Handbook for Practice Managers

26 September 2019
Version 1.0

Approved for external use

My Health Record

aapm
Australian Association of Practice Management

Contents

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.

Provider Digital Access (PRODA)
Help Desk: 1800 700 199

Health Professional Online Services (HPOS)
Help Desk: 1800 723 471

Healthcare Identifier 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 of a NASH PKI Certificate request

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 Customer 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
DHS Department of Human Services	Department of Human Services is a department of the Government of Australia charged with responsibility for delivering a range of welfare, health, child support payments and other services to the people of Australia.
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 be 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 Health Identifier 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.
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.

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, if you have one, 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.
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 Department of Human Services (DHS) 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

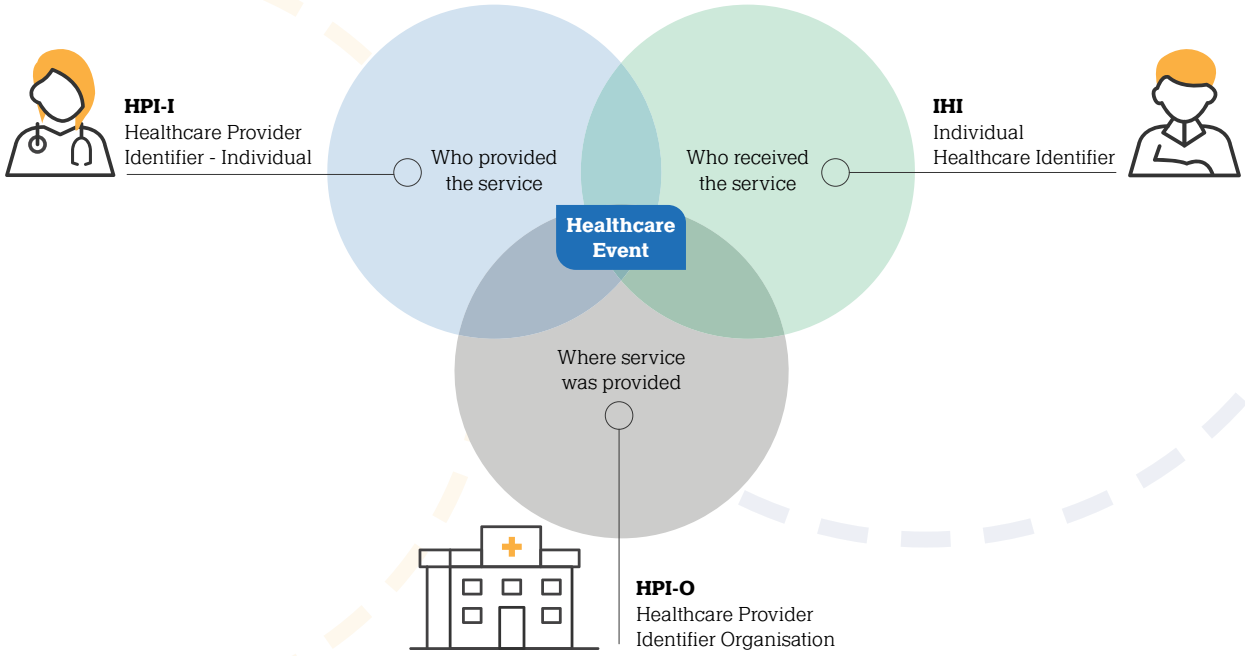
Seed HPI-O is any legal entity that delivers healthcare services within Australia, e.g. medical practices, community healthcare or hospitals.

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).

