nehta

**HIPS Production Release 4.1.0
Initial and Clean Installation Guide**

14 February 2014

Approved for external use

National E-Health Transition Authority

Document Information

Key Information

Owner   Head of Strategy, Architecture and Informatics

Contact for enquiries   NEHTA Help Centre

t: 1300 901 001

e: help@nehta.gov.au

Document Version History

Version	Date	Release comments
4.1.0	14/2/2014	Release 4.1.0

Table of Contents

1. Important information

It is important to note that this installation document has been written as an installation guide for both a testing or production environment. The scripts and configuration files have been provided for both SVT (software vendor testing) and production environments.

Even though HIPS has been CCA tested and has NOC (Notice of Connection) to the PCEHR and the HI Service at Medicare for production there are still CCA and NOC requirements for the local CIS (Clinical information System) and other items (if being used in your location) not already CCA passed that would be need to be performed by the implementer before being able to connect the entire system to the production PCEHR.

1.1 System Environments

This installation guide is targeted at the production environment ("PROD"). A profile of this installation guide should be created for each system environment that is to be created. Suggested values for each environment are given below:

Environment	Database Name	App Site
Production	PcehrDataStoreProd	HIPS_PROD
Pre-Production	PcehrDataStorePreProd	HIPS_PREPROD
System Test	PcehrDataStoreTest	HIPS_SYSTEST
Development	PcehrDataStoreDvlp	HIPS_DEV

2. Purpose

The purpose of this document is to provide an installation guide, for the 4.1 Release of the Healthcare Identifier and PCEHR Solution (HIPS).

2.1 Background

HIPS is a communications solution to enable Patient Administration Systems and Clinical Information Systems to interact with the National eHealth Record System.

The solution can interface with the Enterprise Service Bus (ESB) / Health Integration Broker (HIB) to receive HL7 records from the PAS systems for patient and episode information and IHI lookups, and CDA documents from the clinical systems for upload to PCEHR. The solution can also be used as a broker to the PCEHR without the need of an interface to an ESB/HIB for upload and retrieval of documents from the PCEHR.

The HIPS 4.1 Release has been through system testing, performance testing, NEHTA Conformance Assessment Process (CAP) and also has NOC approval for the HI Service at Medicare and the PCEHR.

3. Prerequisites

This section outlines the major prerequisites that receiving jurisdictions will need to obtain before implementing HIPS in either a test or production environment.

3.1 Registration to HI Service Vendor Environment

HIPS has passed Healthcare Identifiers CCA and NOC testing, and gained access to the production environment of the HI Service, however for CCA testing of the integrated CIS, you will need to arrange access to the test environment.

To do so, the implementer will need to apply to Department of Human Services (DHS) for a Medicare Location Test Certificate that gives access to the HI Service Vendor Environment.

The following registration details must be used in production:

- Vendor ID: HIPS0001

- Product Name: NEHTA HIPS

- Product Version: 4.1

3.2 Registration to PCEHR SVT Environment

In order to test any PCEHR features, the implementer will need to apply to DHS for a NASH HPI-O Test Certificate that gives access to the PCEHR Software Vendor Testing (SVT) Environment.

The following registration details must be used in production:

- Vendor: NEHTA

- Product Name: NEHTA HIPS

- Product Version: 4.1

3.3 Application Server Operating Environment

To install the HIPS application server, the implementer may:

- Install on an existing workstation or notebook computer with a Windows 7 operating system. This setup is suitable for evaluation only.

- Install on a provisioned Windows Server 2008 R2 operating environment with Internet Information Services (IIS) 7.5 and Microsoft .NET Framework 4.0 installed.

3.4   Database Operating Environment

To install the PCEHR Data Store database, the implementer may:

- Use available capacity on an existing Microsoft SQL Server 2008 R2 database server. This setup is suitable for development and testing environments, but may have insufficient capacity for the production environment.

- Install Microsoft SQL Server 2008 R2 onto the same operating environment as the application server. This setup is suitable for development and testing environments, but may have insufficient capacity for the production environment.

- Provision a separate Windows Server 2008 R2 operating environment and install Microsoft SQL Server 2008 R2. This setup is preferable for the production environment.

4. Database Preparation

4.1 Install SQL Server 2008 R2

If not already installed, install SQL Server 2008 R2 on the database server.

1. For greater performance the tempdb should be installed on a different partition to the data files. Size the tempdb to 5GB as the application will need enough processing space for performance reasons.

4.2 Create the PCEHR Data Store Database

1. On the database server create a new database called PcehrDataStoreProd with the following settings:

2. Add a new Filegroup (in the Filegroups tab) called INDEXES (leave the PRIMARY as the default).

3. For the database files (these are recommended minimum sizes):

   a. For greater performance it is recommended that the Rows Data, Log Data and Index Data should be located on different disk partitions or SAN LUNs.

   b. The initial PcehrDataStoreProd (Rows Data) with PRIMARY file group requires an initial size of 1024MB, with an auto growth of 250MB and unrestricted file growth.

   c. The initial PcehrDataStoreProd_log (Log) requires an initial size of 500MB, with an auto growth of 10% and unrestricted file growth.

   d. A new database file is required and is to be named PcehrDataStoreProd_Index (Rows Data) with the INDEXES file group and requires an initial size of 500MB, with an auto growth of 250MB and unrestricted file growth.

4.3 HIPS Active Directory Service Account Access

HIPS uses Active Directory to secure its internal connections and it is recommended that an AD service account is used (one that does not expire and will not lock). This will be called the "HIPS AD Service account user" for the remainder of the document.

1. Add the HIPS AD Service account user to the SQL Server and assign it db_reader and db_writer to the new PcehrDataStoreProd database.

4.4 Configure and execute the PCEHR Data Store Scripts

1. In the folder "\database\HIPS.PcehrDataStore\scripts" with the supplied binaries 11 script files.

2. Open the "02_HIPS_Roles.sql" script and replace both the '**HIPS AD Service account user**' with the domain and name of the HIPS AD Service account user (e.g. "HAD\nehtaprodhipssvc").

3. The "08_HIPS_HealthProviderOrganisation-Data.sql" script populates the HealthProviderOrganisation table with information about the HPIO, Organisational name and the HI Service and PCEHR Certificate Serial numbers. This table is used to store references to all the certificates that HIPS will use.

Make the following changes in the script (being mindful of whether you are creating this script for SVT or Production):

    a. Replace the 'HPI-O' text with the HPI-O for the Healthcare Provider Organisation.

    b. Replace the 'OU:Name' text with the name of the Healthcare Provider Organisation.

    c. Replace the 'Hi Cert Serial' text with the serial number from the DHS Site PKI Certificate for the Healthcare Provider Organisation.

    d. Replace the 'PCEHR Cert Serial' text with the serial number from the NASH PKI Certificate for the Healthcare Provider Organisation.

