

# Digital Handbook for Practice Management

Version 2.2 August 2023

Approved for use.

# Contents

<b>Contents .....</b>	<b>2</b>
<b>About My Health Record for Practice Management .....</b>	<b>4</b>
<b>Need help?.....</b>	<b>4</b>
<b>Glossary of terms and definitions .....</b>	<b>5</b>
<b>Understanding the Healthcare Identifiers (HI) Service .....</b>	<b>7</b>
<b>My Health Record registration .....</b>	<b>9</b>
Establish a security and access policy.....	9
Register for My Health Record in HPOS via PRODA .....	9
<b>Understanding PRODA.....</b>	<b>10</b>
<b>Register for a PRODA account.....</b>	<b>10</b>
Ensure the right person registers .....	10
Determine how you will access My Health Record .....	11
<b>Determine your organisation structure .....</b>	<b>11</b>
<b>Understanding the seed and network organisation structures .....</b>	<b>12</b>
Network organisations.....	13
Access flags .....	13
<b>Roles and responsibilities .....</b>	<b>14</b>
<b>Other digital health roles and responsibilities .....</b>	<b>15</b>
<b>How the roles might be set up in your organisation.....</b>	<b>16</b>
Seed only HPI.....	16
<b>Register for My Health Record access .....</b>	<b>17</b>
<b>Digital health certificates.....</b>	<b>17</b>
<b>Connecting to and using My Health Record .....</b>	<b>17</b>
<b>Access to the My Health Record system.....</b>	<b>17</b>
<b>Conformant clinical software .....</b>	<b>18</b>
Linking healthcare providers to your organisation .....	18
<b>Using the My Health Record system.....</b>	<b>18</b>
<b>National Provider Portal .....</b>	<b>18</b>
Accessing My Health Record via the National Provider Portal using PRODA.....	19
<b>Managing compliance.....</b>	<b>20</b>

My Health Record security and access policy.....	20
NASH PKI Certificates Policy.....	21
<b>Privacy and security compliance .....</b>	<b>21</b>
<b>Ongoing participation obligations.....</b>	<b>22</b>
<b>Strengthened privacy regulations.....</b>	<b>22</b>
<b>Patient controls.....</b>	<b>23</b>
<b>Access controls .....</b>	<b>23</b>
Limiting access to a My Health Record.....	23
Limiting access to specific documents .....	23
<b>When NOT to upload a patient's record .....</b>	<b>23</b>
<b>Emergency access .....</b>	<b>24</b>
<b>Appendix A: Readiness checklist.....</b>	<b>25</b>
<b>Appendix B: Policies and procedures for the use of NASH PKI Certificate for Healthcare Organisations ....</b>	<b>29</b>
<b>Purpose.....</b>	<b>29</b>
Policies and procedures.....	29
Staff responsibility .....	29
Related resources.....	29

## About My Health Record for Practice Management

This handbook is designed to assist Practice Managers and their teams to understand the overall process for registration of their practice (organisation) to 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 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**

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

**NASH PKI Operations Team** 1300 721 780

**Online Technical Support** for software vendors



## Glossary of terms and 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.

### **Contracted Service Provider (CSP)**

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.

### **Evidence of Identity (EOI)**

Evidence of identity is needed as part of the registration for a PRODA account.

### **Healthcare Identifier (HI)**

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).

### **Healthcare Provider Identifier – Individual (HPI-I)**

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.

### **Healthcare Provider Identifier – Organisation (HPI-O)**

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.

### **Health Professionals Online Services (HPOS)**

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.

### **Individual Healthcare Identifier (IHI)**

An Individual Healthcare Identifier is a 16-digit unique number used to identify individuals who receive care in the Australian healthcare system.

### **National Authentication Service for Health (NASH)**

NASH is a Public Key Infrastructure (PKI) solution used to access digital health services such as:

- Electronic prescribing
- My Health Record
- Secure messaging
- Healthcare Identifiers (HI) Service.

NASH is used by healthcare provider organisations and supporting organisations to:

- authenticate and securely access digital health services
- digitally sign documents and other transactions
- encrypt health information for secure exchange.

### **Network Organisation**

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.

### **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 Responsible Officer (RO) may take on the OMO role as well.

### **Provider Digital Access (PRODA)**

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.

### **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.

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.

There are only three types of Healthcare Identifiers (HI).

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.