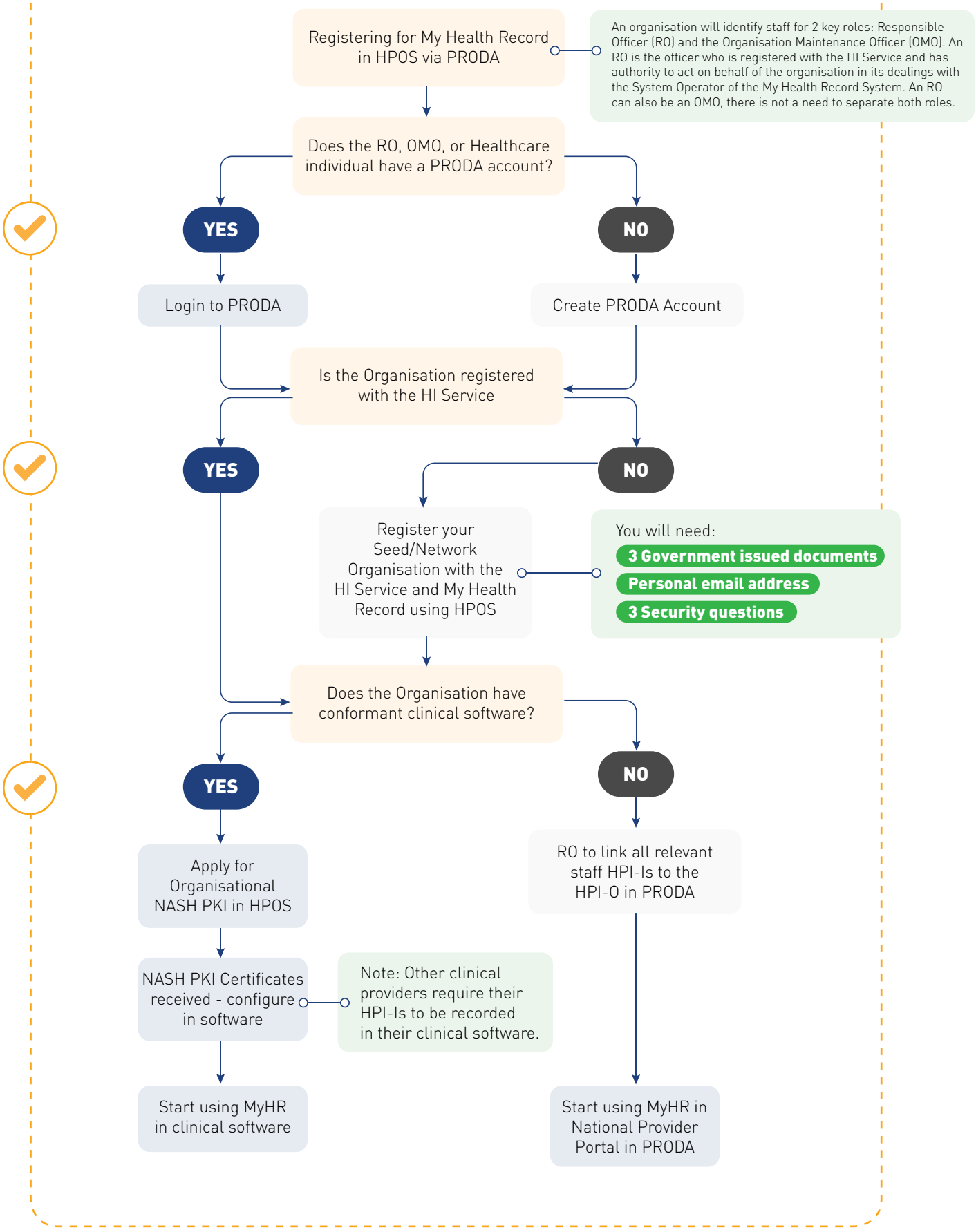
The illustration below shows the role of the three main healthcare identifiers in a healthcare event such as a consultation:



Find out more about registering your practice with the Healthcare Identifier 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 (Human Services 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 by completing an Application to register a healthcare provider form (HW033). 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.

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).

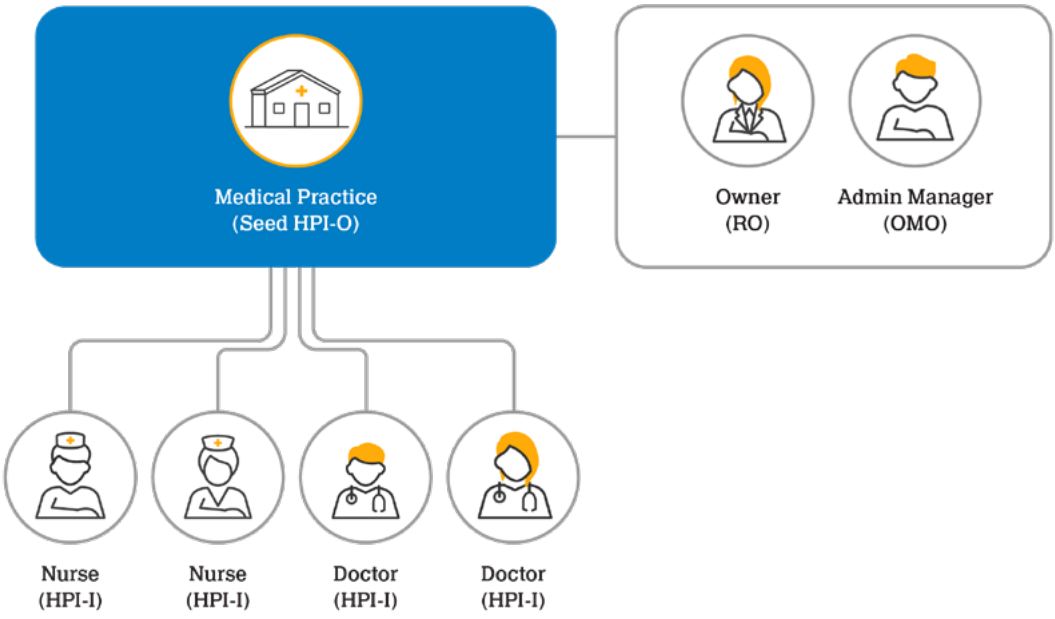
A Seed Organisation is a legal entity that provides or controls the delivery of healthcare services. A Seed Organisation could be, for example, a local GP practice, pharmacy or private medical specialist.