NOTE: It is possible for HIPS to accommodate the use of multiple Health Provider Organisations and certificates. This can be done by creating new insert statements within the script and following the above steps for each Health Provider Organisation. As a implementer will commonly have only one Medicare HI Service Certificate then the serial number for this will be duplicated on each row.

4. The '11_HIPS_HospitalTemplate.sql' script is used as a template to create a single hospital with its mandatory Address record, phone and fax number and link to HospitalCode. If multiple hospitals (facilities) are required then this script can be copied and modified for each facility.

To create a hospital for your group, edit the '11_HIPS_HospitalTemplate.sql' script and replace the following:

    a. "HIPS Hospital": Replace this with the full name of the Hospital/Facility (e.g. Royal Adelaide Hospital).

    b. "HIPS Hospital Description": Replace this with the localised description of the Hospital/Facility, which can be either a long or short name (e.g. RAH)

    c. "Authorised Employee Name": Replace this with the name of the person who within your group has the authority to make calls to the PCEHR. This is not specified by the PCEHR access, however it will be added to the audit records on the PCEHR that are visible to the System Operator and NIO (National Infrastructure Operator) of the PCEHR. For example, this may be the CIO of your organisation.

    d. Replace the values of the [AddressLine1], [AddressLine2], [PlaceName], [AustralianStateId], [Postcode] with the address of the facility. NOTE that the AddressLine2 and PlaceName are not required values and may be set to NULL.

    e. Replace the Contact.Detail main phone number value (as '(08) 8888 6666' in the script) with the main phone number of the Hospital/Facility. This has a [ContactMethodId] of 6 which is the "Work Phone".

    f. Replace the Contact.Detail fax number value (as '(08) 8888 7777 in the script) with the facsimile number of the Hospital/Facility. This has a [ContactMethodId] of 7 which is the "Work Fax".

    g. After editing the Hospital, Address and Contract details they must be linked to the HospitalAddress and HospitalContact table.

        i. HospitalAddress: This is done by editing the HospitalId and AddressId of the HospitalAddress record with the HospitalId from the Hospital record and AddressId from the Address record within the script.

ii. HospitalContact: This is done by editing the HospitalId and ContactId of the HospitalContact record with the HospitalId from the Hospital record and ContactId from the Contact record for both the main phone number and facsimile number within the script.

h. To create HospitalCode relationships edit the '11_HIPS_HospitalTemplate.sql' script and replace '*HOSPITAL-CODE*' with short code for the hospital in question. (e.g. Royal Adelaide Hospital is set as 'RAH') and replace the HospitalId in the HospitalCode record with the Hospital record within the script.

It is a requirement for HIPS, if using the DatabaseLoaderService (for receiving PAS Messages) then the code that represents the hospital in HL7 messages needs to be linked to the hospital in the HospitalCode Table for the CodeSystem with code 'pasFacCd'.

(See the "Technical and Functional Specification v4 for additional details on the DatabaseLoaderService and the values of the 'mrnOid', 'doctorOid' and 'isaacFacCd' for other hospitals)

5. Assisted Registration Visitor Hospitals

   a. If you **ARE** planning to install and use Assisted Registration from the HIPS-UI Web package then it is essential that the "12_HIPS_AssistedRegistration_Data.sql" script is executed **AFTER** the Hospital data and HealthProviderOrganisation has been committed. This script will take the HealthProviderOrganisation HPI-O records and create "Visitor" hospitals from the HPIO(s); this is required when an individual is to be registered with the PCEHR and HIPS does not know whether or not the individual has a current episode in the hospital – hence the term "Visitor".

   b. If you **ARE NOT** planning to install and use Assisted Registration from the HIP-UI package then "12_HIPS_AssistedRegistration_Data.sql" will **NOT** need to be executed.

   c. Note that "12_HIPS_AssistedRegistration_Data.sql" can be executed multiple times if necessary as it will update the relevant records as well as inserting any newer additions.

6. These scripts then need to be executed **in order**:

   a. 01_HIPS_Schema.sql

   b. 02_HIPS_Roles.sql

   c. 03_HIPS_TableScript.sql **** Note this must be run twice due to dependencies within the script**

   d. 04_HIPS_ViewScript.sql **** Note this must be run twice due to dependencies within the script**

   e. 05_HIPS_TriggerScript.sql **** Note this must be run twice due to dependencies within the script**

   f. 06_HIPS_CodeScript.sql **** Note this must be run twice due to dependencies within the script**

   g. 07_HIPS_PermissionScript.sql

   h. 08_HIPS_HealthProviderOrganisation-Data.sql **** (See 4.4-3 above to configure first)**

   i. 09_HIPS_4_1_0_Data_Preload.sql

j. 10_HIPS_Indexes.sql

k. 11_HIPS_HospitalTemplate.sql ** **(See 4.4-4 above to configure first)**

l. 12_HIPS_AssistedRegistration_Data.sql ** **ONLY IF REQUIRED (See 4.4-5 above for more details)**

7. This completes the Database setup.

5. Application Server Operating System Preparation

The following steps are for installation on the assigned HIPS application server on a Windows 2008 R2 Server.

1. Ensure that Microsoft .NET Framework v4.0 is installed

2. Under the Server Manager "Features" enable the following items (as well as any default settings):

   - Message Queuing
     - Message Queuing Services
       - Message Queuing Server
       - Directory Service Integration
       - HTTP Support
   - Windows Process Activation Service
     - Process Model
     - .Net Environment
     - Configuration APIs
   - .Net Framework 3.5.1 Features
     - Net Framework 3.5.1
     - WCF Activation
       - HTTP Activation
       - Non-HTTP Activation
   - Remote Server Administration Tools
     - Role Administration Tools
     - Web Server (IIS) Tools

   NOTE: Restart may be required.

   NOTE: If Message Queuing Services has already been installed on an existing server but Directory Service Integration was not installed then simply checking the Directory Service Integration may not correctly install the service, due to a known issue with MSMQ configuration. Uninstalling Message Queuing Services and reinstalling with Directory Service Integration (and other items as above) has been known to resolve this issue if it occurs.