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

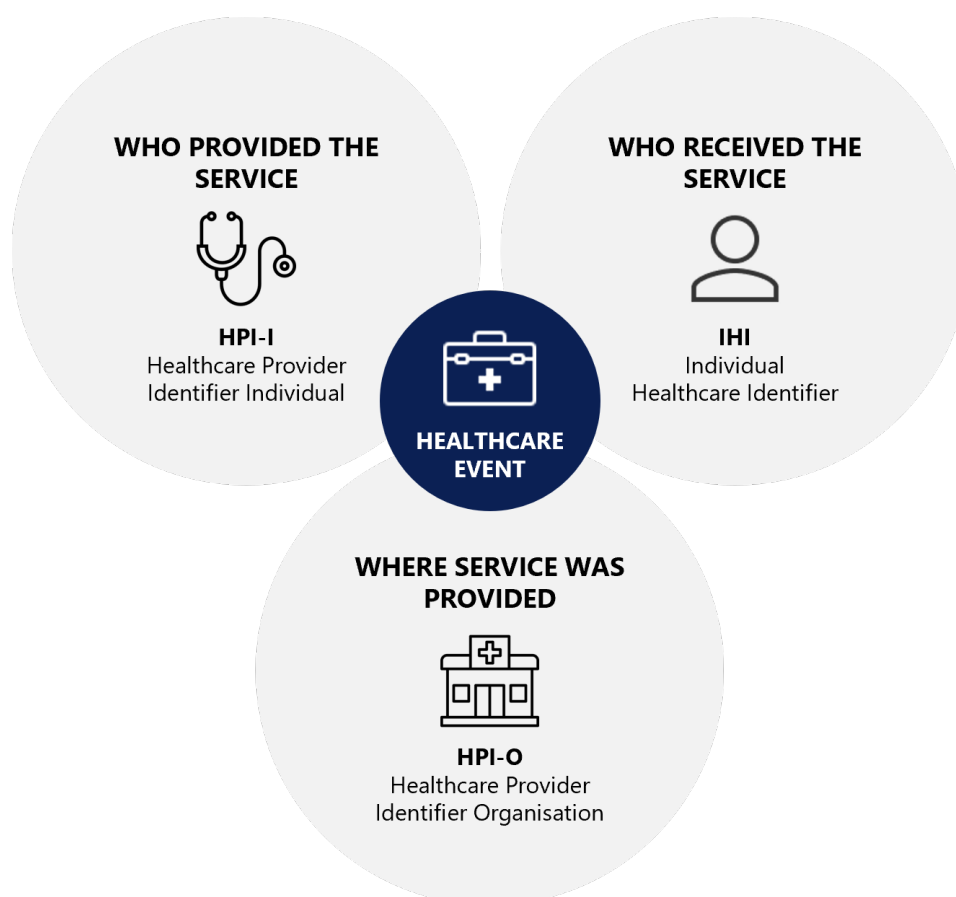
**Healthcare Provider Identifier – Organisation:**

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

**There are two types of HPI-Os (Health Provider Identifier – Organisation):**

- 1. 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** 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

### 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. [Information and sample policy templates](#) can be found on the Australian Digital Health Agency website. [Read more about participation obligations](#).

### Register for My Health Record in HPOS via PRODA

An organisation will identify staff for 2 key roles: Responsible Officer (RO) and the Organisation Maintenance Officer (OMO). An RO is the officer who is registered with the HI Service and has authority to act on behalf of the organisation in its dealings with the System Operator of the My Health Record System. An RO can also be an OMO, there is not a need to separate both roles.



If the RO, OMO or healthcare individual does not have a PRODA account, they will need to [create a PRODA account](#) before registering for My Health Record.

#### STEP ONE

**Login to PRODA and register with the HI Service.**  
(Go to step 2 if your organisation is already registered with the HI Service.)

Register your seed/network organisation with the HI Service and My Health Record using HPOS. You will need:

- three government-issued documents
- a personal email address
- three security questions.

#### STEP TWO

**Check organisation has conformant clinical software.**  
(Go to step 3 if your organisation has conformant clinical software)

RO to link all relevant staff HPI-Is to the HPI-O in PRODA.

#### STEP THREE

**Register for My Health Record.**  
(Complete this step if your organisation is registered with the HI Service and has conformant clinical software)

- Apply for organisational NASH PKI in HPOS.
- NASH PKI Certificates received – configure in software  
(Note: Other clinical providers require their HPI-Is to be recorded in their clinical software.)
- Formalise security and access policy and complete staff training.
- Start using MHR in clinical software.

A **Contracted Service Provider (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.

## 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 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 the National Disability Insurance Scheme (NDIS).

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

**Note: Ensure at least one of your healthcare providers has an 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 an HPI-I prior to your organisation registering for My Health Record. They can apply for an HPI-I via their HPOS account.

See more information on [applying for a HPI-I](#).

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.

### 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](#)

## Determine how you will access My Health Record

There are two options to access patients' My Health Records:

1. Via [conformant software](#) which allows healthcare providers to view and upload to their patient's My Health Record.
2. 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](#) and 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.