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

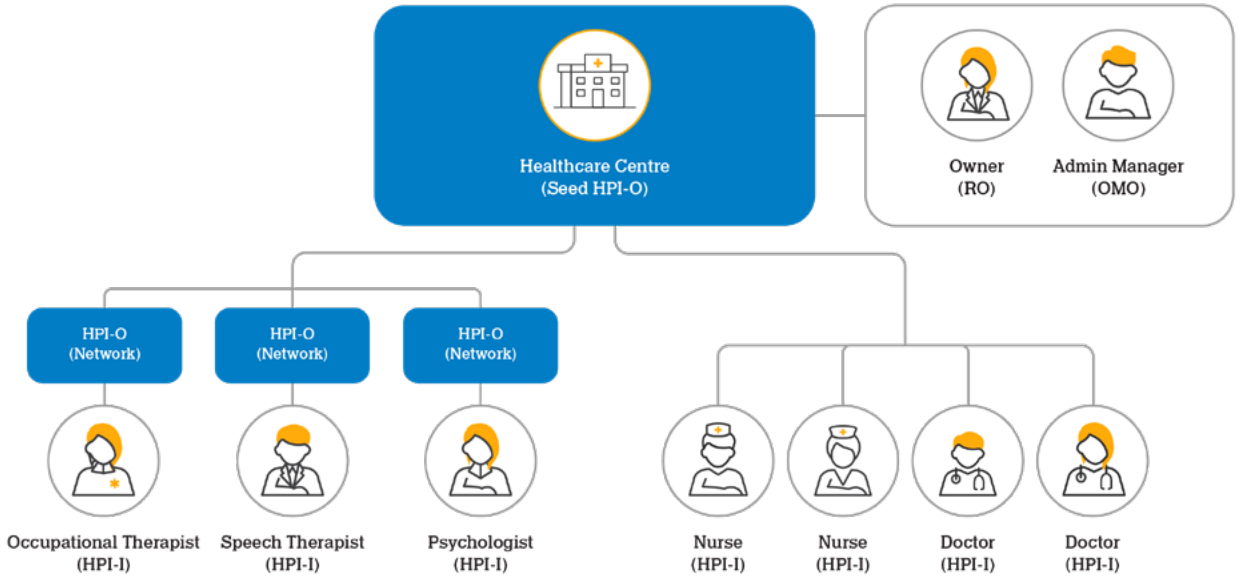


Network Organisations

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: Healthcare Identifiers tile > My Organisation Details > Summary Tab > 'Add organisation'. From here, type in organisation name, ABN, contact details and address. 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.

Roles and Responsibilities

The Healthcare Identifier (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.

	Responsible Officer (RO)	**Organisation Maintenance Officer (OMO)**
	• 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 organisations healthcare organisations, the RO may be a practice manager or business owner. • The RO is also an OMO by default.	• 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 • Publish HPI-O details in the Healthcare Provider Directory (HPD) for HPI-Os 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.

Healthcare Provider Directory

Ensuring your organisation is listed in the HPD will facilitate ease of communication between healthcare providers across the healthcare sector.

When registering your Seed Organisation with the HI Service and the My Health Record System, your organisation will have the opportunity to consent to details being entered in the Healthcare Provider Directory (HPD). A HPD record provides a means for healthcare organisations and individuals registered with the HI Service to search for contact details of other registered healthcare providers and organisations.

Listing your organisation in the HPD means that other healthcare providers can find your organisation and view up to date contact details. The HPD will contain secure messaging information, so providers can confirm that your organisation can receive secure messages and then send referrals and other electronic messages directly. Individual healthcare providers who have been linked to your organisation are also visible when other providers search for your organisation, for example. specialists working within a hospital. This also has the benefit of allowing a General Practitioner to directly refer to a Specialist by name.

Please note that if you are a general practitioner and intend to register your healthcare organisation for the Practice Incentives Program eHealth Incentive (ePIP), an up-to-date HPD record for your organisation is a mandatory component of the secure message delivery requirement.

Download the Healthcare Provider Directory fact sheet 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 proider 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.

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.