3. Under the Server Manager "Roles" enable the following items for the Web Server (IIS) (as well as any default settings):

   - Web Server
     - Common HTTP Features
       - Static Content
       - Default Content

Approved for external use   14 February 2014

- ▪ Directory Browsing

- ▪ HTTP Errors

- ▪ HTTP Redirection

- o Application Development

  - ▪ ASP.NET

  - ▪ .Net Extensibility

- o Health and Diagnostics

  - ▪ HTTP Logging

  - ▪ Logging Tools

  - ▪ Request Monitor

  - ▪ Tracing

- o Security

  - ▪ Basic Authentication

  - ▪ Windows Authentication

  - ▪ Client Certificate Mapping Authentication

  - ▪ IIS Client Certificate Mapping Authentication

  - ▪ URL Authorization

  - ▪ Request Filtering

  - ▪ IP and Domain Restrictions

- o Performance

  - ▪ Static Content Compression

  - ▪ Dynamic Content Compression

- • Management Tools

  - o IIS Management Console

  - o IIS Management Scripts and Tools

  - o Management Service

4. Under the Servers Services, ensure that the following items are set to Automatic start up:

   - • Net.Tcp Listener Adapter

   - • Net.Tcp Port Sharing Service

   - • Net.Msmq Listener Adapter

5. Ensure that PowerShell is installed

6. Start PowerShell as Administrator and execute commands:

```
Get-ExecutionPolicy

Set-ExecutionPolicy Unrestricted

Get-ExecutionPolicy
```

Record the initial value, and ensure that the final value is Unrestricted. This will ensure that the unsigned PowerShell scripts used in Section 6 can run. The execution policy can be set back to the original value after the installation scripts have run.

5.1 Prepare HIPS IIS Application Pool Account

The HIPS service will execute using the account set in the IIS Application Pool.

1. On the HIPS Application Server check that the HIPS AD Service account user is added to the local server group **IIS_USRS**.

5.2 Certificate Installation – NASH HPI-O Certificate (PCEHR)

Follow these steps to install the NASH PKI Certificate for Healthcare Provider Organisations that is supplied by DHS for connection to the PCEHR B2B Services.

1. Start the Microsoft Management Console

   a. Start – Run – Type "mmc" – OK.

2. Add the Certificates snap-in to access the Local Machine stores

   a. Navigate to File – Add/Remove Snap-In – Certificates – Add – Computer Account – Next – Finish – OK.

3. Import the HPI-O certificate into the Local Computer, Personal store.

   a. Right-click on the Personal store and select All Tasks – Import from the menu

   b. Click Next and Browse to open the file browser dialog

   c. Select type Personal Information Exchange (*.pfx, *.p12)

   d. Select the fac_sign.p12 file

   e. Enter the password for the certificate.

   f. Ensure that "Place all certificates in the following store" and "Personal" is selected.

   g. Click Next and Finish to complete the task.

   h. If more than one certificate, due to multiple Health Provider Organisations, then repeat steps a-g for each certificate.

4. Set permissions for the PCEHR HPI-O certificate to allow the HIPS application account to access its private key.

   a. Select the Certificates folder under the Personal store for the Local Computer

   b. Right-click on newly imported certificate and select All Tasks – Manage Private Keys from the menu.

c. Click Add, type the name of the HIPS AD Service account user and click OK.

d. Ensure the Allow check boxes are ticked for the Full control and Read rows.

e. Click OK to close the dialog box.

f. If more than one certificate, due to multiple Health Provider Organisations, then repeat steps a-e for each certificate.

5.3 Certificate Installation – DHS Site Certificate (HI Service)

If your integration strategy is to supply pre-validated IHI numbers to HIPS and disable the built-in IHI search / validation functionality, then this step may be skipped. If you are using the DatabaseLoaderService then this is an essential step.

Follow these steps to install the DHS Site PKI Certificate (or DHS HI Network Organisation PKI Certificate) that is supplied by DHS for connection to the HI Service B2B Services.

1. Start the Microsoft Management Console

   a. Start – Run – Type "mmc" – OK.

2. Add the Certificates snap-in to access the Local Machine stores

   a. Navigate to File – Add/Remove Snap-In – Certificates – Add – Computer Account – Next – Finish – OK.

3. Import the certificate into the Local Computer, Personal store.

   a. Right-click on the Personal store and select All Tasks – Import from the menu

   b. Click Next and Browse to open the file browser dialog

   c. Select type Personal Information Exchange (*.pfx, *.p12)

   d. Select the fac_sign.p12 file

   e. Enter the password for the certificate.

   f. Ensure that "Place all certificates in the following store" and "Personal" is selected.

   g. Click Next and Finish to complete the task.

4. Set permissions for the certificate to allow the HIPS application account to access its private key.

   a. Select the Certificates folder under the Personal store for the Local Computer

   b. Right-click on "Location nnn :nnnnnnnnnn" (issued by "Medicare Australia Organisation Certification Authority") and select All Tasks – Manage Private Keys from the menu.

   c. Click Add, type the name of the HIPS AD Service account user and click OK.

   d. Ensure the Allow check boxes are ticked for the Full control and Read rows.

   e. Click OK to close the dialog box.

6. Application Server Site Installation

Copy all the code from the "appServer" folder in the provided package to a suitable location on the application server.

The directory "\appServer\ps scripts" contains the main installation powershell script AppSiteCreateSSL.ps1 and the environment-specific configuration script HIPS_BuildAppSites.ps1.

Open the "HIPS_BuildAppSites.ps1" script and edit as following:

1. The default location for the Application Files is under the "D:\Projects\HIPS_PROD\" directory, this can be changed in **both** the AppSitePath and AppServerPath entires in this script (keeping the 'blank' and 'Build' text).
   It is recommended that the Application Files are not on the same drive as the system drive, however this may depend on the server configuration and will not affect performance.

2. Replace the "Domain\ServiceAccount" (in the ProcessUserName item) with the HIPS AD Service account user.

3. Replace the "ProcessPassword" with the password of the HIPS AD Service account user.

The code will be installed beneath the directory "AppSitePath", which will be created when the powershell scripts are run.

The following table indicate the settings in HIPS_BuildAppSites.sql for the System Testing environment:

Option Name	Suggested Value	Description
-AppSiteName	HIPS_PROD	An IIS site will be created with this name.
-AppSitePath	D:\Projects\HIPS_PROD\blank	The IIS site will be served from this directory, which should be empty.
-AppPoolName	HIPSServerAppPool_PROD	An IIS application pool will be created with this name
-ProcessUserName	*domain\serviceaccount*	HIPS will run under this user account (Note: this is the same account that was given permissions in the SQL database)
-ProcessPassword	*Password within file*	Password for the user account above
-HTTPBinding	50500	The web services will be accessible using HTTP protocol on this port.
-NETTCPBinding	50000	The web services will be accessible using net.tcp protocol on this port.
-HTTPSBinding	50443	The web services will be accessible using HTTPS protocol on this port.
-NETMSMQBinding	Localhost	The service will be using an internal MSMQ service on the local host
-AppServerName	HIPSServer_PROD	An IIS application will be created using this name, within the above site.

