Australian Government
Australian Digital Health Agency

Clinical Information System to National Provider Portal (CIS to NPP) Implementation Guide

22 November 2019 v1.0

Awaiting approval for external information

Document ID: DH-2878:2019

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000
Telephone 1300 901 001 or email help@digitalhealth.gov.au
www.digitalhealth.gov.au

Acknowledgements

Council of Australian Governments
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

Document information

Key information

Owner Director, Product Manager My Health Record, Technology Delivery and Projects

Contact for enquiries Australian Digital Health Agency Help Centre
Phone 1300 901 001
Email help@digitalhealth.gov.au

Product or document version history

Product or document version	Date	Release comments
1.0	22 November 2019	Initial release

Table of contents

1 Introduction

1.1 Purpose

This document seeks to assist software vendors with implementing the Clinical Information System to National Provider Portal (CIS to NPP) interface implementation.

1.2 Intended audience

This document is intended for business analysts, developers and solution architects.

1.3 Scope

This document is limited to discussing the CIS to NPP solution. It does not cover in detail the NPP user interface. The following link can be used to see a Provider Portal Demonstration.

1.4 Overview

The NPP is a web portal that allows provider-only access to a consumer's My Health Record. It is important to understand that this portal has a small number of features that are not available in the patient access portal. The most notable feature is the immediate access to uploaded pathology and diagnostic imaging reports, where the consumer portal introduces a 7-day delay.

Before the introduction of this CIS to NPP solution, the only method of accessing the NPP was either via a PRODA account or with an individual NASH certificate embedded into a USB device. In both cases the provider was then required to manually enter the consumer's Medicare number, DVA number or IHI number plus family name, date of birth and gender to access that individual's My Health Record.

The new CIS to NPP solution improves on the above methods by allowing a clinical information system to use an organisation's HPI-O NASH certificate and providing the ability for the CIS to pass the patient's context to the NPP via a JSON Web Token. This allows a single HPI-O certificate to be used by many providers within a single CIS and eliminates the risk of transcription errors while saving the provider's time by avoiding the need to type in the consumer's details.

Furthermore, for software vendors, the CIS to NPP interface provides a relatively simple solution that will enable My Health Record viewing within their product. Being a web-based portal, this approach will provide an evolving and up-to-date My Health Record viewing experience to its customers. Vendors seeking the advanced features of the My Health Record system such as uploading clinical content and pulling down atomic clinical data in line with in their own applications are still advised to integrate with the My Health Record Business to Business (B2B) interfaces, which provide the full capabilities of the My Health Record system.

2 Registering to develop a CIS to NPP implementation

Before developing your implementation, you will first need to register for access to the My Health Record. This process will then provide you with the artefacts you require to begin development such as digital test certificates and test patients and providers.

The necessary steps are listed below:

1. Go to https://developer.digitalhealth.gov.au/resources/faqs/my-health-record-software- vendor-support-page
2. Download a '*Software Vendor Welcome Pack*'.
3. Read the document '*Guide to the My Health Record system connection process*' found in the Welcome Pack.
4. Fill in and return the '*Vendor Product Details Form*', found in the Welcome Pack and return to otsliaison@humanservices.gov.au
5. Apply for NASH PKI Test Kit to get test NASH digital certificates by requesting the form '*Application to request a National Authentication Service for Health Public Key Infrastructure Test Certificate kit*' from otsliaison@humanservices.gov.au, as explained on the NASH PKI test kit page
6. Contact the otsliaison@humanservices.gov.au and ask to have your test provider's HPI-I linked to your test organisation's HPI-O. They will require both the HPI-I and HPI-O numbers.
7. Obtain your NASH digital certificates in the NASH PKI Test Kit. You will also be provided test data and Notice of Connection (NOC) test cases.
8. Start developing and testing your CIS to NPP software implementation.
9. Finalise CIS to NPP implementation development and testing.
10. Contact MyHealthRecord.SVT@accenture.com and request to be booked in to perform your observed NOC testing.
11. Complete a 'Conformance Vendor Declaration Form' and email to myhealthrecord.operations@digitalhealth.gov.au
12. You will receive a My Health Record 'Production Access Letter' which finalises the implementation.

Upon completion of the above process you can now deliver the solution to a customer.

3 CIS to NPP solution overview

The CIS to NPP interface allows a CIS to launch a My Health Record NPP session for a patient within the CIS application. The high-level steps and prerequisites for this to take place are as follows:

1. **Obtain a HPI-O organisation identifier and NASH certificate**

   Obtain a HPI-O organisation identifier and NASH certificate to authenticate the healthcare organisation's connection to the My Health Record system for NPP access.

2 **Link the provider's HPI-I to a HPI-O**

   Link the providers who will use the NPP. Each individual's HPI-I identifier must be pre-linked to the HPI-O identifier used for authenticating the connection. This link is within the HI Service and can be achieved through PRODA management of the HPI-O.

3 **CIS software creates and signs a JSON Web Token (JWT)**

   The creation and signing, by the CIS software, of a JSON Web Token (JWT) containing the patient's core demographics, the providers HPI-I, and the organisations HPI-O and more.

4 **Mutually authenticated HTTP REST POST call**

   The HTTP REST POST call providing the JWT to the NPP must be Mutually Authenticated using the healthcare organisation's (HPI-O's) NASH certificate.

5 **Launch the NPP in a web browser**

   If the response's HTTP status is '200 OK' then a web browser, which can be either the system web browser or an embedded web component within the CIS application, can be used to display the NPP HTML content returned in the response body.

