nehta

eHISC v6.0.0

Initial and Clean Installation Guide (Core)

31 May 2016

Approved for external use

National E-Health Transition Authority

National E-Health Transition Authority Ltd

Level 25, 56 Pitt Street

Sydney, NSW 2000

Australia

www.nehta.gov.au

Document information

Key information

Owner   Head of Delivery

Contact for enquiries   NEHTA Help Centre

t: 1300 901 001

e: help@nehta.gov.au

Product version history

Product version	Date	Release comments
1.0	February 2014	Initial release (HIPS 4.1.0).
2.0	February 2015	See release note (NEHTA-2040:2015) for details of changes and bug fixes.
2.0.1 2.0.2		Unpublished updates.
2.0.3	February 2016	See release note (NEHTA-2185:2016) for details of changes and bug fixes.
6.0.0	May 2016	See release note (NEHTA-2263:2016) for details of changes and bug fixes.

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 test or production environment of the eHISC product suite. The scripts and configuration files have been provided for both SVT (software vendor testing) and production environments.

1.1   System Environments

This installation guide is targeted at the system test environment ("SYSTEST"). 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	PROD
Pre-Production	PcehrDataStorePreProd	PREPROD
System Test	PcehrDataStoreTest	SYSTEST
Development	PcehrDataStoreDvlp	DEV

1.2   Global Unique UUID

An instance identifier may be of the UUID form or an object identifier (OID) form. The algorithm for creating a UUID ensures the uniqueness of the identifier whereas the OID form requires the software to have the logic to ensure uniqueness. The CDA documents use the OID option where achieving a unique document identifier relies on the value of the extension attribute being unique within the healthcare provider organisation. Here is an example:

<id extension="**2143**" root="**1.2.36.1.2001.1005.49.1.8003621566687292.2143**" assigningAuthorityName="**HIPS DHSITESTORGD46 Doc**"/>

According to the data types specification "The root and extension scheme means that the concatenation of root and extension shall be a globally unique identifier for the item that this II value identifies".

To ensure global uniqueness across an organisation do not configure the same HPI-O in more than one eHISC Core database.

2. Introduction

eHISC is a communications solution to enable Patient Administration Systems and Clinical Information Systems to interact with the National My Health Record System.

The solution can interface with an Enterprise Service Bus (ESB) or other integration systems to receive HL7 V2 records from the PAS/LIS/RIS systems for patient and episode information and IHI lookups, and CDA documents from the clinical systems for upload to the national digital health record system.

If Mirth Connect is setup and configured then the solution can also accept HL7 V2 messages for Pathology and Diagnostic Imaging report documents. The solution can also be used as a broker to the digital health record system without the need of an interface to an ESB for upload and retrieval of documents from the national digital health record system.

The eHISC Release 6.0.0 has been through system testing, performance testing and NEHTA Conformance Assessment Process (CAP).

2.1 Purpose

The purpose of this document is to provide the technical details and steps required to install the 6.0.0 version of the eHISC product suite.

It can be used by health facilities to install the eHISC product suite into a targeted environment.

This document describes the prerequisites and steps that are required for the eHISC product suite to be installed for the first time (clean installation).

2.2 Scope

This document covers prerequisites required for the targeted environment, the database server preparation and application server operating system preparation. The document will then go on to describe the steps required for the installation of the eHISC on the database server and application server(s).

This document does not describe any functional requirements or features of the eHISC product suite as these are covered by other documentation.

2.3 Assumptions

The following assumptions have been made during the development of this document:

- The user carrying out the installation has server administration access to the targeted database server and application server(s).

- The facility installing the eHISC product suite has appropriate software versions and server operating systems.

2.4   Definitions and Acronyms

Item	Definition
PAS	Patient Administration System
LIS	Laboratory Information System
RIS	Radiology Information System
eHISC	eHealth Integration Sample Code
ESB	Enterprise Service Bus
CAP	Conformance Assessment Process
CIS	Clinical Information System
HPI-O	Health Provider Identifier - Organisation

3. Prerequisites

This section outlines the major prerequisites that an implementer will need to obtain before implementing eHISC in either a test or production environment.

3.1 Registration to HI Service Vendor Test Environment

For CCA testing of the integrated CIS, you will need to arrange access to the test environment. The HI Service Registration Form which is submitted to Medicare as part of the registration process must include the details of the eHISC product which are stored within the application configuration file. These settings are explained further in *Appendix A Application Server Configuration Explanation*.

The Medicare site certificate gives access to the HI Service Vendor Test Environment.

The eHISC compiled binaries need to be registered as a product with the product name, version and vendor details to be able to identify itself to the HI Service. The table below states the HI Service Registration Form Field and what application configuration setting field this should be mapped to.

Field	Description	Application Config Setting
Vendor ID	The registered product Vendor ID	IhiVendorId
Product Name	The registered Product Name	IhiProductName
Product Version	The registered product version number	IhiProductVersion

3.2 Registration to Digital Health Record SVT Environment

In order to test any national digital health record features, the organisation will need to obtain a NASH HPI-O Test Certificate that gives access to the national digital health record Software Vendor Testing (SVT) Environment.

The eHISC compiled binaries need to be registered as a product with the product name, version and vendor details to be able to identify itself to the My Health Record Service. The table below states the My Health Record Service Registration Form Field and what application configuration setting field this should be mapped to. These settings are explained further in *Appendix A Application Server Configuration Explanation*.

