Australian Government

Australian Digital Health Agency

HIPS
Module Guide (Core)

7 June 2019   v7.1.1

Approved for external use

Acknowledgements

Council of Australian Governments

HL7 International

Disclaimer

Document control

Copyright © 2019 Australian Digital Health Agency

OFFICIAL

Document information

Key information

Owner   National Health Chief Information Officer, Infrastructure Operations

Contact for enquiries   Australian Digital Health Agency Help Centre

Phone   1300 901 001

Email   help@digitalhealth.gov.au

Table of contents

1 Introduction

1.1 Purpose

The purpose of this document is to provide architectural detail of the HIPS Core Module which is a one module within the HIPS Product Suite. The HIPS Core Module is a middleware and communications solution to enable a CIS (Clinical Information System), PAS (Patient Administration System), LIS (Laboratory Information System) and/or RIS (Radiology Information System) to interact with the national My Health Record system (formerly known as the Personally Controlled Electronic Health Record/PCEHR system).

The intended use of the document is to assist health facilities to understand the functions and logic within the HIPS Core Module and the interactions between the facility's information systems, the HIPS Core Module and the national My Health Record system.

The document describes the functions the solution can interface with an Enterprise Service Bus (ESB) 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 the My Health Record system. It can also be used as a broker to the My Health Record system without the need of an interface to an ESB for upload and retrieval of documents from the My Health Record system.

1.2 Intended audience

This document is intended for system operators responsible for the operation of their instances of the HIPS product, particularly those responsible for the interface between My Health Record, HIPS, and local infrastructure.

1.3 Scope

This document describes the HIPS Core Module functions including:

- Database Loader, for processing HL7 messages from the PAS
- Get Validated IHI, for interacting with the Healthcare Identifier (HI) service
- checking whether a My Health Record is advertised
- consent and participation services
- uploading or superseding a CDA document in the My Health Record system
- removing a document from the My Health Record system
- searching for, validating, and storing HPI-I records for local providers
- providing assisted registration to create a My Health Record for a consumer
- viewing documents on the My Health Record system.

This document does not list the web services or detail the required HL7 message formats. These are covered in the Service Catalogue – Core, Patient Administration HL7v2 Profile, Pathology Results HL7v2 Profile and Diagnostic Imaging HL7v2 Profile documents respectively.

This document does not describe any details of the other HIPS modules as these are covered by other documentation.

1.4   Assumptions

During the development of this document the following assumptions have been made:

- The document audience have a high-level understanding of health information systems and the terminology used.

1.5   Definitions and Acronyms

Throughout the document the term "Participating Organisation" is used which related to one of the following system implementers of HIPS:

- Healthcare Provider Organisation (HPO),

- Contracted Service Provider (CSP), or

- Jurisdiction (State or Territory Health Department).

2 Architectural Detail

2.1 Component Model

The logical component model describes the high-level architecture for a non-specific implementation of the HIPS Core module in terms of components and the relationships. Each component has a well-defined set of capabilities, responsibilities, and interfaces through which it interacts with other components. At this level, components represent a logical grouping of related functions rather than specific software or hardware modules. The purpose of the logical component model is to depict the overall functionality and organisation of the system.

2.1.1 Functionality for IHI, HPI-I and My Health Record System
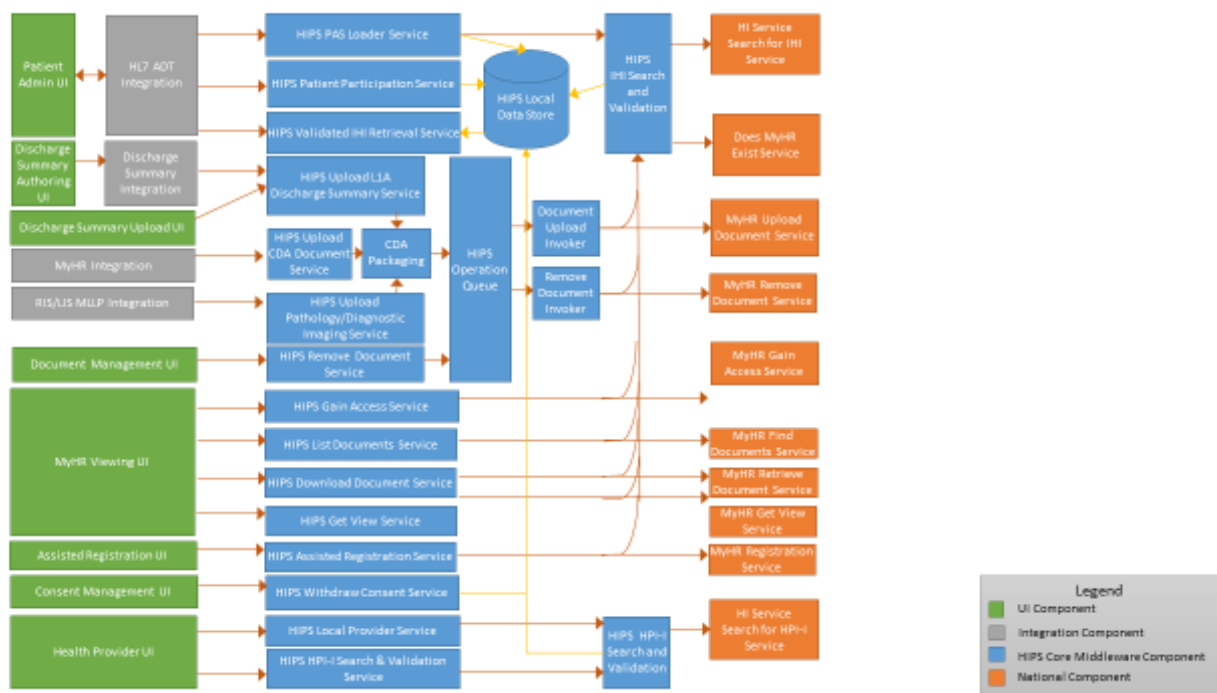
Figure 1 - Logical Component Model for Existing Functionality for IHI, HPI-I and My Health Record system

The logical components identified in Figure 1 are described in the following table, which describes the existing functionality for IHI, HPI-I, and My Health Record system components

Name	Description, Responsibilities, and Implementation Considerations
Patient Administration System	*Description* Hospital patient administration systems (PAS). *Responsibilities* Records patient identifiers, demographic information, admissions, discharges and transfers. Sends HL7 messages to downstream systems whenever a patient record is created or updated, and whenever a patient is admitted, discharged or transferred. *Implementation Considerations* Each hospital may have a separate PAS. These are simulated in development and test using de-identified production messages.
Enterprise Master Patient Index	*Description* Enterprise Master Patient Index (EMPI) *Responsibilities* Records patient identifiers and demographic information. Assigns enterprise identifiers to patients. Sends HL7 messages to downstream systems whenever a hospital patient MRN is moved from one enterprise ID to another. *Implementation Considerations* This is an existing enterprise system in some Jurisdictions. Simulated in development and test using de-identified production messages.
Discharge Summary Authoring	*Description* An application in which users create discharge summary documents. *Responsibilities* Allows creation of discharge summary documents and distribution to the My Health Record system and health provider organisations or individuals selected from a provider directory. Recipients may be selected from a local copy of the healthcare provider directory. This system may include a tool for monitoring and reprocessing failed distributions of clinical documents. *Implementation Considerations* Participating Organisations may have one or more systems that perform this function.
Clinical Document Viewing	*Description* An application in which users view clinical documents. *Responsibilities* Allows viewing of clinical documents, whether locally created, downloaded from the My Health Record system, or received via P2P delivery. *Implementation Considerations* Participating Organisations may have one or more systems that perform this function.

Name	Description, Responsibilities, and Implementation Considerations
LIS / RIS / CIS	*Description* Health Facilities Clinical Information Systems (CIS), Diagnostic Imaging Radiology Information System (RIS) or Pathology Laboratories LIS (Laboratory Information System). *Responsibilities* Records patient identifiers, demographic information, service dates, and requesting information. Sends HL7 messages to downstream systems whenever a pathology or diagnostic imaging order is completed and report produced. *Implementation Considerations* Each Health Facility may have a separate CIS/LIS/RIS. These are simulated in development and test using de-identified production messages.
Patient Integration	*Description* Integration components for HL7 messages from PAS and EMPI systems. *Responsibilities* Integrates the PAS, EMPI, CIS and HIPS. Inserts the state/territory healthcare identifier and transforms PAS messages into the standardised format for HIPS. May allow EMPI and/or CIS to obtain the IHI from HIPS. *Implementation Considerations* Preferably implemented in an enterprise service bus.
My Health Record System Integration	*Description* Integration components for accessing My Health Record system from clinical systems. *Responsibilities* Integrates the CIS with HIPS. May transform clinical documents to or from CDA. *Implementation Considerations* Preferably implemented in an enterprise service bus.
Provider Integration	*Description* Integration components for accessing Healthcare Provider Identifiers from clinical systems. *Responsibilities* Integrates the CIS/LIS/RIS with HIPS. Inserts the Health Provider Individual Identifier and transforms CIS/LIS/RIS messages into the standardised format for HIPS. May allow CIS/LIS/RIS to obtain the HPI-I from HIPS *Implementation Considerations* Preferably implemented in an enterprise service bus.
PAS Loader Service	*Description* HIPS web service that accepts PAS HL7 messages. *Responsibilities* Stores patients and episodes in the HIPS Core database. *Implementation Considerations* This is an existing component of HIPS.

