Australian Government
Services Australia

Healthcare Identifiers Service
Application to register a healthcare support service provider (HW096)

When to use this form

Use this form to:

- register a healthcare support service provider (HSP) and a responsible officer (RO) and organisation maintenance officer (OMO) with the Healthcare Identifiers (HI) Service and receive a healthcare identifier for the organisation (complete **Part A**) and/or
- request a National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) certificate for your HSP (complete **Part B**).

Services Australia uses the HI Service to register a HSP. A HSP is issued with a 16 digit registration number. A HSP must be registered in the HI Service before applying for a NASH PKI certificate.

Healthcare support service provider

A HSP is a legal entity that has applied to be registered as, or is registered as a healthcare support service provider under the *Healthcare Identifiers Act 2010*.

Healthcare Identifiers Service

The HI Service is a system that provides a consistent set of identifiers for individuals and healthcare providers. Healthcare identifiers provide a way for you to match the correct records to the person you are treating. You can include them in health records, patient files and other health related information. This improves accuracy when you share health information with other healthcare providers.

The *Healthcare Identifiers Act 2010* is available at **legislation.gov.au**

Role of the responsible officer

The RO is responsible for a HSP organisation's interaction with the HI Service. Their main responsibility is to make sure the HSP and authorised employees comply with the *Healthcare Identifiers Act 2010* and the *Healthcare Identifiers Regulations 2010*.

For more information about the role of a RO, go to **servicesaustralia.gov.au/hiservice**

Role of an organisation maintenance officer

The OMO is responsible for keeping information about their organisation in the HI Service up-to-date and making sure information about authorised employees is maintained.

For more information about the role of an OMO, go to **servicesaustralia.gov.au/hiservice**

Getting a National Authentication Service for Health Public Key Infrastructure certificate

You need a NASH PKI certificate to access the HI Service. If a NASH PKI certificate has already been issued, HI Service access can be added to the existing certificate complete **Part A**, question 16 for a HSP organisation).

Documents needed to prove identity

If you have previously provided us with sufficient evidence of identity (EOI), you do not need to do it again. You can supply your known customer or registration number.

Evidence of identity

If you are **not** a known customer, you must provide a minimum of **one** document from the Primary group and **one** document from the Secondary group. You must include a Deed Poll or marriage certificate if there is a difference in name in these documents.

Primary group

- Australian passport
- Australian birth certificate
- Australian citizenship certificate
- foreign passport
- Australian driver licence
- Australian Government issued proof of age card or photo card
- ImmiCard

Secondary group

- Department of Foreign Affairs and Trade (DFAT) issued Certificate of Identity or Document of Identity
- DFAT issued United Nations convention travel document
- Australian marriage certificate
- Australian change of name certificate
- foreign government issued documents (for example, driver licences)
- Medicare card
- enrolment with the Australian Electoral Commission
- security guard or crowd control photo licence
- evidence of right to a government benefit (Department of Veterans' Affairs or Centrelink)
- consular photo identity card issued by DFAT
- police force officer photo identity card
- Australian Defence Force photo identity card
- Commonwealth, state or territory government photo ID card
- Aviation Security Identification card
- Maritime Security Identification card
- firearms licence
- credit reference check
- Australian tertiary student photo identity document
- certified academic transcript from an Australian university
- trusted referee's report
- bank or credit card
- other authoritative online sources of evidence verified by a third party identity provider.

Certified copies of original documents

If you are attaching documents, the copies provided must be certified. For information about how to certify documents, go to **servicesaustralia.gov.au/hiservice**

Authority to commit the organisation

If the organisation is not a known customer you must provide documentary evidence of the existence of the organisation as a legal business entity and your authority to commit the business. Acceptable documentary evidence includes a certified copy of one of the following documents:

- certificate of registration of a company issued by the Australian Securities and Investments Commission (ASIC) and your name listed as the Public Officer
- the notice issued by the Registrar of the Australian Business Register (ABR) bearing the business entity's name, Australian Business Number (ABN) and your name listed as the Public Officer
- the organisation's appointment as a trustee (if the legal structure is a trust) with you as a stakeholder
- contract for sale or purchase of business addressed to you
- statement of transaction issued by a financial institution in the name of the company, addressed to you and less than 1 year old
- lease agreement for the organisation's primary place of business addressed to you
- rates notice for the organisation's primary place of business addressed to you
- certificate of change of name for the organisation issued by the ASIC and addressed to you
- a document issued by the Australian Taxation Office with the organisation's name and tax file number and addressed to you.