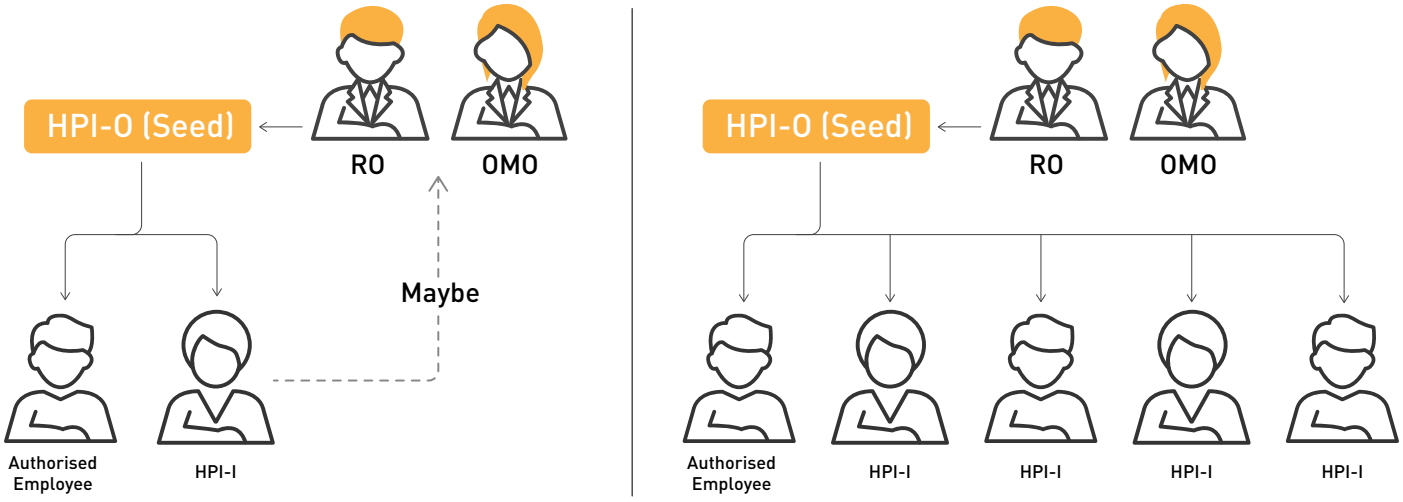
Authorised Employee:

- **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



The table below outlines the different roles, examples of the types of employees who may fulfil each role within a medical practice, and some of the actions which a person in that role is able to carry out.

	Responsible Officer (RO)	Organisation Maintenance Officer (OMO)	Authorised Employee - HI Service	Authorised Employee - My Health Record system	Healthcare Provider (HPI-I)
Example for Medical Practice	Business Owner	Practice Manager	Employee undertaking activities to support the provision of healthcare	Health worker; Administrative staff	Healthcare provider with a HPI-I (e.g. General Practitioner, Nurse)
IHI search and download			✓	✓	✓
My Health Record Assisted Registration			✓	✓	✓
View My Health Record and download clinical documents			✓	✓	✓
Author clinical documents for a My Health Record					✓
Upload clinical document to My Health Record			✓	✓	✓
Manage organisation interactions - HI Service and My Health Record	✓	✓			

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.

See the section Digital Health Certificates 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.

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.

Certificates are valid for 2 years and your organisation will be notified 6 weeks prior to a certificate expiring. 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.

If your organisation still has a physical token, the expiry date is printed on the CD or USB key and renewal certificates will need to be downloaded from HPOS.

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.

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** allows healthcare providers only to view and download or print information and documents.

Note: Providers with conformant software may also use the Provider Portal 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 Provider Portal 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 are 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 searching the HI Provider Directory Service for Individuals in PRODA.

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.