6 **Displaying any response errors to the user**

   If the response's HTTP status is not '200 OK', then a JSON object is returned in the response body and the error message within MUST be displayed to the user.

3.1 Obtain a HPI-O organisation identifier and NASH certificate

A HPI-O is a 16-digit health identifier that uniquely identifies a healthcare organisation. After registering for a HPI-O you can also request a NASH PKI certificate. Each CIS to NPP implementation will require at least one HPI-O identifier and its NASH certificate.

For more information on how to obtain a HPI-O and NASH certificate please see the section '*Register your organisation for a Healthcare Provider Identifier – Organisation (HPI-O) and with the My Health Record system*' at the following link: Register your organisation

3.2 Link provider's HPI-Is to a HPI-O

Each provider that wishes to access the NPP will first require their HPI-I to be linked to the HPI-O used by the NPP implementation. A HPI-I is a 16-digit health identifier that uniquely identifies a healthcare professional individual.

For more information about how to obtain a HPI-I please see the section '*Steps for Healthcare Provider Individuals to obtain a Healthcare Provider Identifier – Individual (HPI-I)*' at the following link: Register your organisation

For more information about linking your HPI-I to your organisations HPI-O please see either of the following section at the link: Access My Health Record using the Provider Portal

- *'I am a healthcare professional who works for myself and I want to set up access to the NPP via PRODA'*
- *'I am a healthcare organisation manager, administrator or similar setting up access for the organisation's healthcare professionals'*

3.3 CIS software creates and signs a JSON Web Token (JWT)

The data required to start a new NPP session is primarily passed within a signed JSON Web Token (JWT). The token contains, among other technical properties, the HPI-O of the organisation which the provider is connecting under and the providers HPI-I and the patient core demographics such as a Medicare number or DVA number or IHI number and their family name, date of birth and gender, at a minimum.

The full technical details for the JWT are specified in section '*3.4.2 Message Body (JWT)*' in the document: *CIS to NPP – Technical Service Specification v1.0.*

3.4 Mutually authenticated HTTP REST POST call

The CIS software must make a mutually authenticated HTTP POST call to the 'CIS to NPP' endpoint providing some defined http headers and the JWT.

The full technical details for HTTP POST request and JWT is specified in section '*3.4.2 Message Body (JWT)*' in the document: *CIS to NPP – Technical Service Specification v1.0.*

For more information about mutual authentication please see the following links:

- The magic of TLS, X509 and mutual authentication explained
- Certificates | Postman Learning Center

3.5 Launch the NPP in a web browser

If the POST request's response has a status of '200 OK' then the body of the response will be a HTML form that submits when loaded into a web browser. This can be loaded into either a system web browser or a web browser component with the CIS software application.

Example '200 OK' response body

```
<HTML>
  <BODY onload="document.forms[0].submit();">
    <FORM METHOD="POST" ACTION="https://myrecord.ehealthvendortest.health.gov.au/oam/server/fed/sp/sso">
      <INPUT TYPE="hidden" NAME="SAMLResponse" VALUE="[SAML token removed for example]"/>
    </FORM>
  </BODY>
</HTML>
```

3.6 Displaying any response errors to the user

If the POST request's response has a status that is not '200 OK' then the body of the response will be a JSON object with a 'message' property which must have its intent communicated to the CIS user.

Example non '200 OK' response body

```
{
  "code" : "400 Bad Request",
  "severity" : "error",
  "message" : "The request includes an invalid sex."
}
```

4 Conformance

4.1 Conformance requirements

There are several conformance requirements that must be adhered to when implementing and developing the CIS to NPP solution. When you finalise the solution and sign off a Conformance Compliance Declaration (CCD) form, it is these conformance requirements that you are declaring conformant too.

The conformance requirements can be found in the document:

CIS to NPP Conformance Profile v1.0.

4.2 Use cases & test cases

The Agency provides a set of use cases which are linked to a limited set of test cases that exercise the conformance requirements. Please be aware that these test cases are separate from the Notice of Connection (NOC) test cases.

These are given to assist vendors in validating that their implementation aligns with the conformance requirements. They are not considered a comprehensive set for a given implementation. Vendors are advised to create and enhance their own wide-ranging set of use cases and test cases with the set provided by the Agency.

The three use cases provided are:

Use Cases No.	Short Description	Long Description
UC.CIStoNPP.001	Using a system browser	An authorised user of a Clinical Information System (CIS) accessing My Health Record (MHR) from National Provider Portal (NPP) within their own CIS using system browsers.
UC.CIStoNPP.002	Using an embedded web-browser component	An authorised user of a Clinical Information System (CIS) accessing My Health Record (MHR) from National Provider Portal (NPP) within their own CIS using web-browsers component.
UC.CIStoNPP.003	User configuration	Clinical Information System (CIS) to National Provider Portal (NPP) user configuration of vendor's CIS.

In summary, all vendors will need to perform the '*User configuration*' use case and then one of either '*Using a system browser*' or '*Using an embedded web-browser component*', depending on their implementation approach towards browser use.

The use cases are documented in both the Conformance Requirement document and found again with the test cases which are located in the spreadsheet titled: Test Cases.

Acronyms

Acronym	Description
B2B	Business to Business
CIS	Clinical Information System
HPI-I	Healthcare Provider Identifier – Individual
HPI-O	Healthcare Provider Identifier – Organisation
IHI	Individual Healthcare Identifier
JSON	JavaScript Object Notation
JWT	JSON Web Token
MHR	My Health Record
NASH	National Authentication Service for Health
NPP	National Provider Portal
PRODA	Provider Digital Access
RAC	Record Access Code