. Most pharmacy software does not require this.</p> <p>Linking HPI-Is to HPI-O in HPOS is required for National Provider Portal, and some software.</p>	<p>The software vendor will support with configuring software. As part of this set-up, all HPI-Is of staff using My Health Record may be required to be entered into the software for setting up access.</p> <p>For those organisations using the National Provider Portal, the RO and/or OMO links all HPI-Is to the HPI-O by managing HPI-I authorisation links. If using conformant software, check with the software provider whether this step is required.</p>
	<p>NASH and Medicare PKI Certificates to be configured into software as required by the software vendor</p>	<p>Call your software vendor or IT Support to arrange configuration support.</p>
	<p>Confirm HPI-O and HPI-I numbers have been configured into software</p>	<p>Contact your software vendor or IT Support for configuration support.</p> <p>When staff leave, close their user accounts. Unlink HPI-Is from the organisation via HPOS as required.</p>
	<p>Software settings are updated to ensure permission for staff accessing My Health Record</p>	<p>Contact your software vendor or IT Support for My Health Record configuration support. Staff will require relevant viewing/uploading permissions enabled for My Health Record and Electronic Transfer of Prescriptions.</p>
	<p>Check if conformant software can access My Health Record</p>	<p>Contact software vendor if there are connection errors or Individual Healthcare Identifier (IHI) errors.</p>
	<p>Organisation has an electronic transfer of prescriptions product installed (<i>if required</i>)</p>	<p>Set up Electronic Transfer of Prescriptions eRx Script Exchange (1300 700 921) or MediSecure (1800 472 747)</p>



Inform your patients

	Provide information to your patients	<p>A range of information and brochures is available on the My Health Record website.</p> <p>Print on Demand resources such as brochures, counter cards and posters can also be ordered online at https://digitalhealth.immij.com/ with the password <i>digitalhealth</i> and the following usernames as applicable:</p> <ul style="list-style-type: none"> • GP • Pharmacy • Hospital • PHN • Specialist
	Add information to your website and privacy policy	Inform consumers that your healthcare organisation uses My Health Record.

For further information and support

Helpline	Queries	Contact	Available
Healthcare Identifiers (HI) Service	Identifier queries and organisation registration	Phone 1300 361 457	Mon–Fri 8.30am – 5.00pm AEST & AWST
PRODA Help	PRODA queries	Phone 1800 700 199	Mon–Fri 8.00am – 5.00pm AWST
HPOS Help	HPOS queries	Phone 132 150	Mon–Fri 8.00am – 5.00pm AWST
eBusiness Service Centre	Certificates, including Medicare PKI Site Certificates and NASH	Phone 1800 700 199	Mon–Fri 8.00am – 5.00pm AEST & AWST
My Health Record Help Line	General enquiries and detailed support for individuals and healthcare providers	Phone 1800 723 471	Open 24 hours, 7 days
Australian Digital Health Agency Help Centre	Complex queries, vendor enquiries, secure messaging delivery enquiries, and digital health education	Phone 1300 901 001 Email help@digitalhealth.gov.au	Mon–Fri 8.00am – 5.00pm AEST

Updated: March 2021

Appendix B: Policies and procedures for the use of NASH PKI Certificate for Healthcare Organisations

Please note that the following is an example and is intended as a guide only and should be tailored to meet the needs of your organisation. We do not recommend implementing the policies and procedures without first considering whether they meet your needs.

Purpose

The NASH PKI Certificate for Healthcare Organisations Terms and Conditions require the healthcare organisation to have a set of policies and procedures in place governing use of the NASH PKI Certificate.

This document describes the policies and procedures that are involved in the usage of the NASH PKI Certificate within **[healthcare organisation name]**.

Policies and procedures

The policies and procedures stated in this document should be known and understood by everyone within **[healthcare organisation name]** using the NASH PKI Certificate for the organisation.

The NASH PKI certificate for the organisation will be securely stored by the responsible officer (RO) or organisation maintenance officer (OMO).

[healthcare organisation name] will not give its NASH PKI certificate to any other entity or organisation or allow any unauthorised person to use the PKI Certificate, except for any outsourced

information technology service provider engaged by it to act as its agent in using its certificate.

NASH PKI certificates for the organisation should only be used for proper purpose as defined in the NASH PKI Certificate terms and conditions.

Individuals who have used the NASH PKI certificates for the organisation understand that they can be identified in respect of each use and the role they performed in respect of that use and are responsible and accountable for this use.

Individuals must notify the practice manager immediately whenever the NASH PKI certificate for the organisation is lost, destroyed, stolen or compromised. **[healthcare organisation name]** must promptly notify Services Australia of the possible loss, destruction or theft of its Certificate, or in the event that **[healthcare organisation name]** considers or suspects that its Certificate has been compromised.

Staff responsibility

It is the responsibility of all administrative staff to support the use of NASH PKI certificates by undertaking any administration tasks involved in its maintenance and use.

Related resources

[NASH PKI Certificate for Healthcare Provider Organisations Terms and Conditions of Use](#)



Australian Government

Australian Digital Health Agency

The Australian Association of Practice Management (AAPM) and the Australian Digital Health Agency have partnered to develop two key resources to assist practice managers and owners to register and connect their practice to My Health Record.