Name	Description, Responsibilities, and Implementation Considerations
Patient Participation Service	*Description* HIPS web services for determining which patients have a My Health Record. *Responsibilities* Allows clinical systems to query or subscribe to a feed of patients who are found to have a My Health Record. Also allows the disclosure of the existence of a hidden My Health Record. *Implementation Considerations* This is an existing component of HIPS.
Consent Withdrawal Service	*Description* HIPS web services for managing the withdrawal of consent to upload documents to the My Health Record system. *Responsibilities* Store and query a patient's withdrawal of consent to upload a document. *Implementation Considerations* This is an existing component of HIPS.
Validated IHI Retrieval	*Description* Web service that returns the IHI for a specified patient. *Responsibilities* Check whether the IHI was last validated more than the configured period of time in the past, and if so, revalidates the IHI before returning it. *Implementation Considerations* This is an existing component of HIPS.
IHI Search & Validation	*Description* Business logic and service invoker for IHI Lookup Service. *Responsibilities* Searches for an IHI for each patient and revalidates the IHI when required. *Implementation Considerations* This is an existing component of HIPS.
My Health Record Check Invoker	*Description* Service invoker for the Does PCEHR Exist check. *Responsibilities* Each time a patient's IHI is obtained from the HI Service, or a new episode is created, invokes the My Health Record system web service to check whether the patient has a My Health Record. *Implementation Considerations* This is an existing component of HIPS.

Name	Description, Responsibilities, and Implementation Considerations
My Health Record System Gain Access Service	*Description* HIPS web service that establishes access to the My Health Record system for a specified patient. *Responsibilities* Check whether the IHI was last validated more than the configured period of time in the past, and if so, revalidates the IHI before calling the My Health Record system Gain Access service. *Implementation Considerations* This is an existing component of HIPS.
Upload CDA Document Service	*Description* HIPS web service that accepts a document for upload to My Health Record system. *Responsibilities* After checking the user, patient, episode, consent, age and IHI, sends document for CDA packaging and onto the operation queue to be uploaded. *Implementation Considerations* This is an existing component of HIPS.
CDA Packaging	*Description* Business logic for packaging a CDA document. *Responsibilities* Creates an electronic signature for the document, using the NASH PKI Certificate for the Health Provider Organisation that authored the document, and creates the CDA package ZIP file using the attachments supplied and the logo image supplied or configured. For P2P it also supports wrapping the CDA package in an HL7 v2 MDM wrapper to support sending to receivers who publish interaction records with an MDM service category. *Implementation Considerations* This is an existing component of HIPS.
Operation Queue	*Description* Queue for operations that HIPS will take care of completing. *Responsibilities* Process queued HL7 conversion, upload or remove, or HL7 acknowledgement operations. Retry operations that encountered a temporary failure either within HIPS or on the external system. Maintain the original order of upload or remove operations that relate to the same document set. *Implementation Considerations* This is an existing component of HIPS.
Remove Document from My Health Record System Service	*Description* HIPS web service that accepts a request to remove a document from the My Health Record system. *Responsibilities* After checking the user, patient, episode and IHI, adds the request onto the operation queue. *Implementation Considerations* This is an existing component of HIPS.

Name	Description, Responsibilities, and Implementation Considerations
Document Upload Invoker	*Description* HIPS business logic and service invoker for My Health Record system upload document service. *Responsibilities* Processes an upload operation from the queue. *Implementation Considerations* This is an existing component of HIPS.
Remove Document Invoker	*Description* HIPS business logic and service invoker for My Health Record system remove document service. *Responsibilities* Processes a remove operation from the queue. *Implementation Considerations* This is an existing component of HIPS.
List Documents on My Health Record System Service	*Description* HIPS web service that executes a document query against the My Health Record system. *Responsibilities* After checking the user, patient, and IHI, executes the query against the My Health Record System and returns the list of matching documents. *Implementation Considerations* This is an existing component of HIPS.
Download Document from My Health Record System Service	*Description* HIPS web service that downloads a document from the My Health Record system. *Responsibilities* After checking the user, patient, and IHI, requests the document from the My Health Record system, validates the CDA package, checks the patient demographics, and returns the document contents. *Implementation Considerations* This is an existing component of HIPS.
My Health Record System Change History Service	*Description* HIPS web service that obtains a list of all versions of a document from the My Health Record system. *Responsibilities* After checking the user, patient, and IHI, requests the change history view from the My Health Record system, and returns the list of document versions. *Implementation Considerations* This is an existing component of HIPS.

Name	Description, Responsibilities, and Implementation Considerations
Local Provider Service	*Description* HIPS web services for managing the storage of Local Health Provider information. *Responsibilities* Stores local health provider details in the HIPS Core database. *Implementation Considerations* This is an existing component of HIPS.
Validated HPI-I Retrieval	*Description* Web service that returns the HPI-I for a specified health provider. *Responsibilities* Check whether the HPI-I was last validated more than the configured period of time in the past, and if so, revalidates the HPI-I before returning it. *Implementation Considerations* This is a potential future component of HIPS. The retrieval of a validated HPI-I based on the configured period of time is part of the HL7 Conversion business logic but not currently exposed as a web service.
HPI-I Search & Validation	*Description* Business logic and service invoker for HPI-I Lookup Service. *Responsibilities* Searches for an HPI-I for specified health provider and revalidates the HPI-I when required. *Implementation Considerations* This is an existing component of HIPS.
HI Service Search for IHI Service	*Description* Web service for looking up a consumer's IHI given certain demographic details. *Responsibilities* Allows the search and validation of IHI numbers. *Implementation Considerations* This is an existing component of the HI Service operated by the federal Department of Human Services (DHS).
Does PCEHR Exist Service	*Description* Web service for checking whether a consumer has a My Health Record that is visible to the accessing organisation. *Responsibilities* Determine the access permission for the organisation – no My Health Record or hidden, already gained access, can gain access with code, or can gain access without code. *Implementation Considerations* This is an existing component of the 'My Health Record' System B2B Gateway operated by the 'My Health Record' National Infrastructure Operator (NIO).

Approved for external use

Name	Description, Responsibilities, and Implementation Considerations
PCEHR Gain Access Service	*Description* Web service for gaining access to a consumer's My Health Record *Responsibilities* Adds the accessing organisation to the Provider Access List of the consumer's My Health Record. Sets the access permission according to the code that was supplied. *Implementation Considerations* This is an existing component of the My Health Record system B2B Gateway operated by the 'My Health Record' National Infrastructure Operator (NIO).
PCEHR Upload Document Service	*Description* My Health Record system web service for uploading a document to a consumer's My Health Record *Responsibilities* Validates and stores a document, optionally superseding an existing document. *Implementation Considerations* This is an existing component of the My Health Record system B2B Gateway operated by the My Health Record National Infrastructure Operator (NIO).
PCEHR Remove Document Service	*Description* Web service for effectively removing a document that was previously uploaded to a consumer's My Health Record. *Responsibilities* Mark the document so that it is hidden from the consumer and other healthcare providers. *Implementation Considerations* This is an existing component of the My Health Record system B2B Gateway operated by the My Health Record National Infrastructure Operator (NIO).
PCEHR Find Documents Service	*Description* Web service for listing the documents that match a query. *Responsibilities* List the documents that match the given query. *Implementation Considerations* This is an existing component of the My Health Record system B2B Gateway operated by the My Health Record National Infrastructure Operator (NIO).
PCEHR Retrieve Document Service	*Description* Web service for retrieving a document from a patient's My Health Record. *Responsibilities* Retrieve the document with the specified unique ID and repository ID. *Implementation Considerations* This is an existing component of the My Health Record system B2B Gateway operated by the My Health Record National Infrastructure Operator (NIO).