Option Name	Suggested Value	Description
-AppServerPath	D:\Projects\HIPS_PROD\Build	The IIS application will be served from this directory, which should contain the svc files, Web.config file and bin directory. The bin directory should contain all the DLL files.
| Out-File	"HIPS_PROD_Creation.log"	The setup process will be logged to a file with this name.

6.1 Removing an earlier HIPS version for a new installation

***If you are installing Release 4.1.0 onto a server running an earlier release and you are NOT performing an upgrade then the existing web site MUST be removed first.**

Follow these steps to remove the old web site and application:

1. From the File Explorer take a backup of the entire site content under "D:\Projects\HIPS_PROD" (or where ever the existing version of HIPS resides) and move it to a safe location.

2. Open IIS Manager and right click on the "HIPS_PROD" (or whatever the existing version of HIPS is named) site

3. Select "Remove" from the context menu and accept the removal.

4. Also within the IIS Manager navigate to the Application Pools and right click the "HIPSServerAppPool_PROD" application pool (or whatever the existing version of the HIPS application pool is named).

5. Select "Remove" from the context menu and accept the removal.

6. Open a command window as an administrator and type in "iisreset".

7. Go back to the File Explorer under "D:\Projects\" and delete the entire "HIPS_PROD" (or where ever the existing version of HIPS resides) directory.

8. This has now cleaned the server ready for the new implementation.

6.2 Installing the new web site and application

Follow these steps to install the new web site and application:

1. Start PowerShell as Administrator

2. Change to the directory containing the build scripts

   ("\appServer\ps scripts")

3. Execute command:

   ```
   ./HIPS_BuildAppSites.ps1
   ```

Check the on-screen output and the log file to ensure that the installation completed successfully.

Test the configuration in IIS Manager by navigating to the IIS Site – Basic Settings – Test Settings. The result should be similar to the figure below. If Authorisation fails then ensure that the account used above has read and write access to the folder and subfolders, where the application is installed (i.e. "D:\Projects\HIPS_PROD\")
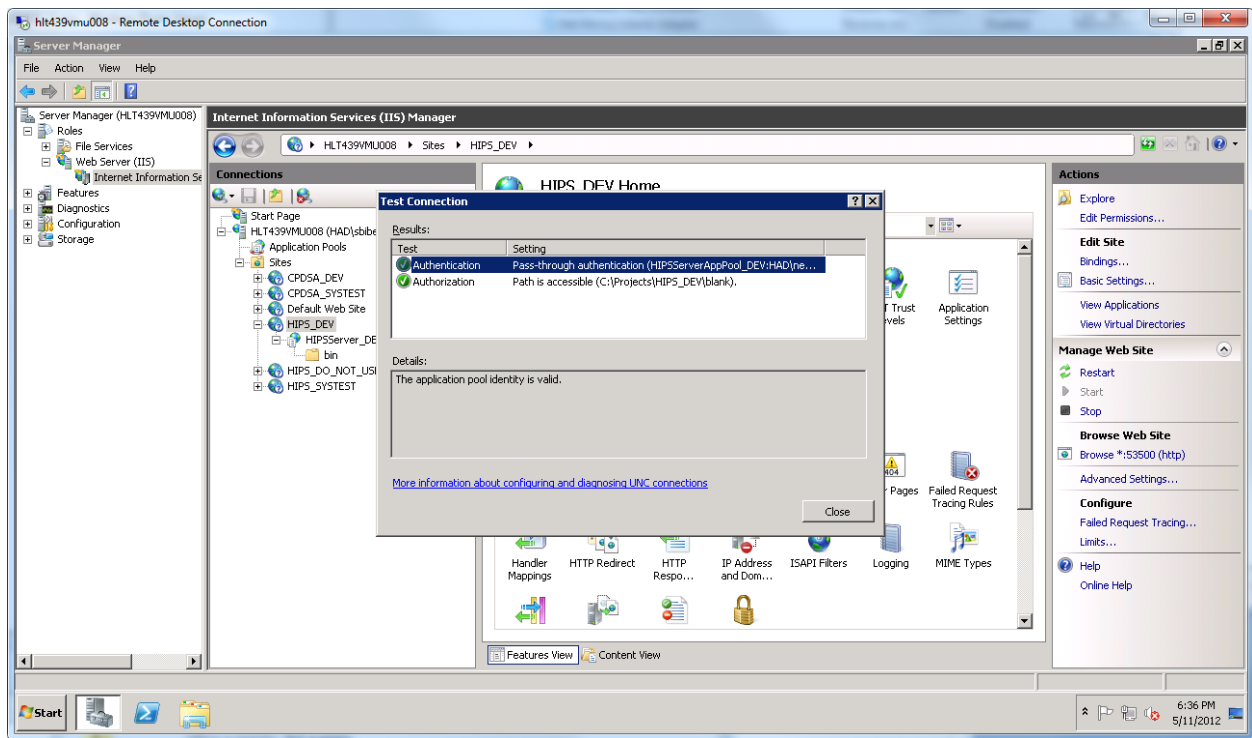
Figure 1 – IIS Connection Test Results

The following must also be applied to the Application Pool HIPSServerAppPool_PROD.

Select the HIPSServerAppPool_PROD application pool and click the "Advanced Settings"