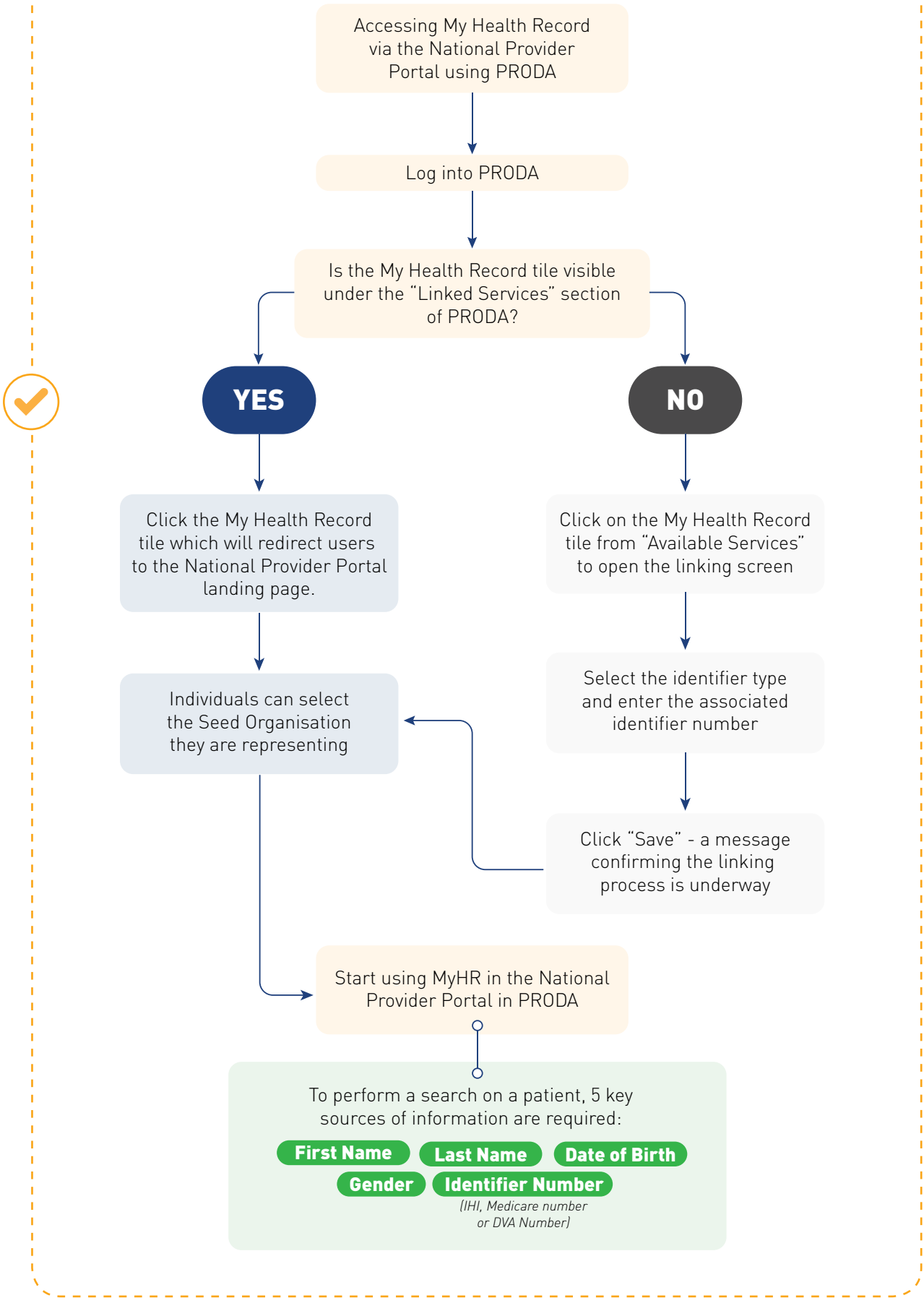
National Provider Portal

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 My Health Record system policy which addresses several areas:

1. My Health Record System 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 System 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.

A sample **Security and Access Policy** is included in ***Appendix B***.

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 in included in Appendix C.

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 system security 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 System Security 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 that 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.

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 who 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.

Download the Emergency Access fact sheet here.

Appendix A: Readiness Checklists

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

My Health Record

Organisation Readiness Checklist

This checklist supports healthcare organisations register to 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 for My Health Record.
☐	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 us. 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**	
Street Address **Postal Address**		**Mobile Phone (to receive SMS)**	
Email		**Organisation Type** Check options on the DHS website	

Important Numbers in the Preparation Process

☐	Healthcare Provider Identifier for Organisations (HPI-O)	The HPI-O is generated when the Organisation My Health Record registration has occurred.
☐	Healthcare Provider Identifier – Individual (HPI-I)	If registered with AHPRA, clinical staff can contact AHPRA for their HPI-I (phone: 1300 419 495). Non-AHPRA health professionals can apply for a HPI-I by submitting the form HW033. HPI-Is can also be searched via PRODA-HPOS.
☐	Individual Registration Authority (RA)	May be required to identify individual management staff in the organisation that do not have an HPI-I. Obtained either from an existing Individual Medicare PKI certificate or under Profile in PRODA.

Responsible Officer (RO) and Organisation Maintenance Officer (OMO)

☐	Organisation identifies a RO & OMO	Understand My Health Record roles and responsibilities including RO and OMO.
☐	OMO and/or RO registers for a PRODA account.	RO creates or signs into a PRODA account. If a change in RO has taken place, submit application to replace the RO for an organisation with an existing HPI-O.
☐	Nominating the OMO(s)	Once the organisation is registered for My Health Record, ensure the person managing the organisation is nominated as an OMO in PRODA-HPOS. OMOs can be added, removed or changed via PRODA-HPOS as required.