Name	Description, Responsibilities, and Implementation Considerations
PCEHR Change History Service	*Description* Web service for listing the versions of a specified document. *Responsibilities* List the versions of the document with the specified entry UUID. *Implementation Considerations* This is an existing component of the My Health Record system B2B Gateway operated by the My Health Record National Infrastructure Operator (NIO).
HI Service Search for HPI-I Service	*Description* Web service for looking up a health provider's HPI-I given certain demographic details. *Responsibilities* Allows the search and validation of HPI-I numbers. *Implementation Considerations* This is an existing component of the HI Service operated by the federal Department of Human Services (DHS).

2.2　Business Logic

2.2.1　My Health Record System Participation and Authorisation Model

Each healthcare facility within Australia, that intends to upload clinical documents to the My Health Record system, must be associated with a participating Healthcare Provider Organisation (HPO), identified by an HPI-O number. Multiple facilities may be associated with the same HPO. For example:

- Some or all hospitals, clinics or laboratories within a participating organisation may be associated to the seed HPO for the participating organisation.

- Some or all hospitals within a Local Health Network (LHN) may be associated to the network HPO for that LHN.

- Some or all hospitals, clinics or laboratories may themselves be a seed or network HPO.

For any patient record to which HIPS has assigned a valid IHI, the creation of a new episode of care in the Patient Administration System (PAS) at the health facility will trigger HIPS to send a message to the My Health Record system, asking if the consumer has a My Health Record. The message will include:

1 The consumer's IHI;

2 The facility's associated healthcare provider organisation's HPI-O; and

3 The local system identifier of the authorised employee for the facility or the interactive user.

Once the My Health Record system receives this message, the My Health Record system will proceed to verify the right of the HPO to access the My Health Record system, and determine whether the consumer has an advertised record. The system then advises the HPO whether the consumer has a My Health Record, with the answer being "no" if the consumer does not have a record, or does not have an advertised record.

HIPS will store this advice separately for each participating HPO. In the case where the consumer has elected to hide the existence of his/her My Health Record, it is possible that one participating HPO has gained access and therefore "knows" the consumer has a My Health Record, while

another HPO has not gained access and therefore does not "know" that the same consumer has a My Health Record. The Participating Organisation should respect this separation of information for privacy reasons.

When a clinical document is distributed, if the My Health Record system advice to the healthcare facility's HPO indicated that the consumer has a My Health Record, the expected outcome is that the clinical document will be uploaded, unless the consumer requests that it is not uploaded (via withdrawal of consent), or the clinical information system user requests that it is not uploaded.

Otherwise, if the advice indicated the consumer does not have a My Health Record, the expected outcome is that the clinical document will not be uploaded, unless the consumer disclosed the existence of the My Health Record.

2.2.2 Database Loader Service

2.2.2.1 Description

This service is designed to accept messages from patient administration systems via a SOAP or MLLP message broker. This message broker should transform the messages to comply with the format expected by HIPS, which is based on the international HL7 standard, version 2.3.1. Refer to the document "*Patient Administration HL7v2 Profile*" for details of this format.

This service stores the patient and episode information into the HIPS Core database and triggers the automatic IHI lookup and check for advertised My Health Record.

A failure to store the message, patient or episode will result in a negative acknowledgement being returned. A failure to obtain an IHI or check the My Health Record status will not result in a negative acknowledgement. The IHI is not returned in the acknowledgement but stored into the HIPS Core database.

An example of the minimal input for registering a patient is as follows:

```
MSH|^~\&|App|Facility||||DateTime|O3V1|ADT^A28|MsgID|P|2.3.1|||AL|NE|AU|ASCII|EN
PID|||MRN^^^Facility^MR~Medicare^^^^MC||Surname^First Name||DOB|Sex|||Address
Line 1^Address Line 2^Suburb^State^Postcode^^H
```

2.2.3 Patient Identifier

Each HIPS service that is designed to act upon a single patient record will contain a parameter "patientIdentifier". The Patient Identifier object is used to identify which facility and patient to operate upon. The Patient Identifier can be either:

- Medical Record Number (MRN), scoped within a specified facility (Hospital Code),

- State Patient Identifier, scoped within the Participating Organisation,

- Registered Enterprise Patient, scoped within the Participating Organisation,

- Validated Individual Healthcare Identifier (IHI), scoped nationally,

- Patient Master Identifier, internal to the HIPS Core database, or

- Demographic, used within Assisted Registration calls when the person is not a current patient.

2.2.3.1 Mrn

This class represents a Medical Record Number (MRN) that identifies a patient at a facility. It is usually allocated by the facility PAS or PMI and the maximum length of Mrn is 40 characters. This value is stored in the Mrn column of the HospitalPatient table in the HIPS Core database.

2.2.3.2 StatePatientId

This class represents a number or code that identifies a patient across an entire Participating Organisation. It can be allocated by a type of EMPI (Enterprise Patient Master Index), but may also be allocated by a PAS and the maximum length of StatePatientId is 64 characters. This value is stored in the StatePatientId column of the PatientMaster table in the HIPS Core database

2.2.3.3 RegisteredEnterprisePatient

This class is a patient identifier that identifies a patient who is registered at the enterprise level using a "StatePatientId" and can extend the registration to a new facility using the supplied "Mrn".

The biggest difference between a StatePatientId and a RegisteredEnterprisePatient is that the RegisteredEnterprisePatient allows the operation to access patient records in a different facility to the facility where the patient was originally registered.

The following business logic is used when the RegisteredEnterprisePatient class is used to identify the patient:

- Get the patient information using the StatePatientId

    o If the patient cannot be found then set the response to null and return

- Get the hospital patient information using the MRN

    o If the hospital patient record is found and the PatientMasterId matches with the patient information from the StatePatientId then return the patient information

    o If the hospital patient record is found but the PatientMasterId does not match then it means the hospital patient is on the wrong patient master record

        – Log an error message with the relevant information and return a "IncorrectStatePatientId" result

- If the hospital patient record is not found then use the PatientMasterId to retrieve the MRN of the patient

    o If an MRN is returned then the patient is currently registered using a different MRN

        – Log an error message with the relevant information and return a "IncorrectMrn" result

    o If an "InvalidPatient" result was returned then we can create a hospital patient record

        – Use the PatientMasterId obtained from the StatePatientId look up, the hospital passed in and MRN passed in via the patient identifier to create the hospital patient record

        – If this fails log an error message and return a "DatabaseError" result

        – Check the local IHI information of the patient and if not "OK" or "InvalidIhi" then return the result

        – Validate the IHI which if successful will perform a My Health Record check against the current facility and store the result.

2.2.3.4 ValidatedIhi

This class represents the set of information that makes up a validated IHI. The information includes everything that is required to determine whether the IHI remains valid, and to revalidate

the IHI. These values are stored in the PatientMaster and PatientMasterIhi tables in the HIPS Core database.

When a validated IHI is used to identify a patient in the HIPS service call, then HIPS will create or update the patient record as necessary, taking the incoming information as authoritative. This makes it possible to operate HIPS in a distributed system where HIPS does not receive a feed of PAS messages and does not make its own connections to the HI Service.

Note that this class does not contain properties for Medicare Card Number or DVA File Number, because this information is not required for IHI validation, but only when the IHI is first retrieved.

2.2.3.5   PatientMasterId

This class represents the internal primary key of the PatientMaster table in the HIPS Core database. This option is made available for applications that share use of the HIPS Core database with HIPS and hence have direct knowledge of the database keys.

2.2.3.6   Demographic

This class defines a patient's demographics for use within the registration process. This type of patient identification can only be used with Assisted Registration and cannot be used with other HIPS services that access the My Health Record System.

2.2.4   Get Validated IHI

This function retrieves the IHI information that must be inserted in a CDA clinical document to identify the patient and to allow the receiver of the document to revalidate the IHI.

2.2.4.1   Business Rules/Functional Business Logic

HIPS will first attempt to locate an existing patient record using the given patient identifier. With that patient record:

1   If the stored date of birth does not match that which is specified in the service call, then an InvalidDateOfBirth error is returned and no further action is taken. If the *RegisteredDateOfBirthEnabled* flag is true then the date of birth specified in the service call will also be checked against the registered date of birth.

2   If no IHI has been obtained for the patient record, then HIPS will attempt to obtain the IHI using the current demographic information and assign the IHI to the local patient record, possibly creating an exception alert in the process. An example of an exception alert is when the IHI status changes from Active to another status, or the IHI number is already assigned to another patient record from the same hospital.

3   If an IHI is obtained or had already been obtained for the specified patient record, and there is an outstanding exception alert on the IHI, such as a suspected duplicate or replica, then HIPS will not return the IHI to the caller.

4   If the IHI was obtained or last validated outside the time period that has been configured for this purpose, then HIPS will attempt to validate the IHI information with the HI Service, and will only return the IHI to the caller if the validation was successful. However, if the HI Service is unavailable but the IHI is available locally, the IHI will be returned with a warning that validation must still occur before the IHI can be trusted. This will occur when the document with the IHI embedded is passed back to HIPS for upload.