1. Set the "Queue Length" to **2000**

2. Under the "Generate Recycle Event Log Entry" set all sub values to True (as indicated in the image below)

3. Set the "Regular Time Interval (minutes) to **10080**.
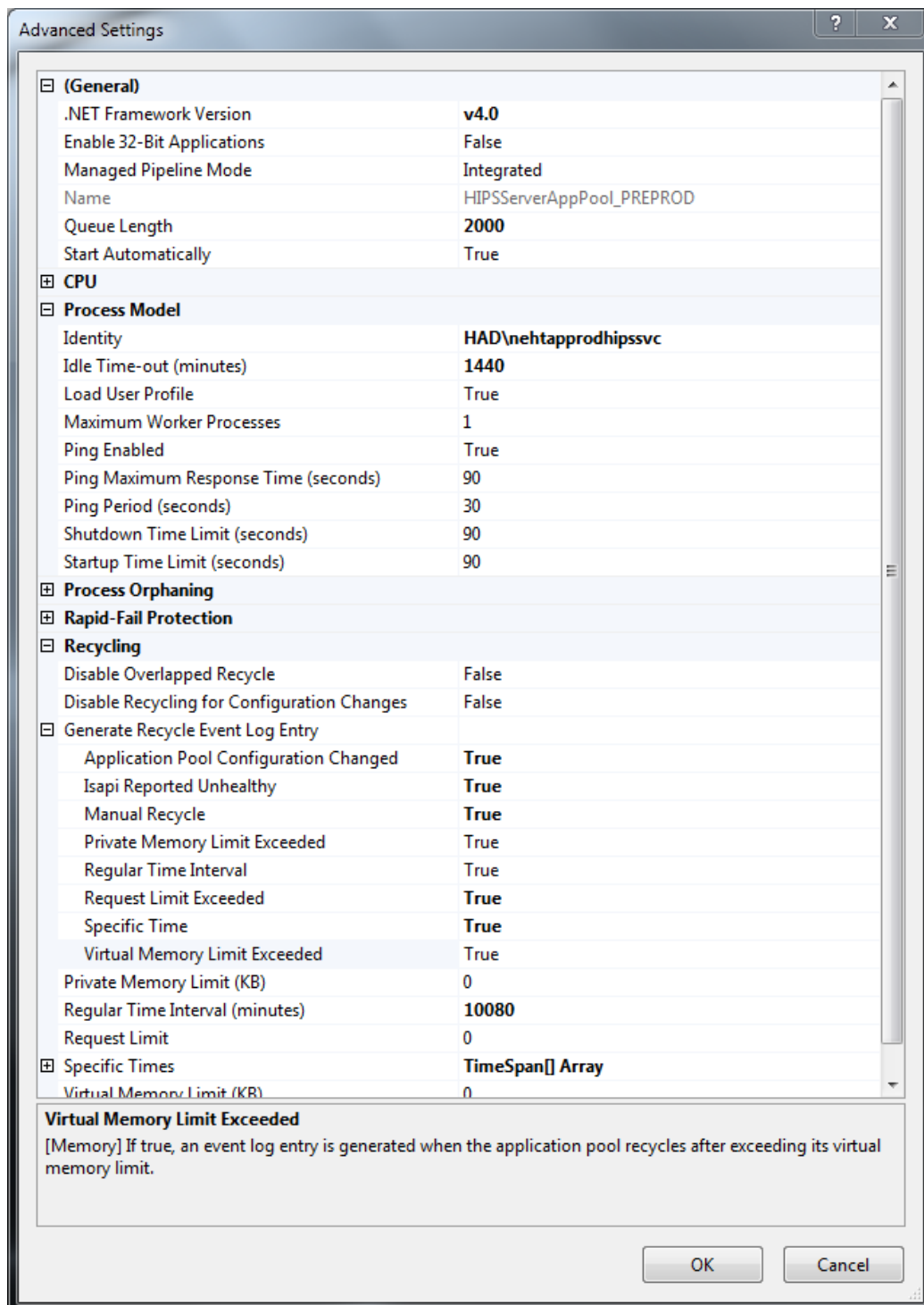
Figure 2 - Application Pool Settings

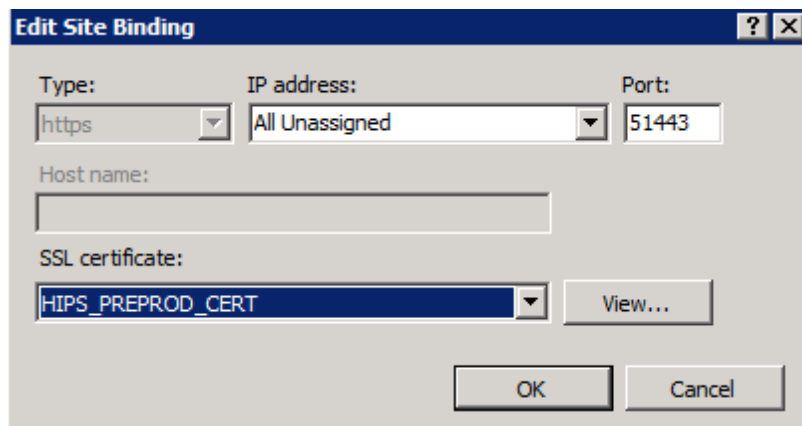# 7. Application Server Self-Signed SSL Certificate

HIPS can be configured to use HTTP or HTTPS connectivity.

A risk assessment of the HIPS solution has resulted in a recommendation that all traffic between HIPS and internal applications should occur using an encrypted connection, i.e. using HTTPS rather than HTTP. However, this is not essential to the connectivity of HIPS, so if your datacentre allows HTTP communications between applications within the datacentre then this is also possible.

While it is possible to use an internal PKI certificate service, or a commercial certificate, a Self-Signed SSL certificate is also considered an acceptable solution for communication between internal applications and HIPS.

A self-signed certificate may be configured via the steps below:

1. Select the main IIS instance of the application server and double click the "Server Certificates" icon.

2. On the far right click the action "Create Self-Signed Certificate…"

3. Specify a friendly name as "HIPS_PROD_CERT" and click OK.

4. To apply the self-signed certificate - Select the "HIPS_PROD" site and in the far right select the "Bindings…" action

5. Select the "https" row from the "Site Bindings" dialog and click "Edit".

6. In the "Edit Site Bindings" dialog, select the "HIPS_PROD_CERT" from the "SSL Certificate" drop down and click OK.

Edit Site Binding		? X
Type:	IP address:	Port:
https	All Unassigned	51443
Host name:		
SSL certificate:		
HIPS_PREPROD_CERT	View...	
	OK	Cancel

7. Close the "Site Bindings" dialog.

8.   HIPS Operation Queue - MSMQ Configuration

The HIPS services for uploading, superseding and removing documents in a PCEHR are implemented using a one-way operation model, also known as fire-and-forget. HIPS uses Microsoft Message Queuing (MSMQ) to guarantee transactional, first-in first-out processing for all document upload and document removal operations.

Follow these steps to create the transactional MSMQ queue for HIPS.

1. On the HIPS Application Server open the "Server Manager" and under "Features" expend "Message Queuing".

2. Right-click Private Queues and select New > Private Queue.

3. Enter the name of the queue as
   "hipsserver_prod/hips.service.pcehrqueue.svc".

   NOTE: if the site name has been modified something other than
   hipsserver_prod then the above must be changed to reflect this and must also be changed within the web.config file.

4. Check the Transactional box, and click OK.

5. Right-click the new Queue item create and select Properties.

   a. In the General Tab - Check the Enabled box in the Journal area

   b. In the Security Tab - Add in the HIPS application account and check Full Control.

   c. Then click OK.

The MSMQ storage folders must allow access to the HIPS application account so that messages can be placed on the private queue

1. Expand "Services and Applications" and then "Message Queuing".

2. Right click on the "Message Queuing" item and select Properties.

3. In the Storage tab identify the Message file folders. The default setting is "<root_drive>:\Windows\System32\msmq\storage".