Registering the Organisation via PRODA-HPOS

☐	Register Seed Organisation for My Health Record via PRODA-HPOS	My Health Record registration step by step guides are on the My Health Record website and the HPOS website. The RO logs into PRODA-HPOS to complete registration request. Follow these steps if you have had a change of ownership. For further advice based on your circumstances, contact the HI Service on 1300 361 457.
☐	RO or OMO signs into their PRODA-HPOS Mail	RO logs into PRODA-HPOS & checks their HPOS mailbox. Email will contain HPI-O, details of the RO and OMO and how to apply for a NASH PKI Organisation Certificate for using conformant software to access My Health Record.
☐	Applying for a NASH PKI Certificate for using conformant software to access My Health Record.	RO or OMO logs into PRODA-HPOS and requests a NASH. Ensure a mobile phone is entered when prompted to receive an SMS with the Personal Identification Code (PIC) to download the NASH within 30 days. 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. If NASH PKI has expired or cannot be accessed, request a new NASH and indicate to revoke the previous NASH Certificate.
☐	Linking existing PKI Certificate	RO or OMO logs into PRODA-HPOS and links existing Medicare PKI Certificate. If your organisation does not have a current Medicare PKI Site Certificate but will be using conformant software, request a PKI Certificate via PRODA-HPOS.
☐	Linking HPI-Is to HPI-O in PRODA-HPOS is required for *National Provider Portal*, and *Simple Aquarius*.	For those organisations using the National Provider Portal or Simple Aquarius, the RO and/or OMO is required to link all HPI-Is to the HPI-O by managing HPI-I Authorisation Links.
☐	If using software using a Contracted Services Provider (CSP) (e.g. Aquarius, MMEx) then link HPI-O to CSP Number.	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 Authorisation Links in HPOS.
☐	Is your software My Health Record Conformant? If not, you can use the National Provider Portal.	Follow these step by step instructions to register the organisation and individuals for the Provider Portal. Click here to access the Provider Portal online or via PRODA.

Software Configuration

☐	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. Linking HPI-Is to HPI-O in PRODA-HPOS is required for *National Provider Portal*, and *Simple Aquarius*.	The software vendor will support with configuring software. As part of this set up all HPI-Is of staff using My Health Record will be required to be entered into the software. For those organisations using the National Provider Portal or Simple Aquarius, the RO and/or OMO is required to link all HPI-Is to the HPI-O by managing HPI-I Authorisation Links.
☐	NASH and Site PKI Certificates to be configured into software.	Call your software vendor or IT Support to arrange configuration support.
☐	Confirm HPI-O and HPI-I numbers have been configured into software	Contact your software vendor or IT Support for configuration support. When staff leave, close their user accounts. If using Aquarius or the National Provider Portal, unlink HPI-Is from the Organisation via PRODA-HPOS.
☐	Organisation has an electronic transfer of prescriptions product installed (*if required*)	Set up Electronic Transfer of Prescriptions eRx (1300 700 921) or MediSecure (1800 472 747)
☐	Software settings are updated to ensure permission for staff accessing My Health Record.	Contact your software vendor or IT Support for My Health Record configuration support. Staff will require relevant viewing/uploading permissions for My Health Record and Electronic Transfer of Prescriptions enabled.
☐	Check if conformant software can access My Health Record	Contact software vendor if there are connection errors or Individual Healthcare Identifier (IHI) errors.

My Health Record Readiness Checklist

Policies and Education

☐	My Health Record Security Policy	It is a requirement that a My Health Record Security Policy be implemented as described in the My Health Records Rule 2016. Examples of My Health Record Policy templates are published by the RACGP and the Pharmaceutical Society of Australia (PSA).
☐	Staff complete My Health Record training	Internal My Health Record training is provided to organisation staff. Access the Australian Digital Health Agency online eLearning Modules. On Demand Software Training simulators and demonstrations. Username is OnDemandTrainingUser and password TrainMe. Access software Summary Sheets or request My Health Record manuals from the software vendor. Request an Australian Digital Health Agency Educator presentation.

Inform and support your patients

☐	Provide information to your patients	A range of information and brochures are available on the My Health Record website. Resources can also be ordered online at http://myhealthrecord.immij.com with the password *myhealthrecord* and the following usernames as applicable: • MHR_GP • Pharmacy_MHR • Hospital_MHR • PHN_MHR
☐	Add information to your website and privacy policy	Inform consumers that your healthcare organisation uses My Health Record.
☐	Display brochures and posters in your organisation	Contact your local Primary Health Network (PHN) to request additional My Health Record resources and collateral.

For further information and support

Helpline	Queries	Contact	Available
Healthcare dentifiers (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 to 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 ine	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: July 2019

Appendix B: My Health Record Security and Access Policy

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 this policy without first considering whether it meets your needs.

This sample policy was initially developed by Inner East Melbourne Medicare Local.

Purpose

- To provide guidance for staff and contractors about access to, and use of, the My Health Record system.
- To provide guidance in the use of information technology in **[name of organisation]** as it relates to the My Health Record system.
- To outline the roles and responsibilities of the Responsible Officer and the Organisation Maintenance Officer in relation to the My Health Record system.

Scope of Policy

This policy applies to all staff (including its employees and any healthcare provider to whom [name of organisation] supplies services under contract) with access to the My Health Record system.