5   If no IHI is able to be obtained (for instance in the case that the HI Service is unavailable, or invalid or incorrect demographic information was provided to the HI Service for validation [example: invalid DVA number]), and no IHI is available locally, HIPS will return an error

response with a status indicating a HI Service Error and stating "An error prevented HIPS from successfully contacting the HI Service to retrieve a validated IHI and no IHI is available locally.". The response will include additional details returned from the HI Service, and in this case will not include an IHI. The error is also logged to the HIPS System Error Log.

6   If the IHI was obtained or last validated within the configured valid time period, then the IHI will be returned immediately without triggering another validation.

2.2.4.2   Usage Notes

This method is intended for use after a patient is registered in the PAS, to extract the IHI that was obtained from the HI Service, for use in a clinical document that will be distributed to an external health provider, to a shared repository or the My Health Record System.

One model for usage is where the clinical system is enhanced to handle IHI and CDA directly:

- A clinical system user finalises a clinical document for a patient who has a My Health Record

- The system makes a call to an ESB to find or validate the IHI for the patient

- The ESB calls this method of HIPS and returns the validated IHI to the clinical system

- The clinical system produces a CDA document with the validated IHI

- The system makes a call to the ESB to upload the document to the My Health Record System

- The ESB sends the CDA document to HIPS for upload to the My Health Record System

However, there are other implementations where the clinical system is not aware of IHIs, and thus custom-developed middleware would be needed to handle the conversion of clinical documents (e.g. HL7 discharge summaries) into CDA format:

- A clinical system user finalises a clinical document for a patient who has a My Health Record

- The clinical system delivers the clinical document data to the ESB for upload to My Health Record System, perhaps in the form of an HL7 message

- The ESB calls this method of HIPS to obtain the IHI for the patient

- The ESB embeds the IHI into the message and delivers it to a CDA conversion middleware

- The middleware converts the clinical document to CDA format and returns it to ESB

- The ESB sends the CDA document to HIPS for upload to the My Health Record System

2.2.5   Check Whether My Health Record is Advertised

2.2.5.1   Description

A user-facing system may call this service method to obtain information necessary to inform the user about whether a patient has registered for a My Health Record and wants the existence of that My Health Record to be visible to the provider organisations participating in his/her healthcare.

This method wraps the My Health Record System B2B Gateway service "Does PCEHR Exist". That name is misleading because the result is not strictly whether a My Health Record exists for the consumer, but is also affected by whether the consumer has chosen to advertise the existence of

his/her My Health Record. The result is also affected by whether the HPO is on the provider access list of the consumer's My Health Record, and if so what read access permission the consumer has given the HPO.

For a record with default access settings the result of "doesPCEHRExist" is "true, access granted" if the HPI-O is on the list, versus "true, without code" if not. For a non-hidden record with a Record Access Code (RAC), the result is "true, access granted" or "true, with code" respectively. For a hidden record, the result is "true, access granted" or "false" respectively.

The result is also used internally by HIPS to drive the related function to determine whether a patient is registered and therefore given standing consent to documents being uploaded to his/her My Health Record. The latter service is described in the Patient Participation section. The main difference is that Patient Participation is also affected by the disclosure of the existence of a My Health Record. If the patient has disclosed the existence to the HPO then they are considered to be participating regardless of whether the My Health Record is hidden.

The response contains a property AccessCodeRequired, which provides some information as to whether an access code is required in order to access the patient's My Health Record to list or view documents:

- Null – meaning that the patient has not registered for My Health Record, or has chosen to hide the existence of his/her My Health Record. The patient may still give advice of My Health Record existence and may or may not provide an access code.

- With Code – meaning that the provider can gain access to the My Health Record using an access code provided by their patient.

- Without Code – thus meaning that access is open and no RAC is required. The patient may still advise of a Limited Document Access Code (LDAC) to grant restricted access.

- Access Granted – thus meaning that access has been granted and no code is required unless the patient advises of a change to access level and provides an access code.

2.2.5.2 Usage Note

For implementations where the HI Service is called by HIPS and/or HL7 patient and episode messages are sent to HIPS, this method may not be required to be called separately, because:

- HIPS automatically calls DoesPCEHRExist immediately after obtaining an IHI from the HI Service

- HIPS automatically calls DoesPCEHRExist after creating a new episode for an existing patient

Thus, this method is a mechanism to manually trigger calls to DoesPCEHRExist. It is primarily of use where:

- The Participating Organisation does not provide a feed of HL7 messages from the PAS into HIPS, therefore this is the main mechanism to check whether a patient has a My Health Record or not.

- The clinical system requires the latest information about the access status for the My Health Record, such as immediately before or after a call to Gain Access.

2.2.5.3 PcehrExistsReuseIntervalMinutes Application Setting Behaviour

For the services that explicitly request HIPS to check with the My Health Record (IsPcehrAdvertised and RefreshPatientParticipationStatus), the setting

PcehrExistsReuseIntervalMinutes is not used, instead HIPS always calls the doesPCEHRExist web service operation of the My Health Record system to get the latest status.

For the DatabaseLoaderService NotifyPasEvent, if a new episode is created, HIPS will call the doesPCEHRExist web service operation of the My Health Record system to get the latest status, unless a call was made for this patient and HPO within the number of minutes in setting PcehrExistsReuseIntervalMinutes.

For the PathologyImagingService UploadOrRemoveImaging and UploadOrRemovePathology, if a report is to be uploaded that has not been uploaded before, and there is no AUSEHR flag, HIPS will call the doesPCEHRExist web service operation of the My Health Record system to get the latest status, unless a call was made for this patient and HPO within the number of minutes in setting PcehrExistsReuseIntervalMinutes.

After any HIPS service performs an IHI search or validation in the HI Service and obtains the IHI of a patient from the HI Service, if the setting CheckDoesPCEHRExist is true, HIPS will call the doesPCEHRExist web service operation of the My Health Record system to get the latest status, unless a call was made for this patient and HPO within the number of minutes in setting PcehrExistsReuseIntervalMinutes.

2.2.6 Consent and Participation

2.2.6.1 Consent to Upload

Under the My Health Record system consent model, the consumer grants a standing consent to upload a clinical document to the My Health Record system in the process of registering for a My Health Record. The standing consent is extended to all providers involved in that patient's care.

Although it is expected to be rare in practice, where a patient withdraws consent to the uploading of a clinical document, it is a legal obligation on the organisation to support the ability for the patient to withdraw consent and as a result the organisation shall not upload that document to the My Health Record system. HIPS stores a flag against each patient episode that indicates whether the patient has withdrawn consent to upload documents for that episode.

HIPS provides a web service method "RecordConsent" that can be used in two situations:

1   Withdrawal of Consent: When the patient has advised the provider that he/she does not want the document to be uploaded.

2   Rescind Withdrawal: when such a withdrawal of consent was recorded in error or the patient has changed their mind.

Whenever a clinical system requests to upload or supersede a clinical document, HIPS will first check the flag for the episode to which the clinical document relates, to find whether consent has been withdrawn. If consent has been withdrawn, then HIPS will refuse to upload the document.

A provider is not obliged to allow their patient to withdraw consent after a document has been uploaded to the My Health Record System. So long as the first version was uploaded while the consumer was consenting, then any later versions of that document can and should be uploaded. The provider faces a choice, if a patient wants to withdraw consent after a document is uploaded, which is either:

- to refuse the withdrawal of consent, advising that the consumer can remove the document, but leave the document uploaded so that it can be amended by later corrections, or

- to remove the document and record the withdrawal of consent to ensure that it is not uploaded again.

However, if the consumer withdrew consent before the document was uploaded, and the information was not entered into the system in time, so the document was uploaded, then the provider has an obligation to first remove the document from the My Health Record system and then enter the withdrawal of consent to prevent it being uploaded again.

2.2.6.2 Participation Status

In most cases when a patient has registered for a My Health Record, HIPS will find out that the My Health Record exists when it calls the My Health Record system B2B Gateway method "doesPCEHRExist". At a minimum, this call is triggered once at the creation of an episode of care.

However, for those rare cases when a patient has chosen to hide the existence of his/her My Health Record, but the patient wishes the provider organisation to upload the document despite this, HIPS provides a web service method "RecordDisclosure". This service can be used in two situations:

1   Disclose My Health Record: when the patient has advised the provider organisation of the existence of his/her My Health Record (and by inference, consented to have his/her document uploaded), even though the My Health Record is not advertised (or may later become not advertised).

2   Rescind Disclosure: when such a disclosure was recorded in error.

HIPS will record the disclosure for each patient at each health provider organisation (HPO). If a Participating Organisation using HIPS consists of multiple HPOs, then the patient's disclosure to one HPO will not automatically apply to that patient at any other HPO unless the functionality to disclose to the root facility is employed.