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, private medical specialist, or the head office of a larger medical group.

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. All organisations will need to first register a Seed Organisation, prior to establishing any network organisations.

The majority of Healthcare Provider Organisations in Australia are independent – for example, suburban GP practices, pharmacies, private health specialists, or allied health care organisations. They will most likely participate in the My Health Record system as an independent Seed Organisation, rather than part of a network hierarchy.

It is important for organisations to determine their structure within the HI service prior to registration for My Health Record.

Larger medical groups or hospital groups are encouraged to contact the Agency help desk for support and to discuss considerations before determining their structure.

- Phone: 1300 901 001 during business hours
- Email: [help@digitalhealth.gov.au](mailto:help@digitalhealth.gov.au)

## Understanding the seed and network organisation structures

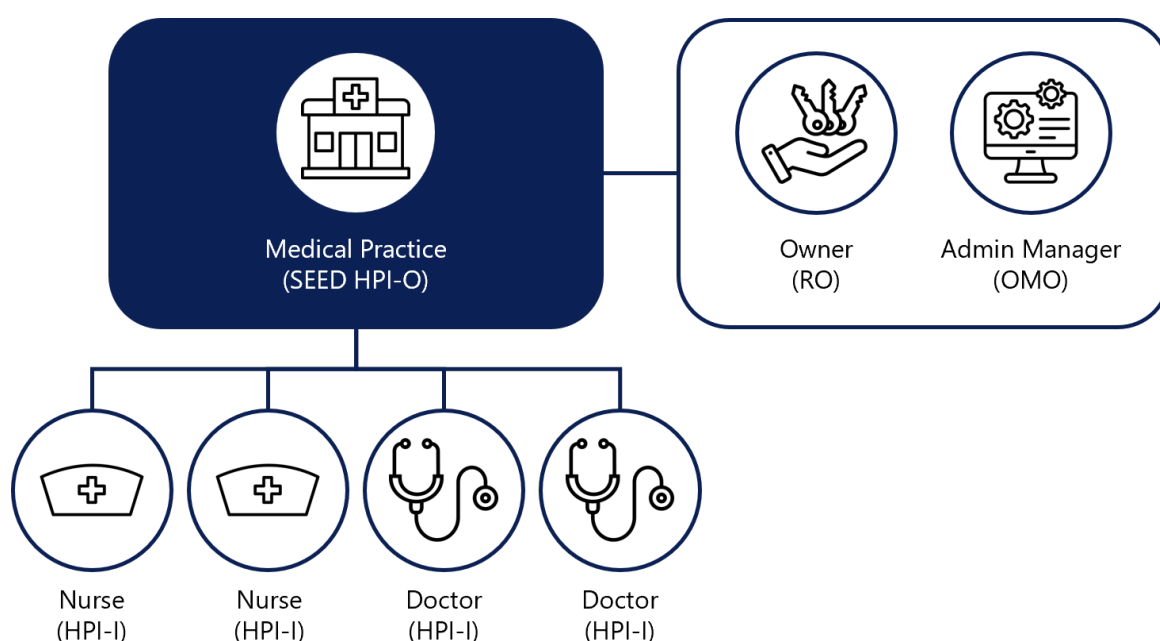
Healthcare provider organisations participate in the My Health Record system either as a seed organisation only or as a network organisation that is part of a wider 'network hierarchy' (under the responsibility of a seed organisation).

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.