If you are not listed on these documents you will also need to establish that you are authorised to act on behalf of the organisation and to commit the business. You may need to provide one of the following:

- an affidavit or statutory declaration sworn by a member of the board or executive of the organisation
- a deed of appointment
- any other documentation which displays that you hold a position of authority to commit the business.

Reviewing your organisation's privacy processes

We recommend that you review your organisation's privacy policy and relevant privacy notices as part of this application process.

You need to check that your organisation is either:

- obtaining consent from the individual receiving healthcare for the collection, use and disclosure of sensitive health information
- required or authorised to collect this information under an Australian law or a court or tribunal order.

You also need to check that your organisation has processes in place to provide the individual receiving healthcare with a privacy notice.

For more information about the Healthcare Identifiers Service

You can:

- go to **servicesaustralia.gov.au/hiservice**
- email **healthcareidentifiers@servicesaustralia.gov.au**
  There may be risks with sending personal information through unsecured networks or email channels.
- call 1300 361 457 Monday to Friday, 8:30 am to 5 pm, Australian Eastern Standard Time (call charges may apply).

Filling in this form

You can complete this form on your computer using Adobe Acrobat Reader, or you can print it.

For help on how to fill in our forms, go to **servicesaustralia.gov.au/formhelp**

If you have a printed form:

- Use black or blue pen.
- Print in BLOCK LETTERS.
- Where you see a box like this ☐ ***Go to 1*** skip to the question number shown.

Returning this form

Return this form and any supporting documents by:

- **email** to **healthcareidentifiers@servicesaustralia.gov.au**
  There may be risks with sending personal information through unsecured networks or email channels.
- post to
  Services Australia
  HI Service
  GPO Box 2987
  MELBOURNE VIC 3001

PART A — Healthcare Identifiers Service

Complete **Part A** if your HSP organisation is not registered in the HI Service and you want to register a HSP, an RO and an OMO with the HI Service and receive a healthcare identifier for that HSP.

Applicant's details

The applicant for this form must be the person who will be the RO for the HSP and must complete all sections of **Part A**.

1 Are you a known customer?

No ☐ Certified EOI must be provided with this application ▶ ***Go to 3***

Yes ☐

2 Type of known customer

Tick one only and provide the associated number in the field below

You have an existing individual Provider Digital Access (PRODA) Registration Authority *(RA number)* ☐

You have a Medicare provider number ☐

You are an existing responsible officer (RO) of a healthcare provider organisation (*RO number*) ☐

You are an existing contracted service provider (CSP) officer registered in the HI Service (*CSP officer number*) ☐

You are the Certificate Manager for a healthcare provider organisation's existing NASH PKI certificate (*RA number*) ☐

Known customer identifier

Responsible officer's details

3 Dr ☐ Mr ☐ Mrs ☐ Miss ☐ Ms ☐ Mx ☐ Other ☐

Family name

First given name

Second given name

4 Date of birth (DD MM YYYY)

5 Gender

Male ☐

Female ☐

Non-binary ☐

6 The address, phone number and email address supplied must be for business purposes. This information is required for the HI Service and, if relevant, will also be used for the My Health Record system.

Business address

Postcode

7 Daytime phone number (including area code)

Email

Organisation maintenance officer's details

8 Will you be the OMO for the HSP organisation?

If you are not sure, you can become the OMO and designate a new OMO at a later date.