When a clinical system requests the participation status for a certain patient via web service method "GetPatientParticipationStatus", or requests a list of patients who have changed participation status since a certain date via method "GetRecentPatientParticipationStatus", then HIPS will indicate that the patient is participating in My Health Record System if the patient has disclosed the existence of a My Health Record to the health provider organisation, otherwise it will indicate whether the existence of the My Health Record is currently advertised or not.

2.2.6.3 Refresh Participation Status

HIPS was designed to store the My Health Record advertised and disclosed statuses, for a patient, separately for each healthcare provider organisation, to support the consumer's right to choose which organisations have access to their My Health Record. Some Participating Organisations require that disclosure is stored once for each patient across the entire Participating Organisation, even when they have multiple facilities with separate HPI-O's.

The RefreshPatientParticipationStatus service operation combines the My Health Record advertised and disclosed lookup for different facilities and refreshes the advertised status from the My Health Record System. The following logic is performed when the method is called:

- Retrieves information about the current facility and the disclosure facility. If no disclosure facility is provided, then the current facility will be used as the disclosure facility.
    - o   If either of the facilities cannot be found, then throw an "ItemNotFoundException" with the "ItemType" set to "Hospital"

- Retrieve the patient information from the current facility including the MRN and State Patient ID.

  o If the patient is not found, then throw an "ItemNotFoundException" with the "ItemType" set to "Patient".

- Look up the current disclosure status of the patient at the disclosure facility.

- Validate the patient's IHI.

  o If the response from the HI Service is "HiServiceError" then throw a "HiServiceException"

  o If the response is "PcehrServiceError" then throw a "PcehrServiceException"

  o If the response is not OK then throw a "HipsResponseException"

  o If the response is OK then check the local IHI information. If this is not valid then throw a "InvalidIhiException"

- If the "ForceRefresh" parameter is set to "Never" then return the patient participation status without refreshing the My Health Record status.

- If the "ForceRefresh" parameter is set to "WhenNotAdvertised", and either the advertised or disclosed status of the patient is true, then return the patient participation status without refreshing the My Health Record status.

- Otherwise call the "DoesPcehrExist" method to refresh the My Health Record advertised status.

  o If the response is not OK then a "PcehrServiceException" will be thrown.

2.2.7   Upload or Supersede Document to My Health Record System

This service implements a "fire and forget" pattern that adds a document instance to the queue for uploading to the My Health Record. The service will return as soon as the item is added to the queue.

2.2.7.1   Patient Matching

The patientIdentifier parameter is used to look up a patient record. If the patient identifier is of type Mrn, StatePatientId or PatientMasterId then the patient must already exist in the HIPS Core database, otherwise an "InvalidPatient" error will be returned. However, if the patient identifier is of type ValidatedIhi, then the patient need not exist in the HIPS Core database; if they do not exist, a minimal stub record will automatically be created.

2.2.7.2   IHI Validation

If the IHI has an unresolved data-quality alert, then an "UnresolvedIhiAlert" error will be returned and the document will not be placed on the queue for upload.

If the IHI was last validated more than the configured period of time in the past, the IHI will be revalidated with the HI Service. If validation returns no records found with the IHI and the stored demographic information, an "InvalidIhi" error will be returned and the document will not be placed on the queue for upload. However, if the HI Service is unavailable then the document will be placed on the queue with a stale IHI, which will be revalidated when the item is taken off the queue to be processed.

Each time an upload operation is taken off the queue to be processed, HIPS will check that the IHI was validated within the configured period. If there is an outage that stops the upload for longer

than the configured period, then HIPS will automatically revalidate the IHI before attempting the upload again.

This has a critical impact on implementations where HIPS is not connected to the HI Service. Without a connection to the HI Service, HIPS cannot upload a document after it remains on the queue beyond the configured period. Therefore, the configured period should be long enough that HIPS will not need to revalidate the IHI. Otherwise, documents will fail to upload and need to be resent with a newly validated IHI.

2.2.7.3 Document Validation

HIPS will not run a full CDA validation on documents before uploading them to the My Health Record System, because that would duplicate the work that the My Health Record System does itself. If documents fail validation that implies there is a deficiency in the software that generated the CDA document. The document should be resent from the source system after the deficiency has been corrected.

HIPS will extract and validate the following items from the document:

- The Document Type is extracted from the <code> element. The code must match to a code that is configured in the DocumentType table. Each document type is associated with a repository. HIPS will connect to the associated repository (My Health Record System) for uploading and removing documents.

- The Document ID is extracted from the <id> element. The root must be an OID or a UUID. The extension must be numeric and is optional for OID. Extension is NOT supported for UUID. Note that the My Health Record System requires that the root is unique, so when using an extension to show a user-friendly numeric ID, it is necessary to repeat the extension inside the root.

- The Set ID is extracted from the <setId> element. The root must be an OID or a UUID. The extension is optional. Although the Set ID is optional in some CDA implementation guides, it is mandatory for HIPS.

- The IHI is extracted from the <id> element whose assigningAuthorityName is "IHI". The IHI must match the IHI assigned to the patient in the HIPS database, otherwise an "InvalidIhi" error is returned and the document is not uploaded.

If the CDA document is not valid XML, or HIPS is unable to extract any of these items, an "InvalidDocument" error is returned. There is one exception to this; HIPS will fail document upload queue operations with a validation error if a partial date or a date with fractional seconds is found in the creationTime, serviceStartTime and serviceStopTime metadata in upload requests prior to sending the request to the My Health Record.

2.2.7.4 Document Format Codes (Template Package IDs)

The document format code, also known as a template package ID, is used to specify which validation rules the My Health Record System will apply to the document when it is uploaded. There is a different format code for each conformance level of each document type. Also, as the My Health Record System is upgraded over time, there are new document format codes that can be used. These new format codes allow for changes to be made in the document validation rules over time, without affecting systems that upload documents developed under the older rules.

Each of the document format codes that HIPS will use for uploading documents must be configured in the DocumentFormat table. If the specified format code is not found in the DocumentFormat table, an "InvalidDocument" error is returned.

For Participating Organisations that upload only one conformance level of one document type, there is no need to include the parameter "documentFormatCode". When this parameter is omitted or null, HIPS will use the format code that is configured as "DefaultDocumentFormatCode" in the web.config file. Otherwise, specify the format code in the parameter "documentFormatCode" of each upload request.

The HPI-I Relaxed templates are restricted to Participating Organisations who have been granted permission from the My Health Record System operator, for the document author's identifier to be a local system identifier instead of an HPI-I. This permission may be time-limited, after which Participating Organisations will need to transition to the HPI-I Enforced templates.

The following format codes and document types are supported in HIPS by default:

Document Type	Version	HPI-I	Conformance Level	Document Format Code
Discharge Summary	R2	Relaxed	1A	1.2.36.1.2001.1006.1.20000.12
			1B	1.2.36.1.2001.1006.1.20000.9
			2	1.2.36.1.2001.1006.1.20000.10
			3A	1.2.36.1.2001.1006.1.20000.11
	R3	Relaxed	1A	1.2.36.1.2001.1006.1.20000.13
			1B	1.2.36.1.2001.1006.1.20000.14
			2	1.2.36.1.2001.1006.1.20000.15
			3A	1.2.36.1.2001.1006.1.20000.16
			3B	1.2.36.1.2001.1006.1.20000.17
	R4	Relaxed	1A	1.2.36.1.2001.1006.1.20000.18
			1B	1.2.36.1.2001.1006.1.20000.19
			2	1.2.36.1.2001.1006.1.20000.20
			3A	1.2.36.1.2001.1006.1.20000.21
			3B	1.2.36.1.2001.1006.1.20000.22
		Enforced	1A	1.2.36.1.2001.1006.1.20000.23
			1B	1.2.36.1.2001.1006.1.20000.24
			2	1.2.36.1.2001.1006.1.20000.25
			3A	1.2.36.1.2001.1006.1.20000.26
			3B	1.2.36.1.2001.1006.1.20000.27
My Health Record System Prescription Record	R4	Relaxed	3A	1.2.36.1.2001.1006.1.170.2
		Enforced	3A	1.2.36.1.2001.1006.1.170.3
My Health Record System Dispense Record	R4	Relaxed	3A	1.2.36.1.2001.1006.1.171.2
		Enforced	3A	1.2.36.1.2001.1006.1.171.3
Event Summary	R4	Relaxed	3A	1.2.36.1.2001.1006.1.16473.9
			3B	1.2.36.1.2001.1006.1.16473.8
		Enforced	3A	1.2.36.1.2001.1006.1.16473.10
			3B	1.2.36.1.2001.1006.1.16473.11
Shared Health Summary	R4	Relaxed	3A	1.2.36.1.2001.1006.1.16575.4