Field	Description	Application Config Setting
Vendor	The registered Product Vendor Name	PcehrVendorId
Product Name	The registered Product Name	PcehrProductName
Product Version	The registered product version number	PcehrProductVersion

3.3 Application Server Operating Environment

To install the eHISC application server, the organisation 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 4.5 installed.

3.4   Database Operating Environment

To install the PCEHR Data Store database, the organisation 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.

nehta

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 using the database name suggested in section 1.1 System Environments (example PcehrDataStoreTest) 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 data store rows data (PcehrDataStoreTest) with PRIMARY file group requires an initial size of 1024MB, with an auto growth of 250MB and unrestricted file growth.

   c. The initial Log (PcehrDataStoreTest_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 PcehrDataStoreTest_Index (or appropriate name based on system environment setup) (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   eHISC Active Directory Service Account Access

eHISC 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 "eHISC AD Service account user" for the remainder of the document.

1. Add the eHISC AD Service account user to the SQL Server and assign it db_datareader and db_datawriter to the new PcehrDataStore database.

4.4   Configure and execute the PCEHR Data Store Scripts

1. In the folder "\database\2.0.3_scripts" there is 12 SQL script files.

2. Open the "02_HIPS_Roles.sql" script and replace both the '**eHISC AD Service account user**' with the domain and name of the eHISC AD Service account user

3. The "08_HIPS_HealthProviderOrganisation-Data.sql" script populates the HealthProviderOrganisation table with information about the HPIO, Organisational name and the HI Service and My Health Record Service Certificate Serial numbers. This table is used to store references to all the certificates that eHISC 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 or Contracted Service Provider (CSP). If using a CSP certificate, change the value for 'HiCsp' from 0 to 1.

   d. Replace the 'PCEHR Cert Serial' text with the serial number from the NASH PKI Certificate for the Healthcare Provider Organisation or Supporting Organisation. If using a Supporting Organisation certificate, change the value for 'PcehrCsp' from 0 to 1.

   e. Replace the 'HPO Cert Serial' text with the serial number from the NASH PKI Certificate for the Healthcare Provider Organisation. This certificate is required to create the digital signature when uploading documents.

   NOTE: It is possible for eHISC 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 an organisation 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-eHISC.sql' script is used as a template to create the Laboratory Information System (LIS) or Radiology Information System (RIS) 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 organisation, edit the '11_HIPS_HospitalTemplate-eHISC.sql' script and replace the following:

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

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

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

d.   "ID of Authorised Employee": Replace this with the identifier or username of the person who within your organisation has the authority to make calls to the My Health Record System.

e.   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.

f.   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".

g.   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".

h.   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.

i.   To create HospitalCode relationships replace '*HPI-O*' with the Hospital HPI-O value and '*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 eHISC that the code that represents the hospital (facility) in HL7 messages needs to be linked to the hospital in the HospitalCode Table for the CodeSystem with code 'pasFacCd'. If the Pathology and Diagnostic Imaging functionality is used then a code that represents LIS/RIS needs to be linked to the hospital (facility) in the HospitalCode Table for the CodeSystem with code "patientIdAuthCd".

(See the "eHISC Release 6.0.0 - Module – Core" 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 eHISC-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 My Health Record System and eHISC 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_Reference_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. In the folder "\database\2.0.3_to_6.0.0_Upgrade" and application named "HIPS.PcehrDataStore.DBUpgrade.exe" which will run all necessary scripts to upgrade the database from 2.0.3 to 6.0.0.

8. Open the "HIPS.PcehrDataStore.DBUpgrade.exe.config" and changed the DatabaseConnection property to point to the newly created PcehrDataStore.

9. Open up a command prompt and change the directory to be the directory which contains the HIPS.PcehrDataStore.DBUpgrade.exe application.

10. Run the application. If the script was successful a green 'Success!' notice should be displayed. Any errors will be display in red.

11. If the PDI functionality is to be used to upload Pathology or Diagnostic Imaging Reports to the National My Health Record System then the following SQL script should be run to create the RIS/LIS System Code and assign it to each Health Facility created above.

    a. Under the "database\2.0.3_to_6.0.0_Upgrade\ConfigurationScripts" folder open the "01_PDI_HospitalCode-eHISC.sql" file.

    b. Update the *RIS/LIS SYSTEM* text to be the system code that will be contained in the HL7 message PID-3 field, i.e. 'NATA' or 'LSPN8234'.

    c. If more than one Health Facility or Laboratory was added then copy and paste the insert statement for each HospitalId created in Step 6 (k) above.

    d. Execute the script.

12. This completes the Database setup.

5.   Application Server Operating System Preparation

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

1. Ensure that Microsoft .NET Framework v4.5 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
        - Directory Browsing
        - HTTP Errors
        - HTTP Redirection
    - Application Development
        - ASP.NET
        - .Net Extensibility
    - Health and Diagnostics
        - HTTP Logging
        - Logging Tools
        - Request Monitor
        - Tracing
    - Security
        - Basic Authentication
        - Windows Authentication
        - Client Certificate Mapping Authentication
        - IIS Client Certificate Mapping Authentication
        - URL Authorization
        - Request Filtering
        - IP and Domain Restrictions
    - Performance
        - Static Content Compression
        - Dynamic Content Compression
- Management Tools
    - IIS Management Console
    - IIS Management Scripts and Tools
    - Management Service

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

   o Net.Tcp Listener Adapter

   o Net.Tcp Port Sharing Service

   o 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 eHISC IIS Application Pool Account

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

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

5.2   Certificate Installation – NASH HPI-O Certificate (My Health Record System)

Follow these steps to install the NASH PKI Certificate for Healthcare Provider Organisations that is supplied by DHS for connection to the My Health Record 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 My Health Record System HPI-O certificate to allow the eHISC 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 eHISC 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 eHISC 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 eHISC application account to access its private key.