Related Documents/Links

This policy is to be read in conjunction with the following documents:

My Health Records Act 2012
My Health Records Rule 2016
My Health Records Regulation 2012
My Health Records (Assisted Registration) Rule 2015
Healthcare Identifiers Act 2010

Definitions

- ***Access flag*** means an information technology mechanism made available by the System Operator to define access to a consumer's digital health record.
- ***HI Service*** is the 'Healthcare Identifiers Service', a national system for uniquely identifying healthcare providers and individuals, which makes sure the right health information is associated with the right individual.
- ***Information Commissioner*** is the Office of the Australian Information Commissioner (OAIC).
- ***Network*** means a network of healthcare provider organisations created and managed in accordance with subsections 9A (3) to (6) of the Healthcare Identifiers Act 2010.
- ***Network organisation*** is a healthcare provider organisation which is part of a Network and is subordinate to a Seed Organisation; it can be used to represent different departments, sections or divisions within an organisation or can be separate legal entities from the Seed Organisation
- ***Organisation maintenance officer (OMO)*** has the same meaning as in the Healthcare Identifiers Act 2010.
- ***Provider portal*** means the portal provided by the System Operator that allows for identified healthcare providers from participating healthcare provider organisations to access the My Health Record system without having to use a conformant clinical information system.
- ***Responsible officer (RO)*** has the same meaning as in the Healthcare Identifiers Act 2010.
- ***Seed organisation*** is a healthcare provider organisation which provides or controls the delivery of healthcare services; in a Network, the Seed Organisation is the principal entity in the Network.
- ***System Operator*** is the Australian Digital Health Agency.

Organisation Structure, Roles and Responsibilities

ORGANISATION STRUCTURE

All healthcare providers and organisations wishing to participate in the My Health Record system must first be registered with the HI Service. Healthcare provider organisations will usually participate in the My Health Record system as a 'Seed Organisation' only. However, in large or complex organisations, there may be a network made up of a Seed Organisation and one or more 'Network Organisations' that is part of or subordinate to the Seed Organisation.

[name of organisation] is registered in the HI Service as a: **[insert 'Seed Organisation' or 'Network Organisation']**

MY HEALTH RECORD SYSTEM ROLES

The My Health Record system requires people to be

assigned to key roles, which authorises them to carry out certain actions in relation to [name of organisation]'s access to, and use of, the system. These roles are set out below:

- *Responsible Officer (RO):* the RO is an employee of the Seed Organisation and has the authority to act on behalf of the Seed Organisation (and any Network Organisations) in its dealings with the System Operator. The RO has primary responsibility for an organisation's compliance with participation requirements in the My Health Record system.
  The RO for **[name of organisation]** is: **[name of RO]**
- *Organisation Maintenance Officer (OMO)*: the OMO is an employee of a healthcare provider organisation that is a Seed Organisation, or a Network Organisation. The OMO's primary role is to undertake the day to day administrative tasks in relation to the My Health Record system. A healthcare provider organisation can have multiple OMOs.
  The OMO for **[name of organisation]** is: **[name/s of OMO]**

KEEPING INFORMATION ABOUT THE ORGANISATION UP-TO-DATE

If [name of organisation] becomes aware that information held by the HI Service or the My Health Record system in relation to [name of organisation] is not accurate, up-to-date and complete, the RO or OMO must provide an update to the HI Service and/or System Operator in writing of the correct information. This shall be provided within 20 days of [name of organisation] becoming aware that the information held is not accurate, up-to-date and complete.

NETWORK OBLIGATIONS: ACCESS FLAGS/LINKAGES

ACCESS FLAGS

Where **[name of organisation]** is part of a Network, it is a requirement that appropriate Access Flags are set and maintained. Access Flags must be set in a way that balances:

- reasonable expectations of patients about the sharing of their healthcare information; and
- existing arrangements within the Network for the collection and sharing of healthcare information.

It is the responsibility of the RO and/or the OMO of the Seed Organisation to set appropriate Access Flags. The RO and/or the OMO of the Seed Organisation will undertake reviews of the Network and Access Flag assignments at such times as the structure changes, or in the case that a System Operator or consumer query reveals potential structural issues. **[name of organisation]** commits to making reasonable changes in line with requests from the System Operator.

LINKAGES

Where **[name of organisation]** is part of a Network, the RO and/or the OMO of the Seed Organisation will establish and maintain an up-to-date record with the System Operator, which details the linkages between organisations in the Network.

Access and Use Of The My Health Record System

AUTHORISING ACCESS TO THE MY HEALTH RECORD SYSTEM

Organisational staff must only access the My Health Record system if this access is required by the duties of their role.

All staff members whose role requires them to access the My Health Record system will be provided a unique user account with individual login name. **[name of organisation]** will maintain records linking user accounts to individual staff so that these can be matched in the case of an audit by the System Operator. **[name of organisation]** will maintain records (for example staff rostering records) to allow it to determine which user accessed the My Health Record system on a particular day. These records must be maintained to allow audits to be conducted by the System Operator.

User accounts will not be used by multiple staff members.