Document Type	Version	HPI-I	Conformance Level	Document Format Code
			3B	1.2.36.1.2001.1006.1.16575.5
		Enforced	3A	1.2.36.1.2001.1006.1.16575.6
			3B	1.2.36.1.2001.1006.1.16575.7
Specialist Letter	R4	Relaxed	1A	1.2.36.1.2001.1006.1.16615.13
			1B	1.2.36.1.2001.1006.1.16615.14
			2	1.2.36.1.2001.1006.1.16615.15
			3A	1.2.36.1.2001.1006.1.16615.16
			3B	1.2.36.1.2001.1006.1.16615.17
		Enforced	1A	1.2.36.1.2001.1006.1.16615.18
			1B	1.2.36.1.2001.1006.1.16615.19
			2	1.2.36.1.2001.1006.1.16615.20
	R4	Enforced	3A	1.2.36.1.2001.1006.1.16615.21
			3B	1.2.36.1.2001.1006.1.16615.22
	R5	Relaxed	1A	1.2.36.1.2001.1006.1.16615.23
			1B	1.2.36.1.2001.1006.1.16615.24
			2	1.2.36.1.2001.1006.1.16615.25
			3A	1.2.36.1.2001.1006.1.16615.26
			3B	1.2.36.1.2001.1006.1.16615.27
		Enforced	1A	1.2.36.1.2001.1006.1.16615.28
			1B	1.2.36.1.2001.1006.1.16615.29
			2	1.2.36.1.2001.1006.1.16615.30
			3A	1.2.36.1.2001.1006.1.16615.31
			3B	1.2.36.1.2001.1006.1.16615.32
Pathology Report	R5	Relaxed	3A	1.2.36.1.2001.1006.1.220.1
		Enforced	3A	1.2.36.1.2001.1006.1.220.2
Diagnostic Imaging Report	R5	Relaxed	3A	1.2.36.1.2001.1006.1.222.1
		Enforced	3A	1.2.36.1.2001.1006.1.222.2

2.2.7.5   Episode Matching

Every clinical document uploaded by HIPS must be attached to an episode, which can be a stub record or an inpatient admission, an emergency visit, an outpatient appointment or another type configured in the EpisodeType table in the HIPS Core database.

There are two ways to create and manage episodes. One is by sending HL7 messages (such as A01 or A08) to the HIPS PAS Loader, while the other is to use the ValidatedIhi type of patient identifier and allow HIPS to create and manage episode stub records for uploaded documents.

HIPS will look for a previous episode stub for the upload of a document with the same Set ID as this document instance. If one is found, then this episode stub is used and updated to the given admission date/time. Otherwise, the date and time provided in the "admissionDate" parameter are used to match an Episode record.

If there is no episode matched by Set ID, and there is more than one episode within one minute of the given date/time, then a Multiple Episode stub episode will be created. The Multiple Episode stub episode will have withdrawn consent if any of the episodes within one minute of the given date/time had withdrawn consent.

If there is no episode matched by Set ID, and no episode within 1 minute of the given date/time, and the patient identifier is of type ValidatedIhi, then a Validated IHI stub episode will be created.

Both types of stub record have the document Set ID as their source system episode ID, so that future supersedes and removals of this document can proceed even if the relevant date/time has since changed.

For other patient identifier types, if there is no episode matched, then an "InvalidEpisode" error will be returned.

2.2.7.6   Consent Checking

The ability to handle a patient's withdrawal of consent is a core requirement for Clinical Information Systems connecting to the My Health Record System. Participating Organisations using HIPS can make use of the HIPS consent management services or ignore this functionality and handle consent in other systems. In line with the My Health Record System consent model, when an episode is created, the default value for ConsentWithdrawn is false, that the patient has not withdrawn consent to upload documents. This can be changed using the RecordConsent service.

Once an episode is matched, HIPS will check the ConsentWithdrawn flag. If the flag is set to true, this means the patient withdrew consent to upload this document. HIPS will return a "ConsentWithdrawn" error and prevent the upload of the document.

2.2.7.7   Age Checking

Some Participating Organisations may have a policy that they will disable uploading documents for children under a certain age. This age can be configured for each facility in the Hospital table. This feature can also be disabled by setting the value 0.

For consistency, HIPS will calculate the age of the patient at the time of "admissionDate", rather than the time of discharge or the time of the upload.

If the value of "UploadDocumentMinimumAge" configured for the hospital is non-zero, and the patient was under the configured age at the time of "admissionDate", then HIPS will return a "PatientUnderAge" error and the document will not be added to the queue.

2.2.7.8 Attachment Validation

HIPS will ensure that each attachment is under the maximum size for attachments in the My Health Record System (10 megabytes) and that each attachment belongs to one of the supported file types. If either of these checks fails, an "InvalidDocument" error will be returned and the document will not be added to the queue.

The types of attachment files supported by the My Health Record System are:

MIME type	File Extensions	Description
image/gif	.gif	Graphics Interchange Format
image/jpeg	.jpg, .jpeg	Joint Photographic Experts Group
image/tiff	.tif, .tiff	Tagged Image File Format
image/png	.png	Portable Network Graphics
application/pdf	.pdf	Portable Document Format

2.2.7.9 CDA Packaging

An electronic signature is created for the CDA document. The signature asserts the author's name and either the author's local system identifier or HPI-I that is extracted from the CDA document. The signature is created using the NASH certificate for the HPI-O that is in use by the hospital. This certificate has the serial number indicated by the HpoCertSerial value in the HealthProviderOrganisation record in the database.

An "InvalidDocument" error is returned if these elements cannot be extracted from the CDA document, or the logo exceeds the maximum dimensions of 400 x 100 pixels.

An XDM package (ZIP file) is created, consisting of:

- The XML provided in the cdaDocument parameter as CDA_ROOT.XML. The XML is unchanged except that integrity check attributes are added to the logo reference if HIPS is including an organisational logo from the facility configuration.

- The created electronic signature as CDA_SIGN.XML.

- If a logo file is configured for the facility, and not provided as an attachment, the logo file from the facility configuration is included with the file name specified in the document.

- Any additional attachments provided in the attachments parameter.

After the consent check, signing and packaging, the upload request is added to the upload queue and the service returns to the caller. After the service has returned, the status of the document upload may be determined using the GetQueuedOperations method.

2.2.7.10 NASH Certificate Validation

HIPS Core supports the separate configuration of NASH organisation certificates for digital signing of clinical documents and for connecting to the My Health Record system.

Validation of the configured signing NASH certificate by HIPS is performed prior to signing any package. The certificate used for signing is firstly checked that is a NASH certificate and that it belongs to the authoring organisation.

2.2.7.11 Cancellation of a Queued Upload Operation

It may be necessary to manually cancel a queued upload operation, if the My Health Record System returns an error message that is documented to have the meaning of system temporarily unavailable, but is actually due to an error in the structure of the uploaded document or metadata. This can be done by setting the message state in the MessageQueue record to 3 (failed).

Each time an upload operation is taken off the queue for processing, HIPS checks the current value of the MessageQueueStateID in the MessageQueue record. If the message state is no longer set to 1 (pending) then HIPS will stop processing this upload operation, and the queue processor will move to the next message in the queue.

2.2.7.12 Ordering of Queued Operations

If the My Health Record System is temporarily unavailable, the queued upload operation will be placed on a retry queue. The delay between retries and the number of retries are configured when installing the HIPS Queue Consumer.

While one or more operations are on the retry queue, other upload requests can arrive. HIPS will attempt to process these operations immediately as the My Health Record System may now have sufficient capacity to process these requests.

However, it is important to ensure that requests that relate to the same document set are processed in the correct order. Therefore, before an upload operation is taken off the queue for processing, HIPS checks whether there are any earlier pending operations for the same document set. If there are, then HIPS will not proceed to process the current operation until after any earlier operations are completed.

2.2.7.13 Determination of Request Type

When an upload operation is taken off the queue for processing, the Set ID and Document ID are used to locate existing records in the database that related to the document that is being uploaded.

If the Document ID exists in the ClinicalDocumentVersion table, then the queued operation will be marked as failed because the document has already been uploaded. HIPS will not attempt to upload the document again.

If the Document ID does not exist, but the Set ID exists in the ClinicalDocument table, then a request is generated with the type of replacement (supersede) of the most recently uploaded Document ID in the ClinicalDocumentVersion table that is recorded against the matched record in the ClinicalDocument table. This is the mechanism by which HIPS ensures that it only replaces documents that it uploaded itself.

If neither the Document ID nor the Set ID exists in the database, then the request type is an upload of a new document.