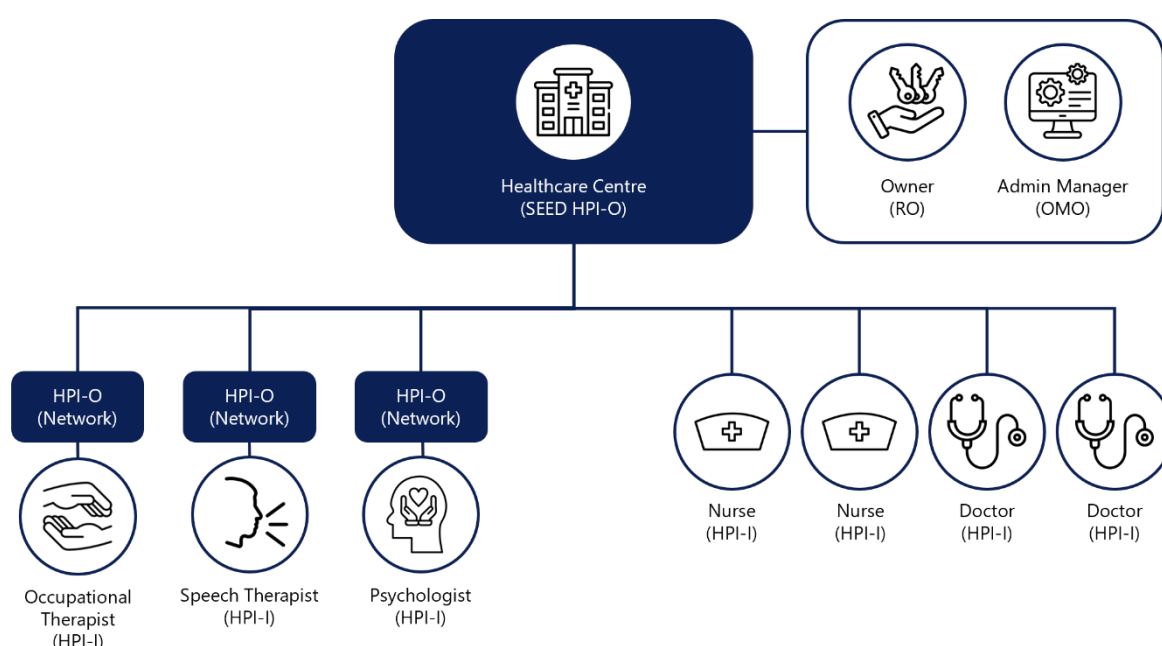
## Network organisations

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.



## 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.



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

	Responsible Officer (RO)	Organisation maintenance officer (OMO)
HI Service	<ul style="list-style-type: none"> <li>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.</li> <li>The RO is also an OMO by default.</li> </ul>	<ul style="list-style-type: none"> <li>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.</li> <li>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</li> </ul>
	<ul style="list-style-type: none"> <li>Register a seed organisation.</li> <li>Request a PKI certificate (or link an existing one) for the organisation.</li> <li>Maintain the HPI-O details with the HI Service.</li> <li>Maintain their own RO details with the HI Service (add or remove RO).</li> <li>Maintain OMO details with the HI Service (add or remove OMO) for seed and network levels.</li> <li>Retire, deactivate and reactivate the HPI-O.</li> <li>Maintain links between the seed organisation (and any network organisation/s) and any Contracted Service Provider.</li> </ul>	<ul style="list-style-type: none"> <li>Maintain their own OMO details.</li> <li>Validate, link or remove linked HPI-Is to HPI-O(s) they are linked to.</li> <li>Request PKI certificate(s) (or link existing one) for organisation(s) they are linked to.</li> <li>If required, maintain a list of authorised employees within the organisation who access the HI Service.</li> <li>Register a network HPI-O for lower network levels.</li> <li>Register OMO details for lower network levels.</li> </ul>
My Health Record System	<ul style="list-style-type: none"> <li>Authorise the addition/removal of HPI-Os.</li> <li>Adjust the My Health Record system access flags for participating organisations within their hierarchy (OMO at seed level can also do this).</li> <li>Set HPI-O/HPI-I authorisation links.</li> </ul>	<ul style="list-style-type: none"> <li>Set and maintain access flags according to the organisational network hierarchy, in accordance with meeting the principles outlined in the My Health Record Rules.</li> <li>Set HPI-O/HPI-I authorisation links.</li> <li>Act on behalf of the seed and network organisation(s) (that they are linked to) according to the hierarchy.</li> <li>Maintain accurate and up-to-date records of the linkages between organisations within their network hierarchy.</li> </ul>



### QUICK TIP:

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

## 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.

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 \$315,000.00 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 My Health Record, 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 My Health Record, and legislation specific to the My Health Record 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 Australian Digital Health Agency 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.

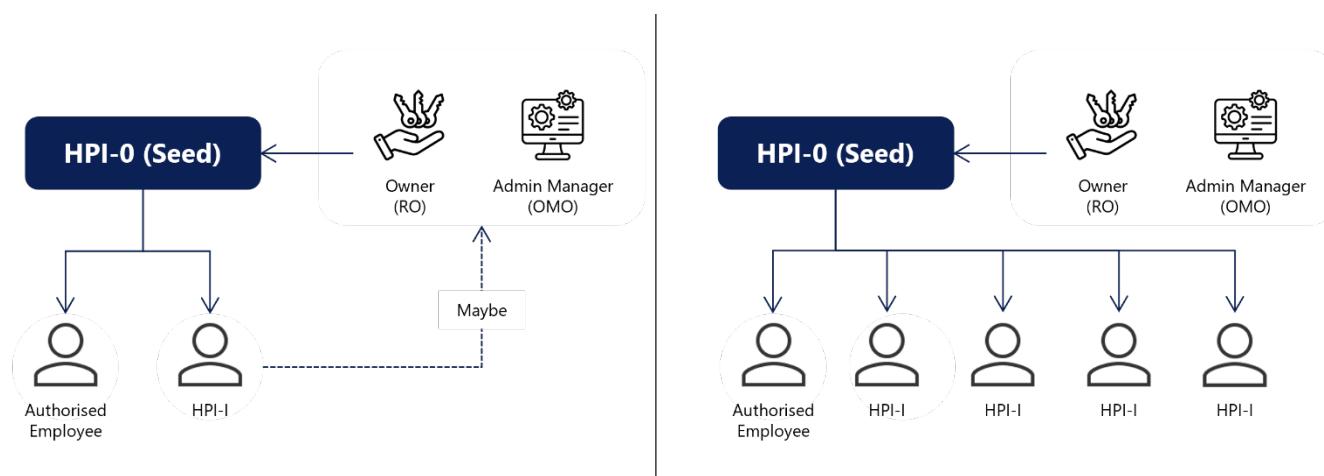
#### Authorised employee:

