Australian Government
Services Australia

Healthcare Identifiers Service
Application to register a general supporting organisation (HW013)

When to use this form

Use this form to:

- register a general supporting organisation (GSO) and an authorised officer with the Healthcare Identifiers (HI) Service (complete **Part A**)
- request a National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) certificate for your GSO (complete **Part B**).

Services Australia uses the HI Service to register a GSO. A GSO is issued with a 16 digit registration number. This number is not a healthcare identifier.

A GSO must be registered in the HI Service before applying for a NASH PKI certificate.

General supporting organisation

A GSO is any one of the following:

- a legal entity that has applied to be registered as, or is registered as, a repository operator or a portal operator under the *My Health Records Act 2012*
- the National Repositories Service under the *My Health Records Act 2012*
- the operator of any component of the My Health Record System that the Australian Digital Health Agency determines to be a GSO.

The following organisations are not GSOs:

- a healthcare provider organisation (for example, an organisation which is generally directly involved in the delivery of healthcare)
- a contracted service provider (CSP) organisation within the meaning of the *Healthcare Identifiers Act 2010* or the *My Health Records Act 2012* (for example, an organisation which provides services under a contract to a healthcare provider organisation).

Register a general supporting organisation

To register a GSO, an authorised person must apply to be registered as the authorised officer of that GSO. An authorised officer will be linked to the GSO at the time of the GSO's application for registration.

Role of an authorised officer

An authorised officer must keep their own details and the details of the GSO they represent up to date.

A GSO must have at least one and up to a maximum of 3 authorised officers linked to it.

If an individual is registered in the HI Service in another capacity (see **known customer** section of this form), and that individual is applying to become an authorised officer of a GSO, existing details may be linked to a GSO using this form.

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/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/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.

Documents required from a repository operator or a portal operator

You must provide documentary evidence that:

- the organisation is registered as a repository operator or a portal operator under the *My Health Records Act 2012*, **or**
- you have applied for the organisation to be registered as a repository operator or a portal operator under the *My Health Records Act 2012*.

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 your organisation has a NASH PKI certificate AND you are listed as the approved person, this number can be provided as evidence of the business AND your authority to commit the business.

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 one 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.

National Authentication Service for Health Public Key Infrastructure

Public Key Infrastructure is technology and procedures that provide security and confidentiality for electronic business. NASH PKI provides digital certificates for authentication and protection of confidentiality, and integrity of electronic communications with Relying Parties.

For more information about NASH PKI, go to **servicesaustralia.gov.au/nash**

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.

For more information about the My Health Record system

Go to **digitalhealth.gov.au** or call 1800 723 471 Monday to Friday, 8:30 am to 5 pm, Australian Eastern Standard Time.

Filling in this form

You can fill this form digitally in some browsers, or you can open it in Adobe Acrobat Reader. If you do not have Adobe Acrobat Reader, you can print this form and complete it.

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
  PO Box 7788
  CANBERRA BC ACT 2610

PART A — Healthcare Identifiers Service

Authorised officer's details

As the person completing this form, you will be the authorised officer for the GSO being registered. If more than one officer is registering, **Part A** must be copied and completed for each individual applying to become an authorised officer for the GSO being registered.

Known customer

1 Are you a known customer?

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

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

You are an existing 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

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 both the HI Service and NASH PKI registration and, if relevant, will also be used for the My Health Record system.

Applicant's business address

Postcode

7 Daytime phone number (including area code)

Email

Type of general supporting organisation

8 The organisation is, or is applying to be:

Tick one only

a repository operator ☐

a portal operator ☐

the operator of a component of the My Health Record system ☐

the operator of a component of the National Repositories Service ☐

General supporting organisation details

If the GSO operates under a trading or preferred name, this name will appear within your organisation's NASH PKI certificate.