2.2.7.14 Auditing of System Interactions, Request and Response

HIPS will upload or supersede the clinical document to the My Health Record System and write an audit record into the PcehrAudit table. For all failed interactions with the HI Service and My Health Record system, and also for successful interactions where configured to do so in the SystemInteractionLogConfiguration table, HIPS will also write an entry to the SystemInteractionLog table containing the full SOAP request and response, which is vital for troubleshooting when documents have failed to upload.

2.2.7.15 Response Classification

Using the configured classifications in the PcehrErrorCode table, which are based on the definitions of the My Health Record System error messages in the Technical Service Specification, each response from the My Health Record System is classified as one of:

- Success

- Warning (e.g. operation successful but persisted as unstructured document)

- Duplicate Document ID

- System Temporarily Unavailable

- Unrecoverable Error.

In the case of a success, warning or duplicate document ID message, the queued operation is deleted (unless overridden by the configuration setting "QueueConsumer.RemoveOnSuccess") and records of the document are stored into the ClinicalDocument and ClinicalDocumentVersion tables.

In the My Health Record System model, superseding a document that was removed with reason Withdrawn changes its status back to active; all versions, including the one that was removed, are once again visible to both consumers and providers. Accordingly, in the HIPS ClinicalDocument table the document status will be reset to "Uploaded" (even if it was previously "Removed"). The removal date and removal reason will be reset to null and -1 (unknown) respectively.

The reason why duplicates are treated the same as success at this point is because the document was missing from the HIPS database even though it was already on the My Health Record System. This can happen in the case when the HIPS database is restored from backups following the disaster recovery process, and documents that were uploaded after the recovery point are resent to ensure they are recorded correctly in the restored HIPS database.

In the case of a message classified as System Temporarily Unavailable, HIPS will retry the upload operation as described previously.

In the case of an unrecoverable error, such as an invalid document structure, the queued operation is marked as failed, and the queue processor will move to the next message in the queue.

2.2.8   Upload or Supersede Discharge Summary Level 1A

2.2.8.1   Description

This service is used specifically to upload a Level 1A Compliant Discharge Summary to the My Health Record System. Level 1A documents can also be uploaded using the main Upload or Supersede web service; however, this is specific to Level 1A documents as it does not require a CDA document format to be pre-created and passed to the web service. It simply requires some specific metadata (for the CDA header) and the PDF attachment, which the service is then able to create the CDA document and then upload to the My Health Record System.

The facility, HPO and associated signing certificates must be fully configured within HIPS for this process to occur without errors. This includes the validation of configured signing NASH certificate.

When the returned object from the request (UploadDischargeSummaryLevel1AResponse) has a success response this indicates that the message has successfully passed validation and has been placed in the HIPS MHR Operation queue waiting to be uploaded to the My Health Record System, but it does not mean that the document has yet been successfully uploaded to the My

Health Record System. The HIPS message queue status can be queried using the *GetQueuedOperation*, *GetQueuedOperations* and *SearchQueuedOperations* web services.

2.2.8.2   Business Rules/Functional Business Logic

1   The *Hospital*, *HospitalPatient*, and *PatientMaster* records for the provided *PatientIdentifier* are resolved using a mechanism appropriate to the provided *PatientIdentifier* type.

2   A patient requires a *PatientMasterIhi* with a current and verified IHI.

If an IHI is not present, or is found to be invalid for any reason, the upload is not performed and an error is returned.

If an IHI is present but out of date an attempt to revalidate it via the HI Service is performed. Upload will continue if this revalidation verifies the IHI. However, if the revalidation indicates the IHI is invalid then the upload is not performed.

3   The *Episode* is resolved by finding Episode records matching the resolved *HospitalPatient* and provided *AdmissionDate*. *Episodes* will be found if they are the only *Episode* for the *HospitalPatient* within a set tolerance of 1 minute of the provided *AdmissionDate*. *Episodes* will also only be found if they do not have a cancelled *EpisodeLifecycle*. Relevant logic for handling multiple episode stub episodes and Validated IHI stub episodes is covered in 2.2.7.5 Episode Matching.

4   The *DocumentId* and *DocumentSetId* are generated internally by HIPS and used for the CDA document. These are sequentially generated numbers from the *CDASetNumber* and *CDADocumentNumber* tables.

5   The *CDASetNumber* table contains an auto-generated, sequentially increasing, *DocumentSetId* number with the related *EpisodeId*, *AdmissionDateTime*, *DischargeDateTime*, *ModeOfSeparation, DocumentFormat,* and *DocumentType* code.

The *CDADocumentNumber* table contains an auto-generated, sequentially increasing, *DocumentId* number with the related *DocumentCreationDateTime* and *CDASetNumber* record.

6   If the *Episode* does not already have a *ClinicalDocument* record, then the *DocumentSetId* is auto generated as the next *DocumentSetId* available. The *DocumentId* is also auto generated as the next *DocumentId* available.

7   If the *Episode* already has a *ClinicalDocument* record for an eDischarge Summary, then the *DocumentSetId* will be set to the same value as the previously created *ClinicalDocument*.

   a   If the *DocumentCreationDateTime*, *AdmissionDateTime*, *DischargeDateTime*, and *ModeOfSeparation* is the same as another record for the same *DocumentSetId* then this would indicate that the same document was attempting to be uploaded again. In this case an error will be returned to the user specifying that the same document is attempting to be uploaded.

   b   If the *DocumentCreationDateTime*, *AdmissionDateTime*, *DischargeDateTime*, and *ModeOfSeparation* is not the same as another record for the same *DocumentSetId* then the *DocumentId* will be auto generated as the next *DocumentId* available.

8   The *PatientIdentifier* may be of type *Mrn*, *PatientMasterId*, *StatePatientId* or *ValidatedIhi*. The *PatientIdentifier Demographic* type will not be resolved and if used will return an error.

9   As it is suggested that the *HL7 DatabaseLoader* is used to gather the patient information within HIPS for a 1A upload, but not essential, then the *PatientIdentifier* is best utilised as the *Mrn*, or *StatePatientId* (if one is used). If the *ValidatedIhi* is used then the *PatientAddress*

and the *PatientContactDetails* will become mandatory as they are required information for a Level 1A Compliant Discharge Summary upload to the My Health Record System.

10   The *ParticipatingProvider* with the *CdaHeaderMetadata* object has a conditional mandatory rule over the *LocalIdentifer* and *Hpii* attributes as at least one must be populated or else an error will be returned. If both of the *LocalIdentifer* and *Hpii* attributes are added, then the *Hpii* will be selected over the *LocalIdentifer*.

11   The *CdaHeaderMetadata* object has *DischargeDateTime* and *DischargeDate*. Only one of these can be provided or else an error will be returned.

2.2.9   Upload or Remove Pathology Report

2.2.9.1   Description

The UploadOrRemovePathology operation on the PathologyImagingService service is used to upload a Pathology Report to the My Health Record system or remove a previously uploaded Pathology Report. This service is designed to accept report messages from a LIS via a SOAP or MLLP message broker. This message broker should transform the messages to comply with the format expected by HIPS. The HIPS web service accepts an HL7 ORU Message and the PDF attachment, which the service then uses to create the CDA document and upload to the My Health Record system. Refer to the document *HIPS – Pathology Results HL7v2 Profile* for details of the accepted HL7 message format.

The healthcare provider organisation creating and uploading the reports and their associated NASH PKI certificate must be configured within HIPS for this process to occur without errors.

When the returned object from the web service (UploadOrRemovePathologyResponse) has a success response this indicates that the message has successfully passed validation and has been placed in the HIPS message queue waiting to be uploaded to or removed from the My Health Record system. It does not mean that the document has yet been successfully uploaded to or removed from the My Health Record System. The HIPS message queue status can be queried using the *GetQueuedOperation*, *GetQueuedOperations* and *SearchQueuedOperations* web services. When complete, the queue consumer will return a separate acknowledgement HL7 message, including the Message Control ID of the initial message and the outcome of the operation, and any error codes returned by the My Health Record system.

2.2.9.2   Business Rules/Functional Business Logic

1   Invokes the SendPathologyRequest method providing the parsed HL7 message and optionally the report PDF as an array of bytes or a file location.

2   The Patient Identifiers are extracted from the PID segment, validated and stored.

 a   If the patient's indigenous status, given or family name is not provided, HIPS will return a validation error.

3   If the Result Status is 'X' for all OBR segments, the document is removed from the My Health Record rather than uploaded.

 a   HIPS will look up the Episode corresponding to all Filler Order Numbers in the incoming message.

 b   If no episodes are found, it returns "No results in this message have been uploaded. There is no document to be removed from the My Health Record."

  c If more than one episode is found, it returns "Results in this message were uploaded as separate documents. The documents must be removed from the My Health Record separately."

  d Otherwise, there is only one distinct episode, so HIPS will look up the CDA set ID for the document uploaded under this episode, and then enqueues the removal operation and returns.