4. Open Explorer and navigate to the root msmq folder ("<root_drive>:\Windows\System32\msmq\").

5. Right click on the "storage" folder and select Properties.

6. In the Security Tab - Add in the HIPS AD Service account user and check Full Control.

7. The click Ok.

9.   Web Configuration Setup

Provided with the HIPS binaries are 4 web.config files:

1	web.config.svt.http:	**HTTP** web service connectivity into HIPS and for use against the **SVT** environment.
2	web.config.svt.https:	**HTTPS** web service connectivity into HIPS and for use against the **SVT** environment.
3	web.config.prod.http:	**HTTP** web service connectivity into HIPS and for use against the **PROD** environment.
4	web.config.prod.https:	**HTTPS** web service connectivity into HIPS and for use against the **PROD** environment.

These sample configuration files for HIPS specify the use of HTTP Basic Authentication on top of HTTPS because of a specific SA Health integration requirement. The HIPS application server can also be configured to use other authentication methods, including Windows NTLM Authentication or WS-Security authentication, which may be preferable if the calling systems can support these authentication methods, however these alternate configurations are not documented in this guide.

The following instructions can be used for any of the above configuration files.

(See *"APPENDIX A: Application Server Configuration Explanation"* on page 28 for more details on the items in the configuration file)

1. Open the configuration file for editing

2. Replace the "DBServerName" in the connectionString with the name of the Database Server where the HIPS Database will reside.

3. Replace all references of the "AppServerName" to the name of the server where HIPS will be deployed (e.g. HLT111VMA000, also note that if your domain required FQDN then the full domain may also be used, e.g. HLT111VMA000.had.sa.gov.au)

4. In the appSettings change the IhiUserQualifierHiUser to the user qualified domain in the format that is identified by DHS (e.g. for SA Health, http://ns.sahealth.sa.gov.au/id/{0}/userid/1.0; for NT Health, http://ns.health.nt.gov.au/id/{0}/userid/1.0, etc.)

5. In the appSettings change the IhiUserQualifierAuthorisedEmployee to the user identifier supplied for the authorised employee for non-interactive processing (e.g. for SA Health, "http://ns.sahealth.sa.gov.au/id/ae/userid/1.0"; for NT Health, "http://ns.health.nt.gov.au/id/ae/userid/1.0", etc.)

6. In the appSettings change the CdaUserIdQualifierFormat to the user identifier in the CDA signature file for CDA packaging (e.g. for SA Health, "http://ns.sahealth.sa.gov.au/id/cda/userid/1.0/{0}"; for NT Health, "http://ns.health.nt.gov.au/id/cda/userid/1.0/{0}", etc.)

7. In the netMsmqBinding-binding are the following items:
   receiveRetryCount="3" maxRetryCycles="20000"
   retryCycleDelay="00:05:00"
   These are used for when there are connection errors and govern how often HIPS will retry. This has been configured to retry 3 times (between the connection attempt delays) and then wait for 5 minutes before trying again, it will then cycle this 2000 times before the message becomes a poisoned message. This can be altered if required, however, this setting will give a significant amount of time for connection errors to be addressed before the message queue will start skipping messages.

8. The appSetting of AvoidProxy has been set to **true so that outward external connections can bypass the standard proxy**, however, depending on your network and server configuration this may need to be set to **false** so that the outward external connections will use the **policy proxy settings of the HIPS AD Service account user**.

NOTE: The IhiVendorId and PcehrVendorId must remain as "HIPS0001" and "NEHTA" respectively as these are the items that have been registered in the Notices of Connection (NOC) for the use of HIPS.

10. Application Server Code Installation

From the "appServer" folder that was copied to the application server:

1. Ensure that the web.config that was used in the above step is renamed to simply "web.config".

2. Copy all *.svc and *.dll files and directories under the "appServer\binaries" folder into the "D:\Projects\HIPS_PROD\Build\" directory (or to your customised directory location) on the application server. Ensure that the modified web.config file is placed with the *.svc files as below
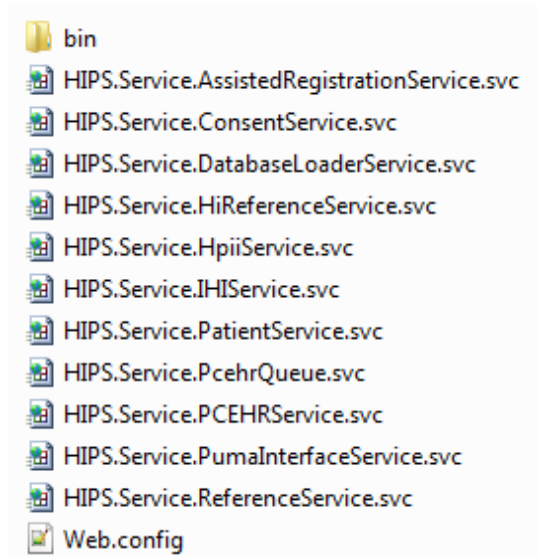
3. Note that there are 36 dll files under the "bin" folder and 11 svc files

**At this time it is reasonable to perform an iisreset while logged into a command prompt as an Administrator.

11. Confirm Installation

11.1 Confirm Available Web Services

In a web browser, navigate to the following URLs and check that the page "You have created a service" appears:

For HTTP

- http://servername:50500/HIPSServer_PROD/HIPS.Service.AssistedRegistrationService.svc

- http://servername:50500/HIPSServer_PROD/HIPS.Service.ConsentService.svc

- http://servername:50500/HIPSServer_PROD/HIPS.Service.DatabaseLoaderService.svc

- http://servername:50500/HIPSServer_PROD/HIPS.Service.HiReferenceService.svc

- http://servername:50500/HIPSServer_PROD/HIPS.Service.HpiiService.svc

- http://servername:50500/HIPSServer_PROD/HIPS.Service.IHIService.svc

- http://servername:50500/HIPSServer_PROD/HIPS.Service.PatientService.svc

- http://servername:50500/HIPSServer_PROD/HIPS.Service.PcehrQueue.svc

- http://servername:50500/HIPSServer_PROD/HIPS.Service.PCEHRService.svc

- http://servername:50500/HIPSServer_PROD/HIPS.Service.ReferenceService.svc

For HTTPS (NOTE: FQDN may be required**)**

- https://servername:50443/HIPSServer_PROD/HIPS.Service.AssistedRegistrationService.svc

- https://servername:50443/HIPSServer_PROD/HIPS.Service.ConsentService.svc

- https://servername:50443/HIPSServer_PROD/HIPS.Service.DatabaseLoaderService.svc