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

   b. Right-click on the imported Medicare Certificate (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 eHISC 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_TEST\" directory, this can be changed in **both** the <u>AppSitePath</u> and <u>AppServerPath</u> 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 eHISC AD Service account user.

3. Replace the "ProcessPassword" with the password of the eHISC 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_TEST	An IIS site will be created with this name.
-AppSitePath	D:\Projects\HIPS_TEST\blank	The IIS site will be served from this directory, which should be empty.
-AppPoolName	HIPSServerAppPool_TEST	An IIS application pool will be created with this name
-ProcessUserName	*domain\serviceaccount*	eHISC 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

Option Name	Suggested Value	Description
-AppServerName	HIPSServer_TEST	An IIS application will be created using this name, within the above site.
-AppServerPath	D:\Projects\HIPS_TEST\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_TEST_Creation.log"	The setup process will be logged to a file with this name.

6.1 Removing an earlier eHISC version for a new installation

***If you are installing Release 6.0.0 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_TEST" (or where ever the existing version of eHISC resides) and move it to a safe location.

2. Open IIS Manager and right click on the "HIPS_TEST" (or whatever the existing version of eHISC 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_TEST" application pool (or whatever the existing version of the eHISC 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_TEST" (or where ever the existing version of eHISC 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_TEST\")
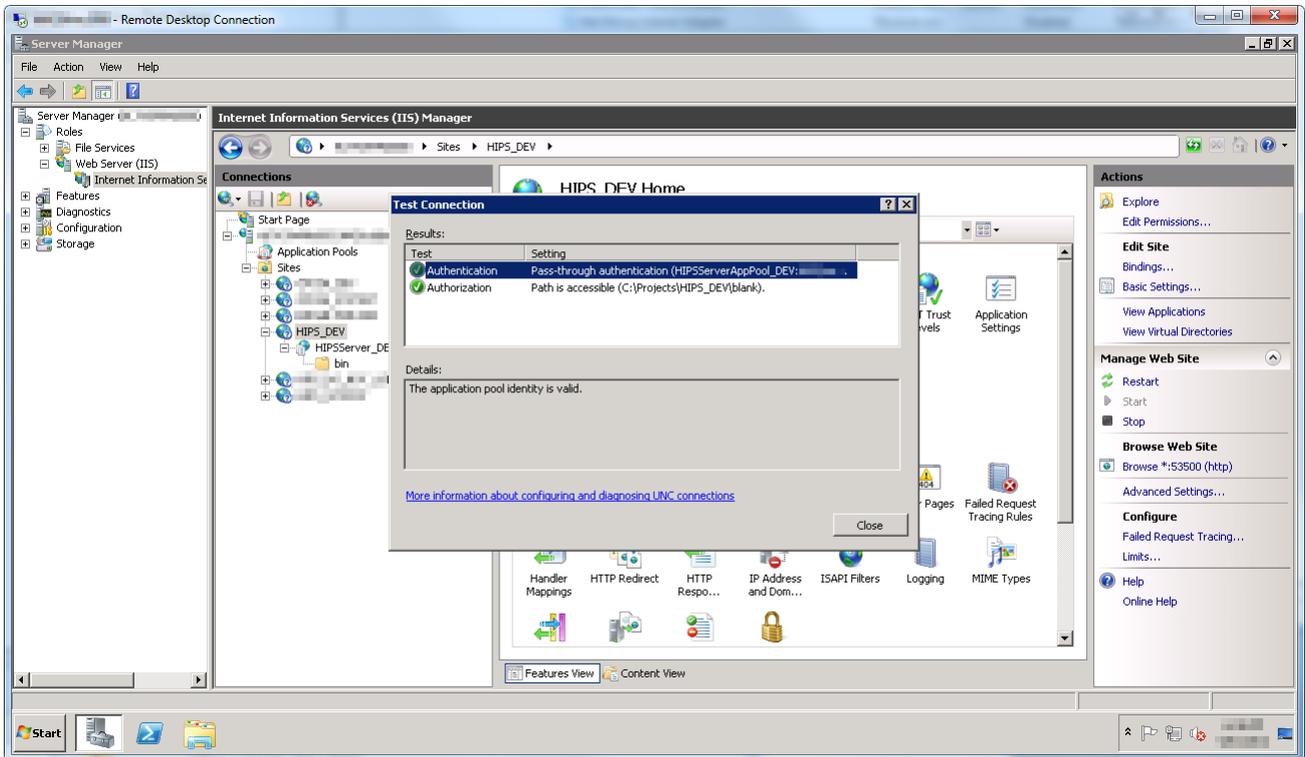
Figure 1 – IIS Connection Test Results