9 Organisation's legal name

10 Trading or preferred name (if different to above)

11 Organisation's Australian Business Number (ABN) or Australian Company Number (ACN)

ABN

OR

ACN

MCA0HW013 2412

12 Business address

Tick one preferred address for communication

Postcode ☐

Postal address (if different to above)

Postcode ☐

13 Daytime phone number (including area code)

Tick one preferred method of communication

☐

Mobile phone number ☐

Fax number (including area code) ☐

Email ☐

Checklist – Part A

14 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 EOI for the authorised officer (if you answered No at **question 1**) (refer to **Documents needed to prove identity** on page 1)	☐
Evidence that the authorised officer has the authority to commit the organisation (if applicable) (refer to **Authority to commit the organisation** on page 2)	☐
Your authorised officer details (required at **question 1** to **7**)	☐
Your GSO details (required at **question 8** to **13**)	☐
Documents required from a repository or portal operator (if applicable at **question 8**) (refer to **Documents required from a repository operator or a portal operator** on page 2)	☐

Privacy notice

15 ***If you complete Part A***

Your 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**

The My Health Record System Operator will collect personal information in this form from Services Australia for the purpose of the My Health Record system and may also use and disclose this information as required or authorised by law, including the *My Health Records Act 2012* and *Privacy Act 1988*.

For more information, see the My Health Record System Operator's privacy policy at **digitalhealth.gov.au/privacy**

Authorised officer's declaration

16 **I declare that**:

- I have attached certified copies of relevant documentation to support this application.
- I am duly authorised to legally bind the general supporting organisation legal business entity.
- the information I have provided in this form is complete and correct.

I understand that:

- giving false or misleading information is a serious offence.

Authorised 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

General supporting organisation details

1 Organisation registration number (if known)

2 Organisation name

General supporting organisation's legal person

Your organisation's legal person's name is the name of an individual (for example, trustee or partner), company or other entity that the organisation 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 GSO's legal person

4 GSO'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 general supporting organisation's legal person agrees to be bound by**:

- the attached **National Authentication Service for Health Public Key Infrastructure certificate for supporting organisations 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 Supporting Organisations**.

The general supporting organisation'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 general supporting organisation'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 5)
- 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 5)
- the general supporting organisation's legal person consents to its organisational 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 general supporting organisation's legal person.

Authorised officers' signature

On completion, print and sign by hand.

Date (DD MM YYYY)

Reset form

National Authentication Service for Health Public Key Infrastructure certificate for supporting organisations
Terms and Conditions of Use

Parties:

The Commonwealth as represented by Services Australia.

The general supporting organisation (Supporting Organisation) named in the Application to register a general supporting organisation

1. In consideration for Services Australia issuing the Supporting Organisation with a National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) certificate for Supporting Organisations (Certificate), provided to it on a compact disc (CD) or through electronic means, the Supporting Organisation 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 Supporting Organisations** (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 Supporting Organisation 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 Supporting Organisation's risk
   e) the Supporting Organisation 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 Supporting Organisation 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 Supporting Organisation 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 Supporting Organisation will promptly notify Services Australia in the event that the Supporting Organisation considers that its Certificate has been, or may have been, lost, destroyed, stolen, disclosed, modified or compromised
   i) the Supporting Organisation may request revocation of its Certificate at any time by written notice to Services Australia
   j) the Supporting Organisation'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 Supporting Organisation 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 Supporting Organisation 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 Supporting Organisation has been affected by a malware/virus and their PKI certificate and access to the My Health Record needs to be revoked.
   k) the Supporting Organisation 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 Supporting Organisation's Certificate does not automatically terminate these Terms and Conditions

m) all information the Supporting Organisation provides and representations the Supporting Organisation has made or makes to Services Australia are complete and accurate

n) the Supporting Organisation will promptly notify Services Australia in the event that the Supporting Organisation considers any information provided, or representation made, by it is or may be incorrect, including the Supporting Organisation's contact details

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

p) either Services Australia or the Supporting Organisation 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 Supporting Organisation agrees that it will not use its Certificate after termination of these Terms and Conditions

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

r) the responsibility of Services Australia for any costs, losses or damage the Supporting Organisation (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 Supporting Organisation notice by mail, by fax or electronically. A message sent to the Supporting Organisation's business email address (as held in the records of Services Australia) is one way of giving the Supporting Organisation notice electronically

t) when the Supporting Organisation uses its Certificate after the Supporting Organisation has been notified of a change or addition to these Terms and Conditions, the Supporting Organisation 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 Supporting Organisation.

2. The Supporting Organisation agrees that Services Australia will automatically renew its Certificate on or before its expiry, unless the Supporting Organisation notifies Services Australia 60 business days before then that it does not want its Certificate to be renewed. The Supporting Organisation 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.