It is the responsibility of the OMO to:

- Provide a unique user account with individual login name for each authorised user; and
- Immediately suspend or deactivate individual user accounts in cases where a user:
  - leaves [name of organisation]
  - has the security of their account been compromised
  - has a change of duties so that they no longer require access to the My Health Record system

STAFF PASSWORDS/LOGGING OUT

Staff will ensure that they assign a secure password to their user account and keep their password secret. Staff must regularly review and change their password.

All staff who have access to the My Health Record system will ensure that they log out of the system when they are not using it to prevent unauthorised access.

IDENTIFYING STAFF WHO ACCESS THE MY HEALTH RECORD SYSTEM

PROVIDER PORTAL

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

CONFORMANT SOFTWARE

Where healthcare providers in **[name of organisation]** access the My Health Record system on behalf of **[name of organisation]** via conformant clinical software, the OMO will maintain a record of authorised Healthcare Provider Identifier – Individual (HPI-I) numbers in the clinical software and in **[name of organisation]**'s internal records.

The clinical 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 TRAINING

[name of organisation] has a formal training program where all staff with authorisation to access the My Health Record system on behalf of **[name of organisation]** are required to undertake regular and ongoing privacy and My Health Record system training.

Existing staff will undertake My Health Record system training before they first access the system, while new staff will be required to undertake training, if appropriate to their role, as part of their orientation to **[name of organisation]**. If any new functionality is introduced into the system, additional training will be provided to all staff with authorised access to the My Health Record system.

Staff training will provide information about how to use **[name of organisation]**'s clinical software, and/or the national Provider Portal, in order to access the My Health Record system accurately and responsibly. Staff training will consist of training materials made available by the System Operator or other materials that **[name of organisation]** deems relevant, and training specific to the clinical software used by **[name of organisation]**. Training will also cover the legal obligations on healthcare provider organisations and individuals using the My Health Record system and the consequences of breaching these obligations.

The OMO will oversee a register of staff training as it relates to the My Health Record system, including the names or those who have completed training and the date on which training was completed.

Security and Privacy Procedures

MITIGATION STRATEGIES

To ensure that My Health Record system related security risks can be promptly identified, acted upon and reported to [name of organisation], [name of organisation] will:

- Regularly review its security and procedures for accessing the My Health Record system, and report the findings to management and revise procedures accordingly.
- Establish a risk reporting procedure to allow staff to inform management regarding any suspected security issue or breach of the system; and
- Consider, and where appropriate, conduct a risk assessment into its ICT systems that examine privacy and security risks, and to conduct this assessment on a regular basis.

REPORTING SECURITY BREACHES

A security breach is when there is an unauthorised collection, use or disclosure of health information included in a patient's digital health record, an example of which is when a staff member with access to the My Health Record system discovers that someone else may have gained access to their user account.

If any staff member becomes aware of a security breach, including where their user account has been compromised or that someone has used their computer to gain unauthorised access to the My Health Record system, they are immediately to inform their manager, who in turn is required to inform the RO or OMO. If only the OMO is informed, it is the OMO's responsibility to ensure that the RO is made aware of the issue.

The RO or OMO will create a log entry of the breach including details of the date and time of the breach, the user account that was involved in the unauthorised access, and which patient's information was accessed (where known).

The OMO will also undertake appropriate mitigation strategies, including, but not limited to:

- Suspending/deactivating the user account
- Changing the password information for the account

The RO or OMO is required to report a data breach to the System Operator (ph. 1800 723 471) and the Information Commissioner (ph. 1300 363 992) as soon as practicable after becoming aware that the following has, or may have, occurred:

- an unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record, or
- the security or integrity of the My Health Record system has, or may have, been compromised by an event or circumstance.

PATIENT DOCUMENT AND RECORD CODES

Patients have the ability to set a number of privacy controls on their digital health record. A patient can set a code that restricts access to providers for certain documents contained within their record, they can also set a different code that restricts access to providers to their entire record.

Where a patient of **[name of organisation]** provides a My Health Record document or record code to unlock their record, the code must not be retained or recorded in the local patient record by staff and must be disposed of (if for example it is written on paper) securely.

RESPONDING TO PATIENT COMPLAINTS

[name of organisation] will make patients aware of the process for raising issues or complaints and will log any issues of which they are made aware.

If a patient raises an issue in relation to unauthorised access to their digital health record, [name of organisation] shall take steps to investigate the issue. Unauthorised access should be managed through [name of organisation]'s existing privacy complaint management processes and privacy policy.

Where a patient asks [name of organisation] to remove or amend a clinical document, and the medical practitioner agrees, the healthcare provider shall take steps to amend or remove the document as soon as possible.

In cases where there is disagreement between the medical practitioner and the patient about amendments to a clinical document, and the provider does not consider an amendment to be appropriate, then the provider may choose to remove the document. If the provider does not consider the removal of the document to be appropriate, then the provider should discuss this with the patient and where relevant direct the consumer to exercise their personal controls over the document.

Appendix C: 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 it meets 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 NSH 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 the Department of Human Services 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 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.