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

Select the HIPSServerAppPool_TEST 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. Check the "Regular Time Interval (minutes) is set to **1740**.
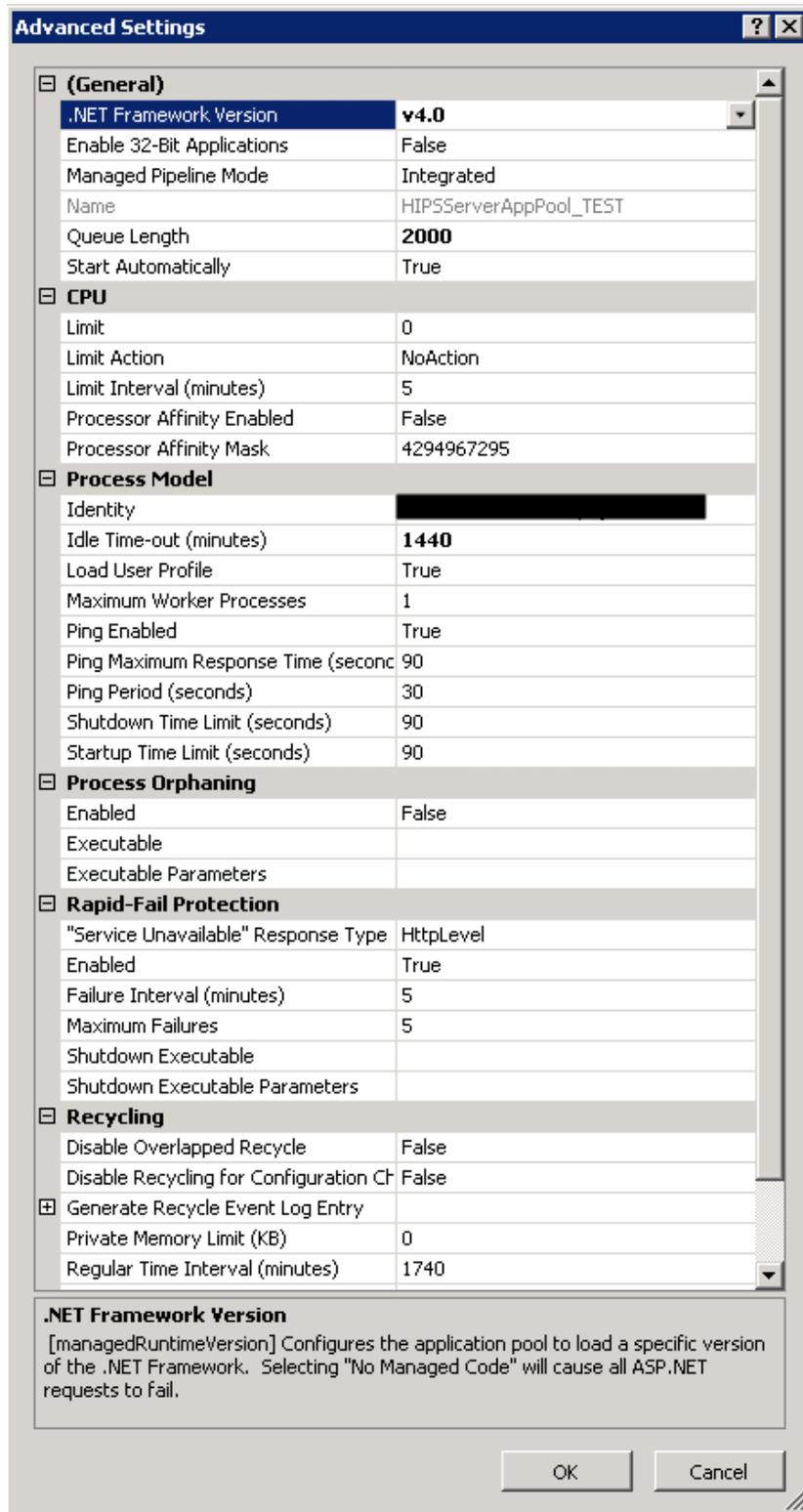
Figure 2 - Application Pool Settings

7.   Application Server Self-Signed SSL Certificate

eHISC can be configured to use HTTP or HTTPS connectivity.

A risk assessment of the eHISC solution has resulted in a recommendation that all traffic between eHISC 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 eHISC, 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 eHISC.

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_TEST_CERT" and click OK.

4. To apply the self-signed certificate - Select the "HIPS_TEST" 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_TEST_CERT" from the "SSL Certificate" drop down and click OK.

7. Close the "Site Bindings" dialog.

8. Mirth Connect Installation and Set Up

Mirth Connect is an optional component that can be set up and used to host the MLLP interfaces that connect to the eHISC SOAP web services to upload Pathology and/or Diagnostic Imaging Reports to the national digital health record system.

Mirth Connect is open-source-software that allows a HL7 message to be sent to Mirth Connect via MLLP from any ESB. The Mirth Connect software will then call the eHISC SOAP web services using the supplied HL7 message.

The configured Mirth Connect channels supplied as part of the release were built using Mirth Connect version 3.3.1 (64-bit).

Set up requirements and the Mirth Connect tool can be downloaded from the Mirth website:

https://www.mirth.com/Products-and-Services/Mirth-Connect#tab_overview

If Mirth Connect is to be implemented to receive the eHISC Acknowledgement, this is the final acknowledgement that eHISC receives from the My Health Record Service when a Pathology or Diagnostic Imaging is uploaded, then an extra setting is required to be updated in the application configuration file. This is described in *Section 10 – Web Configuration Set Up*.