- https://servername:50443/HIPSServer_PROD/HIPS.Service.HiReferenceService.svc

- https://servername:50443/HIPSServer_PROD/HIPS.Service.HpiiService.svc

- https://servername:50443/HIPSServer_PROD/HIPS.Service.IHIService.svc

- https://servername:50443/HIPSServer_PROD/HIPS.Service.PatientService.svc

- https://servername:50443/HIPSServer_PROD/HIPS.Service.PcehrQueue.svc

- https://servername:50443/HIPSServer_PROD/HIPS.Service.PCEHRService.svc

- https://servername:50443/HIPSServer_PROD/HIPS.Service.ReferenceService.svc
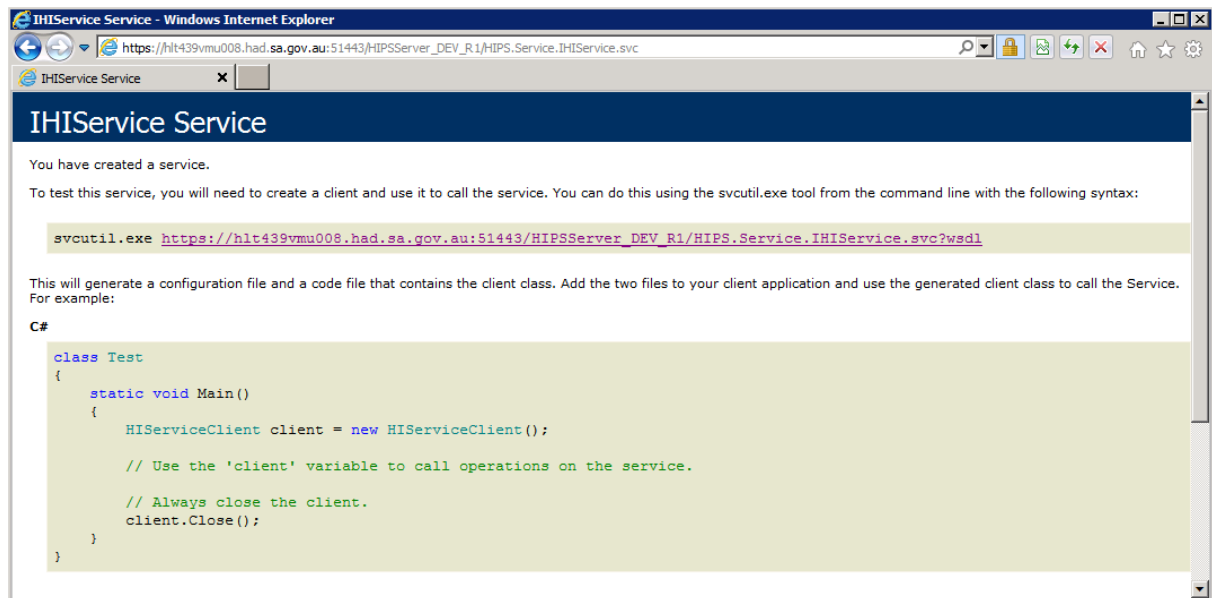
Figure 3 – IIS web service confirmation page

THIS IS THE COMPLETION OF THE INSTALLATION OF HIPS

12.   Demo Harness

Provided with the HIPS binaries is the HIPS Demo Harness.

Please see the "HIPS Release 4.1.0 - Evaluation Guide v4.1.0.docx" for more detailed information.

Provided with the HIPS Demo Harness are two configuration files in the "Config" directory. One is for use against an HTTPS installation of HIPS and one is for an HTTP installation of HIPS.

Either one of these files can be used to replace the contents of the "HIPS.DemoHarness.exe.config" which is in the root folder of the "Demo Harness Application". The "HIPS Demo Harness Configuration" steps can be followed from the "HIPS Release 4.1.0 - Evaluation Guide v4.1.0.docx" to configure the Demo Harness to connect to your HIPS installation.

13. APPENDIX A: Application Server Configuration Explanation

The Web.Config should be pre-configured for each release, however this is a detailed explanation of the contents for configurators.

Most application-wide configuration options are held in the Web.config file in the directory D:\Projects\HIPS_PROD\Build\".

Section	Option Name	Suggested Value	Description
Connection String	Data Source	*Name of SQL server*	HIPS will attempt to connect to this SQL server.
	Initial Catalog	PcehrDataStoreProd	HIPS will use the database with this name.
	Integrated Security	SSPI	If set to SSPI as recommended then HIPS will use the IIS application pool's Windows account credentials for authentication to the database. Otherwise, and this is not recommended, set to false and provide a User ID and Password. This will only work if SQL Server Authentication is enabled on the server.
Consent Service	baseAddress	net.tcp://servername:**50000**/	The Consent service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername:**50500**/ConsentService/	The Consent service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername:**50443**/ConsentService/	The Consent service will be accessible using HTTPS protocol at this URL.
Database Loader Service	baseAddress	net.tcp://servername:**50000**/	The Database Loader service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername:**50500**/DatabaseLoaderService/	The Database Loader service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername:**50443**/DatabaseLoaderService/	The Database Loader service will be accessible using HTTPS protocol at this URL.
IHI Service	baseAddress	net.tcp://servername:**50000**/	The IHI services will be accessible using net.tcp protocol at this URL.

Section	Option Name	Suggested Value	Description
	baseAddress	http://servername:**50500**/IHIService/	The IHI services will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername:**50443**/IHIService/	The IHI services will be accessible using HTTPS protocol at this URL.
Pcehr Queue Service	baseAddress	net.tcp://servername:**50000**/	The Pcehr Queue services will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername:**50500**/PcehrQueueService/	The Pcehr Queue services will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername:**50443**/PcehrQueueService/	The Pcehr Queue services will be accessible using HTTPS protocol at this URL.
PCEHR Service	baseAddress	net.tcp://servername:**50000**/	The PCEHR services will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername:**50500**/PCEHRService/	The PCEHR services will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername:**50443**/PCEHRService/	The PCEHR services will be accessible using HTTPS protocol at this URL.
Reference Service	baseAddress	net.tcp://servername:**50000**/	The Reference service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername:**50500**/ReferenceService/	The Reference service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername:**50443**/ReferenceService/	The Reference service will be accessible using HTTPS protocol at this URL.
Assisted Registration Service	baseAddress	net.tcp://servername:**50000**/	The Reference service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername:**50500**/AssistedRegistrationService/	The Reference service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername:**50443**/AssistedRegistrationService/	The Reference service will be accessible using HTTPS protocol at this URL.