- **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 Australian Digital Health Agency 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.

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](#).

## 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.

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. Many common clinical information systems (CISs) conform to My Health Record and can connect directly to the system. This means that healthcare providers are generally able to access, view and upload information to a patient's record through their conformant CIS. [Click here to check whether your clinical software conforms to the standard](#). To access My Health Record using conformant clinical software, your organisation needs either a National Authentication Service for Health (NASH) certificate or a Contracted Service Provider (CSP) number for linking. Check with your software vendor whether you need to have a NASH PKI Certificate or whether they will be interacting with the system as a Contracted Service Provider (CSP).
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](#)'.

## 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.



### QUICK TIP:

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

## Accessing My Health Record via the National Provider Portal using PRODA

Once you have established, communicated, and maintained a security and access policy for your organisation, you can access My Health Record through the National Provider Portal by logging on to PRODA.

### STEP ONE

**Connect the My Health Record tile under the 'Linked Services' section of PRODA.  
(If the My Health Record tile is visible, go to step two.)**

1. Click on the My Health Record tile from 'Available Services' to open the linking screen.
2. Select the identifier type and enter the associated identifier number.
3. Click 'Save', a message confirming the linking process is underway.

### STEP TWO

**Start using MHR in the National Provider Portal in PRODA.**

1. Click on the My Health Record tile, which will redirect users to the National Provider Portal landing page.
2. Individuals can select the seed organisation they are representing.
3. Ensure staff have completed training and participation obligations have been considered.

To perform a search on a patient, 5 key sources of information are required:

- First name
- Last name
- Date of birth
- Gender
- Identifier number (IHI, Medicare number or DVA number)

## 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.
- 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 Security and Access 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 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 Australian Digital Health Agency 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.

[Get more information about privacy and security compliance.](#)

## 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:
  - there has been an unauthorised collection, use or disclosure of health information included in an individual's My Health Record
  - 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 system is an important part of compliance. A number of [training checklists and training resources](#) can be found on the Australian Digital Health Agency 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 controls

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).

### Access controls

Individuals can decide which of their healthcare provider organisations can view their health information by restricting access to their entire record, or to specific documents within it.

#### Limiting access to a My Health Record

Patients can decide which healthcare provider organisations can view or update their record by setting a Record Access Code (RAC).

Where an RAC has been set, the healthcare recipient can choose to share this code with you, so that you can access their record. Once the patient has shared their RAC with you, you will be listed on their provider access list. Healthcare provider organisations that are listed on a patient's provider access list won't need the patient's RAC to continue accessing their record.

#### Limiting access to specific documents

Where a limited document access code has been set, the healthcare recipient (or their representative(s)) can choose to provide healthcare provider organisation(s) with the limited document access code. Once a healthcare provider enters the limited document access code into their clinical information system, or the National Provider Portal, they will be able to access the restricted document(s). Healthcare providers can still view restricted documents in an emergency.

It is important that any access codes provided by the individual are not retained by the healthcare provider organisation and are destroyed following their use. [Find more information on patient controls](#).

## When NOT to upload a patient's record

The healthcare provider organisation must comply if a patient requests that information not be uploaded to their My Health Record. If a patient requests this, the healthcare provider organisation should inform the patient that Medicare information relating to the clinical encounter may be visible in their My Health Record, so the patient will have to remove or manage access to that information themselves through the National Consumer Portal. This is particularly relevant where the information may be regarded as sensitive.

Generally, there is no need to obtain a patient's consent to upload information to their My Health Record. However, ACT, NSW, and Qld have laws that require a patient's consent to upload specific health information to

their My Health Record. These laws are specified by the My Health Records Regulation 2012 and generally prohibit the disclosure of information relating to HIV (ACT, NSW, Qld), notifiable conditions (ACT, Qld), contagious conditions (Qld), environmental health events (Qld), and perinatal history (Qld). This information can only be disclosed with consent.