8.1 Channel Installation

To install the channels required for the Pathology and Diagnostic Imaging Report uploads:

1. Launch the Mirth Connect Administration tool

2. Open the **Channels** tab.

3. Under Channel tasks click on **Import Channel.**

4. Open the "\app_sever\Mirth\channels\" folder and select the "eHISC Acknowledgement to MLLP.xml". Click **Open.**

5. Repeat step 4 for each of the following channels:

    a. MLLP to eHISC Diagnostic Imaging Upload.xml

    b. MLLP to eHISC Notify PAS Event.xml

    c. MLLP to eHISC Pathology Upload.xml

6. If you want to use the file drop functionality, that is where a HL7 message can be dropped into a folder to be consumed by Mirth then import the following channels:

    a. Filedrop ADT to MLLP.xml

    b. Filedrop Imaging to MLLP.xml

    c. Filedrop Pathology to MLLP.xml

    d. Filedrop Upload Ack from MLLP.xml

7. To configure the MLLP Channels to point to eHISC.

8. Open the "MLLP to eHISC Diagnostic Imaging Upload" Channel.

    a. Select the **Source** tab.

        i. Update the **Source** settings to listen on the Port for your Mirth configuration.

b. Select the **Destinations** tab.
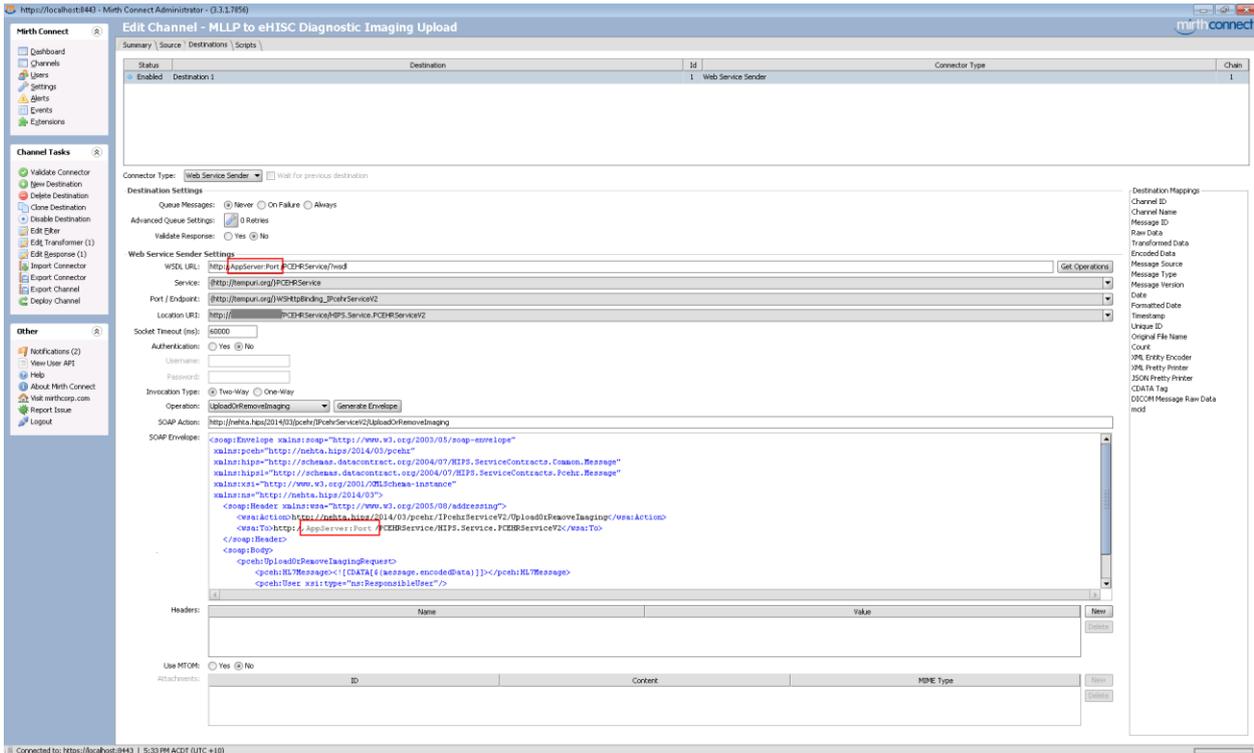
i. Update the **WSDL URL** to:

http://[AppServerName]:[Port]/HIPSServer_Test/HIPS.Service.PCEHR Service.svc?wsdl

where [AppServerName] is the eHISC application server name and [Port] is the port number the eHISC web services are running on.

ii. Update the **SOAP Envelope** details. Find the <wsa:To> element in the SOAP Envelope xml and update the AppServerName and Port to be the eHISC Application Server and Port.

….

<wsa:To>http://[AppServerName]:[Port]/HIPSServer_Test/HIPS.Servi ce.PCEHRService.svc/HIPS.Service.PCEHRServiceV2</wsa:To>

…

iii. Under the **Channel Tasks** menu, click **Save Changes**.

9. Click on the **Channels** menu item under the **Mirth Connect** menu.

10. Repeat steps 8 and 9 for the "MLLP to eHISC Pathology Upload" Channel.

11. Open the "MLLP to eHISC Notify PAS Event" Channel.

a. Select the **Source** tab.

i. Update the **Source** settings to listen on the Port for your Mirth configuration.

b. Select the **Destinations** tab.

Approved for external use   31 May 2016

    i. Update the **WSDL URL** to:

    http://[AppServerName]:[Port]/HIPSServer_Test/HIPS.Service.DatabaseLoaderService.svc?wsdl

    where [AppServerName] is the eHISC application server name and [Port] is the port number the eHISC web services are running on.

    ii. Update the **SOAP Envelope** details. Find the <wsa:To> element in the SOAP Envelope xml and update the AppServerName and Port to be the eHISC Application Server and Port.

    ….