Section	Option Name	Suggested Value	Description
Hpii Service	baseAddress	net.tcp://servername:**50000**/	The Reference service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername:**50500**/HpiiService/	The Reference service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername:**50443**/HpiiService/	The Reference service will be accessible using HTTPS protocol at this URL.
Hi Reference Service	baseAddress	net.tcp://servername:**50000**/	The Reference service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername:**50500**/HiReferenceService/	The Reference service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername:**50443**/HiReferenceService/	The Reference service will be accessible using HTTPS protocol at this URL.
Patient Service	baseAddress	net.tcp://servername:**50000**/	The Reference service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername:**50500**/PatientService/	The Reference service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername:**50443**/PatientService/	The Reference service will be accessible using HTTPS protocol at this URL.
MSMQ Client Endpoint	address	net.msmq://localhost/private/HIPSServer_PROD/HIPS.Service.PcehrQueue.svc	The address for the local MSMQ service
App Settings	IhiProductName	NEHTA HIPS	Product Name registered with DHS
	IhiProductVersion	4.1	Product Version registered with DHS
	IhiVendorId	HIPS0001	Vendor ID registered with DHS
	IhiVendorQualifier	http://ns.electronichealth.net.au/id/hi/vendorid/1.0	This URL qualifies the vendor ID in the header of each request to the HI Service. This is a fixed value defined by DHS technical specifications.
	IhiUserQualifierProviderIndividual	http://ns.electronichealth.net.au/id/hi/vendorid/1.0	

Approved for external use   14 February 2014

Section	Option Name	Suggested Value	Description
	IhiUserQualifierHiUser	http://ns.*healthdomain*.*stateorterritory*.gov.au/id/{0}/userid/1.0	This URL qualifies the domain in which the interactive user's login is identified to DHS, with {0} replaced by the supplied domain,
	IhiUserQualifierAuthorisedEmployee	http://ns.*healthdomain*.*stateorterritory*.gov.au/id/ae/userid/1.0	This URL qualifies the user identifier supplied for the authorised employee for non-interactive processing.
	IhiHpioQualifier	http://ns.electronichealth.net.au/id/hi/hpio/1.0	This URL qualifies an HPI-O in the header of a request to HI Service, but is only used for Contracted Service Providers (CSP) and not if the health provider organisation itself makes the call. This is a fixed value defined by DHS technical specifications.
	IhiValidationPeriodDays	1	HIPS will revalidate an IHI before returning it to the calling system or using it in a call to the PCEHR, if it was not obtained or last validated within the number of days specified here. For implementers that do not connect HIPS to the HI Service, it is necessary to set this to a large number (e.g. 999) to prevent HIPS attempting revalidation.
	HiServiceUrl	Vendor Environment: https://www5.medicareaustralia.gov.au/cert/soap/services/ Production Environment: https://www3.medicareaustralia.gov.au/pcert/soap/services/	HIPS will connect to the HI Service at this URL, which is that of the HI Service vendor or production environment.
	PcehrProductName	NEHTA HIPS	Product Name registered with PCEHR SVT
	PcehrProductVersion	4.1	Product Version registered with PCEHR SVT
	PcehrVendorId	NEHTA	Vendor ID registered with PCEHR SVT
	PcehrRole	CIS	HIPS is designed to communicate with PCEHR B2B Gateway as part of a Clinical Information System (CIS).
	CheckDoesPcehrExist	true	Whether HIPS should check the PCEHR advertised status of each patient immediately upon obtaining his/her IHI.

Section	Option Name	Suggested Value	Description
	CdaUserIdQualifierFormat	http://ns.*healthdomain*.*stateterritory*.gov.au/id/cda/userid/1.0/{0}	This URL qualifies the user identifier in the CDA signature file for CDA packaging. Replace healthdomain and stateterritory. The {0} will be replaced with the author's identifier from the CDA document.
	IhiCleanupProcessMinutes	60	Interval to wake up background thread and process service error IHI calls.
	LookupRefreshSeconds	600	This is the waiting time between cached data refreshes in seconds.
	PumaEnabled	False	PUMA not required within HIPS
	AvoidProxy	True	Avoid standard Proxies
	DoesPCEHRExistUrl	https://b2b.ehealthvendortest.health.gov.au/doesPCEHRExist	HIPS will connect to this URL to check the PCEHR advertised status of an IHI.
	UploadDocumentUrl	https://b2b.ehealthvendortest.health.gov.au/uploadDocument	HIPS will connect to this URL to upload or supersede a document to a PCEHR.
	GetDocumentUrl	https://b2b.ehealthvendortest.health.gov.au/getDocument	HIPS will connect to this URL to download a document from a PCEHR.
	GetViewUrl	https://b2b.ehealthvendortest.health.gov.au/getView	HIPS will connect to this URL to request a view from a PCEHR.
	RemoveDocumentUrl	https://b2b.ehealthvendortest.health.gov.au/removeDocument	HIPS will connect to this URL to remove a document from a PCEHR.
	ListDocumentUrl	https://b2b.ehealthvendortest.health.gov.au/getDocumentList	HIPS will connect to this URL to list documents available to download from a PCEHR.
	GainPCEHRAccessUrl	https://b2b.ehealthvendortest.health.gov.au/gainPCEHRAccess	HIPS will connect to this URL to gain access to a PCEHR.
	RegisterPcehrUrl	https://b2b.ehealthvendortest.health.gov.au/registerPCEHR	HIPS will connect to this URL to register a PCEHR.
	DoesPCEHRExistTimeoutSeconds	120	Connection Timeout (in seconds) for DoesPCEHRExist Service. Defaults to 60 if not included in the configuration file.

Section	Option Name	Suggested Value	Description
	DocumentProductionTimeoutSeconds	300	Connection Timeout (in seconds) for Document Production Services : UploadDocument, RemoveDocument.
			Defaults to 300 if not included in the configuration file.
	DocumentConsumptionTimeoutSeconds	120	Connection Timeout (in seconds) for Document Consumption Services : GetDocument, GetDocumentList, GetChangeHistoryView, GainPCEHRAccess.
			Defaults to 120 if not included in the configuration file.
	IhiSearchTimeoutSeconds	120	Connection Timeout (in seconds) for IHI Search
			Defaults to 60 if not included in the configuration file
	HpiiSearchTimeoutSeconds	120	Connection Timeout (in seconds) for HPII Search
			Defaults to 60 if not included in the configuration file
	BypassHIService	false	**ONLY for Custom Assisted Registration Installations**
			If the HI Service is not to be used for Assisted Registration then this is set to false, when AR Service not configured for HIPS-UI
			This can only be set to true IF the Assisted Registration web service is used outside of the HIPS UI. Note setting this false will mean that HIPS will need to pass Conformance Testing again to use Assisted Registration outside of the HIPS-UI solution of Assisted Registration.