Staff must ensure they are familiar with the process for preventing an upload of information to My Health Record, should the patient request that it not be uploaded or if there is a state or territory law requiring consent that and consent has not been obtained.

[More information on how to stop automatic uploads.](#)

## 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 [Australian Digital Health Agency website](#).

## Appendix A: Readiness checklist

This checklist aims to support healthcare organisations to get ready for using My Health Record. It contains hyperlinks for guidance and further information for each step. You can also access the checklist on the [Services Australia website](#).

	<p><b>Australian Government</b> <b>Australian Digital Health Agency</b></p>	 My Health Record	<p><b>Organisation Registration Checklist</b></p>
---	---	---	---

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

**About My Health Record**

<p>What is My Health Record and what are the benefits?</p>	<p>My Health Record is a secure online summary of key patient health information. Healthcare providers can access the system to view and add information. The following resources provide more information about My Health Record:</p> <ul style="list-style-type: none"> <li>Digital Health <a href="#">website</a> and <a href="#">benefits for healthcare providers</a></li> <li>Access free <a href="#">online eLearning modules</a> or <a href="#">podcasts</a></li> <li>Join an upcoming <a href="#">webinar</a></li> <li>Find information on <a href="#">uploading, viewing</a> and <a href="#">organisation registration</a>.</li> </ul>
<p>Information about <a href="#">PRODA</a> and <a href="#">HPOS</a></p>	<p>Provider Digital Access (PRODA) is an online authentication system used to securely access government online services. Health Professional Online Services (HPOS) is a fast and secure way for health professionals and administrators to do business with <a href="#">Services Australia</a>.</p>

**Information required to register an organisation for My Health Record**

<p>Business <a href="#">ABN/ACN</a></p>		<p>Responsible Officer (<a href="#">RO</a>)</p>	
<p>Trading Name</p>		<p>Organisation Maintenance Officer/s (<a href="#">OMO/s</a>)</p>	
<p>Street Address</p>		<p>Mobile Phone This allows receipt of the PIC code via SMS for NASH PKI Certificate (if required)</p>	
<p>Postal Address</p>		<p>Organisation Type Check options on the <a href="#">Services Australia website</a></p>	
<p>Email Personal email of individual completing registration</p>		<p>Connection Type Will the organisation be connecting to My Health Record via a <a href="#">conformant clinical information system</a> or the <a href="#">National Provider Portal</a>?</p>	

**Understanding Healthcare Identifiers**

<p>Healthcare Provider Identifier – Organisation (HPI-O)</p>	<p>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 <a href="#">Healthcare Identifiers Service (HI Service)</a> via HPOS.</p>
<p>Healthcare Provider Identifier – Individual (HPI-I)</p>	<p>An HPI-I identifies an individual healthcare provider. Health professionals registered with the Australian Health Practitioner Regulation Agency (Ahpra) can locate their HPI-I by accessing their account via the <a href="#">Ahpra website</a> or by calling the HI Service (1300 419 495). Non-Ahpra registered health professionals can <a href="#">apply for an HPI-I online via HPOS</a>.</p>
<p>Individual Healthcare Identifier – (IHI)</p>	<p>An IHI identifies an individual receiving healthcare services. Once the HPI-O and HPI-I are configured and correct patient demographics have been entered, conformant clinical software or the National Provider Portal can retrieve and validate the patient's IHI and confirm the patient's My Health Record status.</p>

PAGE 1





## Organisation Registration Checklist

### Assign Responsible Officer (RO) and Organisation Maintenance Officer (OMO) roles

<input type="checkbox"/>	Organisation identifies a RO & OMO/s	It is important to understand My Health Record and HI Service <a href="#">roles and responsibilities</a> including the Responsible Officer (RO) and Organisation Maintenance Officer (OMO). The RO and OMO/s are responsible for ensuring the steps in this document are completed for their organisation. Each organisation can have only one RO but can have multiple OMOs. The RO will complete the initial organisation registration in HPOS and make a record of the individuals who are the RO and OMO/s in the organisation's My Health Record security and access policy. RO and OMO details can be <a href="#">added, removed or changed via HPOS</a> as required.
--------------------------	--------------------------------------	---