    <wsa:To>http://[AppServerName]:[Port]/HIPSServer_Test/HIPS.Service.DatabaseLoaderService.svc/HIPS.Service.PCEHRServiceV2</wsa:To>

    …

    iii. Under the **Channel Tasks** menu, click **Save Changes**.

12. Copy the accept-ack-message.jar to the MIRTH_HOME\custom-lib directory, then restart Mirth.

9.   eHISC Operation Queue - MSMQ Configuration

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

9.1   My Health Record System Queue

Follow these steps to create the transactional MSMQ My Health Record System queue for eHISC.

1. On the eHISC 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_test/hips.service.pcehrqueue.svc"**.

   NOTE: if the site name has been modified something other than **hipsserver_test** 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 eHISC application account and check Full Control.

   c. Then click OK.

9.2   Ack Queue

Follow these steps to create the transactional MSMQ Ack queue for eHISC.

1. On the eHISC 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_test/hips.service.ackqueue.svc"**.

   NOTE: if the site name has been modified something other than **hipsserver_test** 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 eHISC application account and check Full Control.

    c. Then click OK.

9.3 Permissions

The MSMQ storage folders must allow access to the eHISC 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 eHISC AD Service account user and check Full Control.

7. Then click Ok.

10. Web Configuration Setup

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

1. web.config.svt.http: **HTTP** web service connectivity into eHISC and for use against the **SVT** environment.

2. web.config.svt.https: HTTPS web service connectivity into eHISC and for use against the SVT environment.

3. web.config.prod.http: HTTP web service connectivity into eHISC and for use against the PROD environment.

4. web.config.prod.https: HTTPS web service connectivity into eHISC and for use against the PROD environment.

These sample configuration files for eHISC specify the use of HTTP Basic Authentication on top of HTTPS because of a specific integration requirement by some organisations. The eHISC 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 35 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 eHISC Database will reside.

3. Replace all references of the "AppServerName" to the name of the server where eHISC 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. Under the <system.serviceModel> <behaviours> tag a behaviour named "concurrentMetadataSupport" exists. This allows you to increase the number of concurrent calls that can be made to the PCEHRQueue service. The throttle for MaxConcurrentCalls affects the number of concurrent request threads the service can process. This setting should be approached with the idea of limiting the number of active threads to the PCEHRService, which allows you to do the math and estimate the number of requests that can be processed per second. **Note**: If the MaxConcurrentCalls is set to more than 1 then the ESB sending the message will need to be configured in such a way that the same patient is not sent in concurrently but in a sequential order to avoid documents being uploaded out of order.

5. In the appSettings change the IhiUserQualifierProviderIndividual 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/hi/userid/1.0; for NT Health, http://ns.health.nt.gov.au/ id/hi/userid/1.0, etc.)

6. In the appSettings change the IhiUserQualifierHiUser to the user qualified domain in the format that is identified by DHS (e.g. for RightWell Health, http://ns.rightwellhealth.org.au/id/{0}/userid/1.0)

7. In the appSettings change the IhiUserQualifierAuthorisedEmployee to the user identifier supplied for the authorised employee for non-interactive processing (e.g. for RightWell Health, "http:// ns.rightwellhealth.org.au/id/ae/userid/1.0")

8. In the appSettings change the CdaUserIdQualifierFormat to the user identifier in the CDA signature file for CDA packaging (e.g. for RightWell Health, "http:// ns.rightwellhealth.org.au/id/cda/userid/1.0/{0}")

9. In the appSettings change the PathologyReportUploadLocation and ImagingReportUploadLocation to be a folder where eHISC should retrieve the Pathology and Diagnostic Imaging reports if a Reference Pointer is specified in the HL7 messages.

10. In the appSettings, if required, update the DiagnosticImagingReportDocumentFormatCode and PathologyReportDocumentFormatCode. See *Appendix A Application Server Configuration Explanation* for further details.

11. In the appSettings update the HpiiValidationPeriodDays to the number of days your organisation prefer the number of days after Hpii validation for the Hpii to remain to be valid for.

12. In the appSettings update the FileLocation to a local folder if you have not set the AckService to point to Mirth but the eHISC AckService. See *Appendix A Application Server Configuration Explanation* for further details.

13. 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 eHISC 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.

14. 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 eHISC AD Service account user**.

.

11. 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, *.xml and *.dll files and directories under the "appServer\binaries" folder into the "D:\Projects\HIPS_TEST\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.
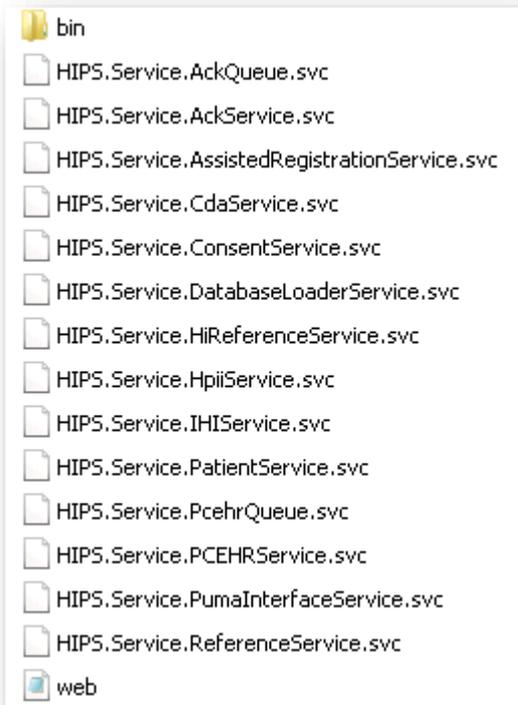
3. Ensure that there are 14 SVC files and a web.config file in this folder.