No, somebody else will have this role ☐ ***Go to 9***

Yes, I will be the RO and the OMO ☐ ***Go to 16***

Yes, I will be the RO and the OMO and would like to register an additional OMO ☐ ***Go to 9***

New or additional organisation maintenance officer details

9 Is the new or additional OMO a known customer?

No ☐ ***Go to 11***

Yes ☐

10 Type of known customer

Tick one only and provide the associated number in the field below

The OMO has an existing individual PRODA Registration Authority *(RA number)* ☐

The OMO has a Medicare provider number ☐

The OMO is an existing RO of a healthcare provider organisation *(RO number)* ☐

The OMO is a CSP officer registered in the HI Service *(Contracted Service Provider (CSP) officer number)* ☐

The OMO is the Certificate Manager for a healthcare provider organisation's existing NASH PKI certificate *(RA number)* ☐

Known customer identifier

MCA0HW096 2611

11 Dr ☐ Mr ☐ Mrs ☐ Miss ☐ Ms ☐ Mx ☐ Other ☐

Family name

First given name

Second given name

12 Date of birth (DD MM YYYY)

13 Gender

Male ☐
Female ☐
Non-binary ☐

14 The address, phone number and email address supplied must be for business purposes. This information is required for the HI Service and, if relevant, will also be used for the My Health Record system.

Business mailing address (if different to the ROs)

Postcode

15 Daytime phone number (including area code)

Email

HSP details

16 HSP organisation's name (registered business name)

17 Trading name (if different to above)

18 HSP organisation's Australian Business Number (ABN) or Australian Company Number (ACN)

ABN

OR

ACN

HSP service details

19 Business address

Postcode

Postal address (if different to above)

Postcode

20 Daytime phone number (including area code) **Tick one preferred method of communication** ☐

Mobile phone number ☐

Fax number (including area code) ☐

Email ☐

HSP organisation's National Authentication Service for Health Public Key Infrastructure details

21 Does the HSP organisation want a NASH PKI certificate?

No ☐
Yes ☐ ***Go to Part B***

Checklist – Part A

22 Which of the following documents are you providing with this form?

Your application cannot be processed unless all relevant questions are answered and supporting documentation is supplied to us. Where you are asked to supply documents, provide certified documents.

If you are not sure, check the question to see if you should provide the documents.

Certified identification for the RO (if applicable) (refer to **Documents needed to prove identity** on page 1)	☐
Certified identification for the OMO (if applicable) (refer to **Documents needed to prove identity** on page 1)	☐
Evidence that the RO has the authority to commit the healthcare support service provider organisation (refer to **Authority to commit the organisation** on page 2)	☐

Privacy notice

23 Your privacy in the Healthcare Identifiers Service

If you complete Part A

The privacy and security of your personal information is important to Services Australia and is protected by law. Services Australia, as the service operator of the Healthcare Identifiers Service, collects your personal information to register a healthcare support service provider and an authorised officer with the Health Identifiers Service.

We collect this information under paragraphs 8(2) and 11 of the Healthcare Identifiers Regulations 2020.

If you do not provide the requested information, Services Australia may be unable to process your application or register healthcare support service provider or authorised officer.

Your personal information may be used by Services Australia or disclosed to other parties, such as other Australian Government departments and agencies, or where it is required or authorised by law (including the *Healthcare Identifiers Act 2010* and *Privacy Act 1988*).

This includes disclosing healthcare identifiers, identifying information and professional business details to the Australian Digital Health Agency as the Healthcare Provider Directory Operator, as authorised under the *Healthcare Identifiers Act 2010* and relevant regulations.

For more information, including how to access or correct your personal information or make a privacy complaint, go to **servicesaustralia.gov.au/privacypolicy**

Declaration

24 I declare that:

- I have provided certified copies of relevant documentation to support this application
- I will only access and use healthcare identifiers for the purposes defined in the *Healthcare Identifiers Act 2010*
- the organisation that I am registering is eligible for provision of a Healthcare Support Service Provider – Organisation under the *Healthcare Identifiers Act 2010*
- I understand the roles and responsibilities of the responsible officer and organisation maintenance officer. If the organisation maintenance officer is someone other than myself I will make sure that person is aware of the requirements of the organisation maintenance officer role
- I have read, understand and agree to **Your privacy in the Healthcare Identifiers Service** on page 5
- the information I have provided in this form is complete and correct.

I understand that:

- penalties for unauthorised access and misuse apply under the *Healthcare Identifiers Act 2010*
- giving false or misleading information is a serious offence.

Responsible officer's signature

On completion, print and sign by hand.

Date (DD MM YYYY)

PART B — National Authentication Service for Health Public Key Infrastructure certificate

Entity details

1 Entity registration number (if known)

2 Entity name

Entity's legal person

Your entity's legal person's name is the name of an individual (for example, trustee or partner), company or other entity that the entity comprises or forms part of, and that has the capacity to enter into contracts, and sue and be sued, in its own name.