### Policies and Education

<input type="checkbox"/>	Establish a My Health Record security and access policy.  See <a href="#">online steps</a> for establishing a My Health Record Policy which covers user account management and access, security measures and management of data breaches, staff training and policy implementation and management.	It is a legislative requirement that a <a href="#">My Health Record security and access policy</a> be implemented as described in the <a href="#">My Health Records Rule 2016</a> .  A My Health Record security and access policy <a href="#">template</a> has been developed by the Office of the Australian Information Commission (OAIC), in collaboration with the Agency, to assist you in developing a policy for your organisation.  A downloadable copy of policy requirements <a href="#">checklist</a> is also available.
<input type="checkbox"/>	Establish a 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 NASH PKI are required to have policies and procedures in place governing use of the NASH PKI Certificate. Full details are available on the <a href="#">Services Australia</a> website. Download <a href="#">Sample NASH PKI certificate policy</a> .
<input type="checkbox"/>	Recognise privacy and security obligations.	Both the <a href="#">Digital Health website</a> and the <a href="#">Australian Digital Health Agency Cyber Security Centre</a> website hold information and resources to optimise privacy and security for My Health Record and other healthcare systems. An <a href="#">online eLearning module</a> is also available. Information regarding ongoing participation obligations are available <a href="#">here</a> .
<input type="checkbox"/>	Complete staff My Health Record training.	Healthcare provider organisations must provide staff with My Health Record training <i>before</i> they are authorised to use the system. See a list of <a href="#">Recommended My Health Record Training</a> . Access a range of training and support materials here: <ul style="list-style-type: none"> <li>• My Health Record <a href="#">education and training</a></li> <li>• Access <a href="#">online eLearning modules</a> or <a href="#">podcasts</a></li> <li>• Join an upcoming <a href="#">webinar</a></li> </ul>

### Registering an organisation with Healthcare Identifiers Service (HI Service) via HPOS

<input type="checkbox"/>	RO registers <a href="#">Seed Organisation</a> for the Healthcare Identifier 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.	My Health Record registration step by step instructions are available on the <a href="#">Digital Health website</a> and the <a href="#">Services Australia website</a> . The RO completes the registration request for a Seed Organisation by accessing HPOS via PRODA. When registering an organization for the HI service, the organisation will be allocated a unique 16-digit HPI-O. To deactivate, reactivate and retire an HPI-O complete <a href="#">this form</a> and follow steps to upload via HPOS.
<input type="checkbox"/>	RO checks HPOS Messages.	RO logs into HPOS via PRODA and checks their HPOS Messages for the message which contains the HPI-O, details of the RO and OMO and how to apply for a <a href="#">NASH PKI Certificate</a> when using conformant software to access My Health Record.
<input type="checkbox"/>	RO or OMO registers network organisation/s, if required. A Network	If your organisation wishes to register one or more <a href="#">Network Organisations</a> , RO or OMO can follow <a href="#">these steps</a> to create a network organisation underneath the Seed



## Organisation Registration Checklist

<input type="checkbox"/>	Organisation is a sub-entity of a Seed Organisation that provides healthcare services.	Organisation. A unique HPI-O will be provided for each new Network Organisation created. Ensure the option to 'apply for access to the My Health Record system' is selected when creating network organisations that will require access to the system. Each network organisation will require a separate NASH PKI certificate (unless using the <i>CSP Approach</i> , see below). RO should consider when it is appropriate to set access flags when registering any network organisations for My Health Record.
<input type="checkbox"/>	Set access flags for any network organisations.	Access flags allow healthcare provider organisations to be identifiable to healthcare recipients in their My Health Record access history and gives different parts of a large organisation different access to the My Health Record system. Information about Access flags can be found on the <a href="#">Services Australia website</a> and in Division 4 of the <a href="#">My Health Record Rule 2016</a> . Access flags allow network organisations to either inherit their parent organisation's access (flag set to 'No') or have access separate from their parent organisation's access (flag set to 'Yes'). A seed organisation is always set to 'Yes'. For further support regarding network organisations, contact the HI Service.
<input type="checkbox"/>	<b>NASH Approach</b> Apply for a <a href="#">National Authentication Service for Health</a> (NASH) Public Key Infrastructure (PKI) Certificate for Healthcare Provider Organisations using <a href="#">conformant software</a> to access My Health Record.  <i>A NASH PKI Certificate may not be required for some conformant software (eg. Genie (CSP), GENTU, Aquarius, Clinic to Cloud, MMEx). Check with your software provider to confirm and proceed to 'CSP Approach'.</i>  <i>If not using conformant software, proceed to 'NPP Approach' step.</i>	RO or OMO logs into HPOS via PRODA and <a href="#">requests a NASH PKI Certificate</a> , selecting the correct software product and version number. Ensure a mobile phone number is entered when prompted to receive an SMS with the Personal Identification Code (PIC) to install the NASH certificate within 30 days. A NASH certificate needs to be configured/installed into the software product to be functional. Contact your software provider for support with NASH certificate installation. Certificates are valid for 2 years and RO or OMO should plan to apply and install a new NASH Certificate before the expiry date.
<input type="checkbox"/>	<b>CSP Approach</b> If using software using a Contracted Services Provider (CSP) then link HPI-O to CSP Number in HPOS. <i>A NASH certificate does not need to be downloaded if the organisation is using a CSP product to access My Health Record.</i>	<a href="#">RO/OMO links HPI-O to CSP number</a> , which is provided by the CSP software provider, in both the 'CSP Links' tab and added under <a href="#">Manage Authorisation Links</a> in HPOS. Follow the steps in this <a href="#">guide</a> .
<input type="checkbox"/>	<b>NPP Approach</b> <a href="#">Is your software My Health Record Conformant?</a> If not, your organisation can access My Health Record using the National Provider Portal.	Follow these <a href="#">step-by-step instructions</a> to register the organisation and individuals for the National Provider Portal. Click here to access the <a href="#">National Provider Portal online</a> or via <a href="#">PRODA</a> . 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 <a href="#">links all HPI-Is to the HPI-O</a> via HPOS to allow appropriate individuals access to My Health Record. If using conformant software, check with the software provider whether this step is required.