4. Ensure that there are 41 DLL files and 13 XML files under the "bin" folder.

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

12. Confirm Installation

12.1 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_TEST/HIPS.Service.AckQueue.svc
- http://*servername*:**50500**/HIPSServer_TEST/HIPS.Service.AckService.svc
- http://*servername*:**50500**/HIPSServer_TEST/HIPS.Service.AssistedRegistrationService.svc
- http://*servername*:**50500**/HIPSServer_TEST/HIPS.Service.CdaService.svc
- http://*servername*:**50500**/HIPSServer_TEST/HIPS.Service.ConsentService.svc
- http://*servername*:**50500**/HIPSServer_TEST/HIPS.Service.DatabaseLoaderService.svc
- http://*servername*:**50500**/HIPSServer_TEST/HIPS.Service.HiReferenceService.svc
- http://*servername*:**50500**/HIPSServer_TEST/HIPS.Service.HpiiService.svc
- http://*servername*:**50500**/HIPSServer_TEST/HIPS.Service.IHIService.svc
- http://*servername*:**50500**/HIPSServer_TEST/HIPS.Service.PatientService.svc
- http://*servername*:**50500**/HIPSServer_TEST/HIPS.Service.PcehrQueue.svc
- http://*servername*:**50500**/HIPSServer_TEST/HIPS.Service.PCEHRService.svc
- http://*servername*:**50500**/HIPSServer_TEST/HIPS.Service.ReferenceService.svc

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

- https://*servername*:**50443**/HIPSServer_TEST/HIPS.Service.AckQueue.svc
- https://*servername*:**50443**/HIPSServer_TEST/HIPS.Service.AckService.svc
- https://*servername*:**50443**/HIPSServer_TEST/HIPS.Service.AssistedRegistrationService.svc
- https://*servername*:**50443**/HIPSServer_TEST/HIPS.Service.CdaService.svc
- https://*servername*:**50443**/HIPSServer_TEST/HIPS.Service.ConsentService.svc
- https://*servername*:**50443**/HIPSServer_TEST/HIPS.Service.DatabaseLoaderService.svc
- https://*servername*:**50443**/HIPSServer_TEST/HIPS.Service.HiReferenceService.svc
- https://*servername*:**50443**/HIPSServer_TEST/HIPS.Service.HpiiService.svc
- https://*servername*:**50443**/HIPSServer_TEST/HIPS.Service.IHIService.svc
- https://*servername*:**50443**/HIPSServer_TEST/HIPS.Service.PatientService.svc
- https://*servername*:**50443**/HIPSServer_TEST/HIPS.Service.PcehrQueue.svc
- https://*servername*:**50443**/HIPSServer_TEST/HIPS.Service.PCEHRService.svc
- https://*servername*:**50443**/HIPSServer_TEST/HIPS.Service.ReferenceService.svc

Figure 3 – IIS web service confirmation page

THIS IS THE COMPLETION OF THE INSTALLATION OF eHISC

Approved for external use

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 application directory

Section	Option Name	Suggested Value	Description
Connection String	Data Source	*Name of SQL server*	eHISC will attempt to connect to this SQL server.
	Initial Catalog	PcehrDataStoreTest	eHISC will use the database with this name.
	Integrated Security	SSPI	If set to SSPI as recommended then eHISC 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.
CDA Service	baseAddress	net.tcp://servername:**50000**/	The CDA service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername:**50500**/CdaService/	The CDA service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername:**50443**/CdaService/	The CDA service will be accessible using HTTPS protocol at this URL.
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.

Section	Option Name	Suggested Value	Description
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.
	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**/PcehrQueue/	The Pcehr Queue services will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername:**50443**/PcehrQueue/	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.

Approved for external use

Section	Option Name	Suggested Value	Description
	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.
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.

Section	Option Name	Suggested Value	Description
Ack Service	baseAddress	net.tcp://servername:**50000**/	The Ack service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername:**50500**/AckService/	The Ack service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername:**50443**/AckService/	The Ack service will be accessible using HTTPS protocol at this URL.
Ack Queue Service	baseAddress	net.tcp://servername:**50000**/	The Ack Queue service will be accessible using net.tcp protocol at this URL.
	baseAddress	http://servername:**50500**/AckQueue/	The Ack Queue service will be accessible using HTTP protocol at this URL.
	baseAddress	https://servername:**50443**/AckQueue/	The Ack Queue service will be accessible using HTTPS protocol at this URL.
PCEHR MSMQ Client Endpoint	address	net.msmq://localhost/private/HIPSServer_TEST/HIPS.Service.PcehrQueue.svc	The address for the local MSMQ service
Ack MSMQ Client Endpoint	address	net.msmq://localhost/private/HIPSServer_TEST/HIPS.Service.AckQueue.svc	The address for the local MSMQ service
Ack Service Client Endpoint	address	http://localhost:663/services.AckService	The endpoint address for the Ack Service. This can either be set to be Mirth Connect eHISC Acknowledgement to MLLP Channel or if Mirth Connect is not implemented the eHISC Acknowledgement Service end point which will require the FileLocation appsetting (below) to be set.
App Settings	IhiProductName	<Product Name of the new product based on the eHISC source code>	Product Name registered with DHS
	IhiProductVersion	<Product Version of the new product based on the eHISC source code>	Product Version registered with DHS

Section	Option Name	Suggested Value	Description
	IhiVendorId	<Vendor Name of the organisation that has created the new product based on the eHISC source code>	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	
	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,
	IhiUserQualifierAuthorised Employee	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	eHISC will revalidate an IHI before returning it to the calling system or using it in a call to the My Health Record System, if it was not obtained or last validated within the number of days specified here. For organisations that do not connect eHISC to the HI Service, it is necessary to set this to a large number (e.g. 999) to prevent eHISC attempting revalidation.
	HiServiceUrl	Vendor Environment: https://www5.medicareaustralia.gov.au/cert/soap/services/ Production Environment: https://www3.medicareaustralia.gov.au/pcert/soap/services/	eHISC will connect to the HI Service at this URL, which is that of the HI Service vendor or production environment.