3 Name of the entity's legal person

4 Entity's Australian Business Number (ABN) or Australian Company Number (ACN)

ABN

OR

ACN

Authorised officer's details

5 Dr ☐ Mr ☐ Mrs ☐ Miss ☐ Ms ☐ Mx ☐ Other ☐

Family name

First given name

Second given name

6 Position

7 Daytime phone number (including area code)

Mobile phone number

Privacy notice

8 ***If you complete Part B***

Personal information is protected by law, including the *Privacy Act 1988*.

Personal information is collected by Services Australia for purposes relating to the provision of healthcare, including the issue of a National Authentication Service for Health Public Key Infrastructure certificate and operation of the National Authentication Service for Health Public Key Infrastructure.

Your organisation's healthcare identifier and other information collected as a result of the submission of this application is regulated by the *Healthcare Identifiers Act 2010*.

As a result of the submission of this application, Services Australia may collect personal information about individuals named in the application from other Commonwealth agencies or people, including, for example, the Chief Executive Medicare (the Healthcare Identifiers service operator).

Personal information may be used by Services Australia or given to other parties, such as other Australian Government departments and agencies, where you have agreed to that, or where it is required or authorised by law (including the *Healthcare Identifiers Act 2010* and *Privacy Act 1988*).

You can get more information about the way in which Services Australia will manage your personal information, including our privacy policy, at **servicesaustralia.gov.au/privacypolicy**

Declaration

9 **The new entity's legal person agrees to be bound by**:

- the attached **National Authentication Service for Health Public Key Infrastructure certificate for entities Terms and Conditions of Use** and the **Relying Party Agreement** referred to in those Terms and Conditions of Use, **and**
- the relevant **Community of Interest Certificate Policy for the National Authentication Service for Health Public Key Infrastructure Certificate for Entities**.

The new entity's legal person declares that:

- the information provided in this form is complete and correct.

I acknowledge and confirm (on behalf of myself and the new entity's legal person) **that**:

- the individuals mentioned in this application form consent to Services Australia collecting, using and disclosing registration numbers of those individuals for the purposes outlined above (see **Privacy notice** on page 6)
- the individuals mentioned in this application form consent to the Healthcare Identifiers service operator, the My Health Record System Operator and the Chief Executive Medicare disclosing personal information about them to Services Australia for the purposes outlined above (see **Privacy notice** on page 6)
- the new entity's legal person consents to its entity details being published in the National Authentication Service for Health Directory.

I understand that:

- giving false or misleading information is an offence.

By signing this application, I confirm that I am duly authorised to legally bind the new entity's legal person.

Authorised officer's signature

On completion, print and sign by hand.

Date (DD MM YYYY)

Reset form

National Authentication Service for Health Public Key Infrastructure certificate for entities

Terms and Conditions of Use

Parties:

The Commonwealth as represented by Services Australia.

The new entity (Entity) named in the Application to register a healthcare support service provider