### Software Configuration

<input type="checkbox"/>	Add HPI-Is of clinical staff to software. Linking HPI-Is to the HPI-O in HPOS is required for <i>National Provider Portal</i> and some conformant software.	Contact your software provider for support with configuring software. HPI-Is of clinical staff who will be accessing My Health Record will need to be entered into the software. For those organisations using the National Provider Portal, the RO and/or OMO must link all HPI-Is to the HPI-O by <a href="#">managing HPI-I Authorisation Links</a> . Please check with your conformant software provider if linking in HPOS is required.
--------------------------	---	--



## Organisation Registration Checklist

<input type="checkbox"/>	Add HPI-O to clinical software.	Check your software providers resources or contact IT service provider for configuration support.
<input type="checkbox"/>	Install NASH PKI Certificate in software.	Check your software provider's resources or contact IT service provider to arrange configuration support. A Personal Identification Code (PIC) will be required.
<input type="checkbox"/>	Update software settings to ensure permission for staff accessing My Health Record.	Check your software provider's resources 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.
<input type="checkbox"/>	Validate an Individual Healthcare Identifier (IHI).	Check your software provider's resources for instructions to confirm that your software has been configured correctly to access My Health Record (using either the NASH or CSP approach) and that your software can retrieve and validate a patient's IHI.
<input type="checkbox"/>	Register with a Prescription Exchange Service (PES).	Contact Prescription Exchange Service (PES) provider: <a href="#">eRx Script Exchange</a> (1300 700 921) or <a href="#">MediSecure</a> (1800 472 747)
<input type="checkbox"/>	Check if conformant software can access My Health Record.	Contact your software provider or the Agency helpline (1300 901 001) if there are connection errors (if you are getting an error message).

### Inform your patients

<input type="checkbox"/>	Provide information to your patients.	A range of information is available on the <a href="#">Digital Health website</a> . Print on Demand resources such as brochures, counter cards and posters are available. Please contact your local Primary Health Network or clinical peak organisation to order.
<input type="checkbox"/>	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
<b>Healthcare Identifiers (HI) Service Enquiry Line</b>	Identifier queries (HPI-Os, HPI-Is, IHIs) and organisation registration	Phone <b>1300 361 457</b> Email <a href="mailto:healthcareidentifiers@servicesaustralia.gov.au">healthcareidentifiers@servicesaustralia.gov.au</a>	Mon–Fri 8.30am – 5.00pm AEST & AWST
<b>PRODA Help</b>	PRODA queries	Phone <b>1800 700 199</b>	Mon–Fri 8.00am – 5.00pm AWST
<b>HPOS Help</b>	HPOS queries	Phone <b>132 150</b>	Mon–Fri 8.00am to 5.00 pm AWST
<b>eBusiness Service Centre</b>	Certificates, including Medicare PKI Site Certificates and NASH	Phone <b>1800 700 199</b>	Mon–Fri 8.00am – 5.00pm AEST & AWST
<b>My Health Record Help Line</b>	General enquiries and detailed support for individuals and healthcare providers	Phone <b>1800 723 471</b> (option 2 for providers)	Open 24 hours, 7 days
<b>Australian Digital Health Agency Help Centre</b>	Complex queries, provider enquiries, secure messaging delivery enquiries, and digital health education	Phone <b>1300 901 001</b> Email <a href="mailto:help@digitalhealth.gov.au">help@digitalhealth.gov.au</a>	Mon–Fri 8.00am – 5.00pm AEST

Updated: March 2023



## 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.