Section	Option Name	Suggested Value	Description
	PcehrProductName	<Product Name of the new product based on the eHISC source code>	Product Name registered with My Health Record SVT or Production
	PcehrProductVersion	<Product Version of the new product based on the eHISC source code>	Product Version registered with My Health Record SVT or Production
	PcehrVendorId	<Vendor Name of the organisation that has created the new product based on the eHISC source code>	Vendor ID registered with My Health Record SVT or Production
	PcehrRole	CIS	eHISC is designed to communicate with My Health Record B2B Gateway as part of a Clinical Information System (CIS).
	CheckDoesPcehrExist	true	Whether eHISC should check the 'digital health record' advertised status of each patient immediately upon obtaining his/her IHI.
	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.
	PatientMasterOverride	False	Allows client apps to provide temporary patient demographic overrides within eHISC
	AvoidProxy	True	Avoid standard Proxies
	DoesPCEHRExistUrl	https://b2b.ehealthvendortest.health.gov.au/doesPCEHRExist	eHISC will connect to this URL to check the 'digital health record' advertised status of an IHI.
	UploadDocumentUrl	https://b2b.ehealthvendortest.health.gov.au/uploadDocument	eHISC will connect to this URL to upload or supersede a document to the My Health Record System.
	GetDocumentUrl	https://b2b.ehealthvendortest.health.gov.au/getDocument	eHISC will connect to this URL to download a document from the My Health Record System.

Section	Option Name	Suggested Value	Description
	GetViewUrl	https://b2b.ehealthvendortest.health.gov.au/getView	eHISC will connect to this URL to request a view from the My Health Record System.
	RemoveDocumentUrl	https://b2b.ehealthvendortest.health.gov.au/removeDocument	eHISC will connect to this URL to remove a document from the My Health Record System.
	ListDocumentUrl	https://b2b.ehealthvendortest.health.gov.au/getDocumentList	eHISC will connect to this URL to list documents available to download from the My Health Record System.
	GainPCEHRAccessUrl	https://b2b.ehealthvendortest.health.gov.au/gainPCEHRAccess	eHISC will connect to this URL to gain access to a digital health record.
	RegisterPcehrUrl	https://b2b.ehealthvendortest.health.gov.au/registerPCEHR	eHISC will connect to this URL to register a digital health record.
	DoesPCEHRExistTimeoutSeconds	120	Connection Timeout (in seconds) for DoesPCEHRExist Service. Defaults to 60 if not included in the configuration file.
	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 eHISC-UI

Section	Option Name	Suggested Value	Description
			This can only be set to true IF the Assisted Registration web service is used outside of the eHISC UI. Note setting this false will mean that eHISC will need to pass Conformance Testing again to use Assisted Registration outside of the eHISC-UI solution of Assisted Registration.
	RegisteredDateOfBirthEnabled	False	**ONLY used if you expect patient to provide a different date of birth to what they have recorded at Medicare** This setting instructs eHISC to store the Medicare registered Date of Birth separately to the patients current Date of Birth and use to use the registered Date of Birth if the current Date of Birth does not return a valid IHI for the patient.
	PathologyReportUploadLocation	C:\Uploads\Pathology\	The folder location where the eHISC service will retrieve Pathology reports when a Reference Pointer is used rather than Embedded reports in the HL7 message.
	ImagingReportUploadLocation	C:\Uploads\Imaging\	The folder location where the eHISC service will retrieve Imaging reports when a Reference Pointer is used rather than Embedded reports in the HL7 message.
	DiagnosticImagingReportDocumentFormatCode	1.2.36.1.2001.1006.1.222.4	The Document Format Code to use for the Pathology Reports 3A. This value indicates if the HPI-I Enforced or HPI-I Relaxed template is to be used to upload the Diagnostic Imaging Reports to the PCEHR Service. By default it is set to HPI-I Enforced. Refer to the PCEHR Service documentation for applicable values.
	PathologyReportDocumentFormatCode	1.2.36.1.2001.1006.1.220.4	The Document Format Code to use for the Diagnostic Imaging Reports 3A. This value indicates if the HPI-I Enforced or HPI-I Relaxed template is to be used to upload the Pathology Reports to the PCEHR Service. By default it is set to HPI-I Enforced. Refer to the PCEHR Service documentation for applicable values.
	HpiiValidationPeriodDays	1	The number of days any stored HPI-I's are valid for.

Section	Option Name	Suggested Value	Description
	FileLocation	C:\mirth\upload-ack	The location where application Acknowledgements will be saved, if Mirth or another ESB provided endpoint is not invoked.
	UseHL7MessageDateTime	True	Flag to indicate if the check for earlier pending HL7 messages for Pathology or Diagnostic Imaging Uploads should use the HL7 Message Date Time or not. If false will use the DateCreated in the HL7MessageLog table.