1. In consideration for Services Australia issuing the Entity with a National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) certificate for Entities (Certificate), provided to it on a compact disc (CD) or through electronic means, the Entity agrees that:
   a) it is legally bound by these Terms and Conditions of Use (Terms and Conditions), the terms of the NASH PKI Relying Party Agreement that apply to the Certificate and the relevant **Community of Interest Certificate Policy for the National Authentication Service for Health Public Key Infrastructure Certificate for Entities** (Certificate Policy), including as these documents are updated from time to time
   b) it will comply with the PKI documents mentioned in the Certificate Policy that are published by Services Australia on or linked to its website at **servicesaustralia.gov.au/pki**
   c) the Entity is responsible for uploading the Certificates from the CD (or electronic communication) onto its operating system
   d) the Certificate will only be used for purposes authorised or approved by Services Australia. Any other use of the Certificate will be at the Entity's risk
   e) the Entity is responsible for making sure that:
      i. when using its Certificate it does not collect, use or disclose any 'identifying information' or 'healthcare identifiers' (as those terms are defined in the *Healthcare Identifiers Act 2010*) except for purposes relating to the provision of healthcare
      ii. it has policies and procedures for the use of the Certificates, Keys and digital signatures generated using a Key attached to a Certificate by anyone acting under or through it or as its agent or representative that enables the individuals who have used the Certificate and Keys to be identified in respect of each use and the role they performed in respect of that use
      iii. those policies and procedures are known and understood by everyone acting under or through it or as its agent or representative in respect of the Certificate, Keys and digital signatures generated using a Key attached to a Certificate.
   f) the Entity will take all reasonable measures to keep its Private Key (attached to its Certificate) and the CD (or the electronic communication of the Private Key) secure at all times and take all necessary precautions to prevent its loss, disclosure, modification or unauthorised use
   g) the Entity will not give its Certificate or CD (or electronic communication of the Certificate) to any other entity or organisation or allow any unauthorised person to use them, except for any outsourced information technology service provider engaged by it to act as its agent in using its Certificate under contractual terms and conditions that require the service provider to only use the Certificate in accordance with these Terms and Conditions
   h) the Entity will promptly notify Services Australia in the event that the Entity considers that its Certificate has been, or may have been, lost, destroyed, stolen, disclosed, modified or compromised
   i) the Entity may request revocation of its Certificate at any time by written notice to Services Australia
   j) the Entity's use of its Certificate may be revoked by Services Australia in its absolute discretion, including but not limited to:
      i. after loss, destruction, theft, disclosure, modification or compromise of its Certificate
      ii. when the Keys or Certificates are considered or suspected to have been compromised
      iii. in the event of its insolvency or if it becomes subject to any form of external administration
      iv. in the event Services Australia cancels its registration with Services Australia
      v. in the event that the Entity breaches a term of the Certificate Policy, these Terms and Conditions or the Relying Party Agreement
      vi. in relation to a person that has applied to be registered as a repository operator or a portal operator under the *My Health Records Act 2012*, in the event that a decision is made not to register the person in that capacity under that Act
      vii. in the event the Entity has transitioned to a NASH Secure Hash Algorithm (SHA-2) PKI certificate, **or**
      viii. in the event Services Australia has been notified by relevant authorities that the Entity has been affected by a malware/virus and their PKI certificate and access to the My Health Record needs to be revoked.
   k) the Entity will immediately notify Services Australia upon becoming aware that any of the circumstances have occurred where its Certificate may be revoked
   l) revocation of the Entity's Certificate does not automatically terminate these Terms and Conditions
   m) all information the Entity provides and representations the Entity has made or makes to Services Australia are complete and accurate
   n) the Entity will promptly notify Services Australia in the event that the Entity considers any information provided, or representation made, by it is or may be incorrect, including the Entity's contact details

o) any use of the Entity's Certificate by any other entity as a result of a breach of these Terms and Conditions by the Entity will be deemed to also be a use of the Certificate by the Entity

p) either Services Australia or the Entity may terminate these Terms and Conditions at any time by giving a written notice to the other party, which will result in the Certificate being revoked. The Entity agrees that it will not use its Certificate after termination of these Terms and Conditions

q) if these Terms and Conditions are terminated, the Entity's obligations will continue in respect of any electronic communications the Entity made using its Certificate before the date of termination

r) the responsibility of Services Australia for any costs, losses or damage the Entity (or people acting on its behalf) incur associated directly or indirectly with its use of its Certificate is subject to and limited by the Certificate Policy and the documents mentioned in it as described in paragraph a) above

s) Services Australia may change or add to these Terms and Conditions at any time, by giving the Entity notice by mail, by fax or electronically. A message sent to the Entity's business email address (as held in the records of Services Australia) is one way of giving the Entity notice electronically

t) when the Entity uses its Certificate after the Entity has been notified of a change or addition to these Terms and Conditions, the Entity will be taken to have agreed to the change or addition in respect of all uses of its Certificate after that date. These Terms and Conditions may not be otherwise changed orally or by conduct by the Entity.

2. The Entity agrees that Services Australia will automatically renew its Certificate on or before its expiry, unless the Entity notifies Services Australia 60 business days before then that it does not want its Certificate to be renewed. The Entity agrees that these Terms and Conditions, as updated from time to time, will apply to the renewed Certificate.

3. These Terms and Conditions are governed by the laws of the Australian Capital Territory. The parties agree to submit to the non-exclusive jurisdiction of the courts of the Australian Capital Territory.