4 If BypassHIService is true, then the message must have an IHI and an HPI-I, unless the organisation has an HPI-I exemption, in which case HPI-I can be omitted. The supplied IHI and HPI-I are assumed valid and stored. If the IHI is already stored on a different patient record in the same facility, a duplicate IHI alert is raised.

5 If BypassHIService is false, the Patient's IHI is obtained or validated using the HI Service and stored. If the patient is an existing patient and a demographic update was made the patient's IHI will be revalidated. If the IHI was last validated outside the configured period, HIPS will validate the IHI with the HI Service using the details provided and store the validation date/time and resulting status. If the demographics used to find the IHI match a different patient record in the same facility, a duplicate patient alert is raised. If the IHI is already stored on a different patient record in the same facility, a duplicate IHI alert is raised.

6 If a duplicate IHI alert or a duplicate patient alert is raised and the configuration option "Ihi.AllowMHRAccessForDuplicates" is false then the document is not uploaded, and a negative acknowledgement is sent.

7 If the Filler Field 1 contains AUSEHR, HIPS will use the value of this key to determine whether a My Health Record exists for the patient and so it will not invoke the DoesPCEHRExist service. If the value is AUSEHR=Y then HIPS will continue with the upload process, otherwise HIPS will reject the message and send a negative acknowledgement.

8 If the Filler Field 1 does not contain an AUSEHR key, and no version of this report has been uploaded before, and DoesPCEHRExist was not invoked for this patient within the configured "PcehrExistsReuseIntervalMinutes" period, HIPS will invoke the DoesPCEHRExist service to retrieve the advertised status of the patient's My Health Record. If the patient's My Health Record is not advertised or disclosed the document is not uploaded and a negative acknowledgement is sent.

9 HIPS will check the principal result interpreter field of each OBR record for the document author.

  a If the assigning authority is "AUSHIC" then HIPS will look up and store the HPI-I. If the name has changed or the HPI-I was last validated outside the configured period, and BypassHIService is false, HIPS will validate the HPI-I with the HI Service using the details provided and store the validation date/time and resulting status.

  b All other assigning authorities will be treated as local identifiers.

    i If the assigning authority is "AUSHICPR" then skip to step iii.

    ii Otherwise check that the assigning authority is a valid facility within HIPS.

    iii Search the hips.HospitalHealthProviderIndividual table with the IDnumberST of the CN for a matching local identifier.

    iv If no match is found, and the facility is configured for HPI-I exemption, and an OID is configured for the assigning authority code in the CodeSystem table, HIPS will populate the local identifier for the document author / responsible pathologist.

<ol type="a" start="22">

v   If no match is found, and the facility is not configured for HPI-I exemption, then reject the message and send a negative acknowledgment with the reason for rejection.

vi   If a match is found, then retrieve the HPI-I for the individual.

vii   Check the deactivated date on the HPI-I and if the observation date time in the OBR record is after the deactivated date then reject the message and send a negative acknowledgement with the reason for rejection.

viii   Check the last validated date on the HPI-I and if it is outside of the validity period then invoke ValidateHpii to confirm its validity.

ix   If the "BypassHIService" setting is set to true and no HPI-I has been provided, and the facility is not configured for HPI-I exemption, then reject the message and do not attempt to upload the report.

c   Return the list of document authors

10   Create a *CdaHeaderMetaData* object and populate it with the required CDA header information.

11   Create an *OrderDetails* object and populate it with the order details of the OBR section of the HL7 message.

12   Create a list of *PathologyTestResult* where each test result is created from an OBR and its corresponding OBX.

13   A CdaDocumentDetails object is created using the CdaHeaderMetaData, the patient's primary identifier, OrderDetails, pathologyTestResult list and the patient's secondary identifier is used as the requesting hospital MRN.

14   Upload or Supersede the Document to the My Health Record System.

2.2.9.3   Avoiding Excessive Revalidation of HPI-Is

HIPS dynamically stores each HPI-I that it receives via HL7v2 message, and the HPI-I status that it obtains the first time each HPI-I is validated.

This reduces the response time for all HI service users by not re-validating an HPI-I every time HIPS receives H7v2 ORU messages. In other words, it stops an HI Service overload by caching the HPI-Is.

Revalidation of the HPI-I against the HI Service is done if the HPI-I validation period has expired or a name change has been detected against the stored Health Provider Individual details for that HPI-I.

2.2.9.4   Narrative Support for Multiple Document Authors

The CDA Document Library supports the narrative to allow the multiple author upload. The support for the narrative for multiple authors is integrated into CDA Document Library.

2.2.9.5   Test Result Mapping

The Mapping specification for first and second set of three components in the OBR-4 segment is as follows:

- The HIPS service shall populate the first three components of OBR-4 test result name in the CDA document as a translation of the code where possible.

- The HIPS service shall populate the second three components of OBR-4 test result name in the CDA document as a code where possible, otherwise as free text.

HIPS Core shall extract the OBR details from an HL7v2 message in the following process:

- Extract the first three components and assign them to the translation code of the Test Result object.

- Extract the second three components and assign them to the primary code of the Test Result object.

- If only the first three components have been passed in, then make these the primary code of the Test Result object.

2.2.10 Upload or Remove Diagnostic Imaging Report

2.2.10.1 Description

The UploadOrRemoveImaging operation of the PathologyImagingService service is used to upload a Diagnostic Imaging Report to the My Health Record system or remove a previously uploaded report. This service is designed to accept messages from a RIS via a SOAP or MLLP message broker. This message broker should transform the messages to comply with the format expected by HIPS. The HIPS method accepts an HL7 ORU Message and the PDF attachment, which the service then validates to create the CDA document and upload to the My Health Record System. Refer to the document *HIPS – Diagnostic Imaging Results HL7v2 Profile* for details of the accepted HL7 message format.

The healthcare provider organisation creating and uploading the reports and the associated NASH PKI certificate must be configured within HIPS for this process to occur without errors.

When the service returns a successful UploadOrRemoveImagingResponse this indicates that the message has successfully passed validation and has been placed in the HIPS message queue waiting to be uploaded to or removed from the My Health Record system. It does not mean that the document has yet been successfully uploaded to or removed from the My Health Record system. The HIPS message queue status can be queried using the *GetQueuedOperation*, *GetQueuedOperations* and *SearchQueuedOperations* web services. The HIPS queue consumer will send a separate acknowledgement message with the Message Control ID of the original message and the outcome of the operation, including any error codes returned from the My Health Record system.

2.2.10.2 Business Rules/Functional Business Logic

1   Invokes the SendImagingRequest method providing the parsed HL7 message and optionally the report PDF as a byte array or file location.

2   The Patient Identifiers are extracted from the PID segment, validated and stored.

    a   If the patient's race, given or family name is not provided, HIPS will return a validation error.

3   If the Result Status is 'X' for all OBR segments the document is removed from the My Health Record rather than uploaded.

    a   HIPS looks up the Episode corresponding to all Filler Order Numbers in the incoming message.

    b   If no episodes are found, it returns "No results in this message have been uploaded. There is no document to be removed from the My Health Record."

    c   If more than one episode is found, it returns "Results in this message were uploaded as separate documents. The documents must be removed from the My Health Record separately."

    d   Otherwise, there is only one distinct episode, so HIPS will look up the CDA set ID for the diagnostic imaging report uploaded under this episode, then enqueue the removal operation and return.

4   If BypassHIService is true, then the message must have an IHI and an HPI-I, unless the organisation has an HPI-I exemption, in which case HPI-I can be omitted. The supplied IHI and HPI-I are assumed valid and stored. If the IHI is already stored on a different patient record in the same facility, a duplicate IHI alert is raised.

5   If BypassHIService is false, the Patient's IHI is obtained or validated using the HI Service and stored. If the patient is an existing patient and a demographic update was made, or if the IHI was last validated outside the configured period, HIPS will validate the IHI with the HI Service using the details provided and store the validation date/time and resulting status. If the demographics used to find the IHI match a different patient record in the same facility, a duplicate patient alert is raised. If the same IHI is already assigned to a different patient record in the same facility, a duplicate IHI alert is raised.

6   If a duplicate IHI alert or duplicate patient alert is raised and the configuration option "Ihi.AllowMHRAccessForDuplicates" is false then the document is not uploaded, and a negative acknowledgement is sent.

7   If the Filler Field 1 contains AUSEHR, HIPS will use the value of this key to determine whether a My Health Record exists for the patient and so it will not invoke the DoesPCEHRExist service. If the value is AUSEHR=Y then HIPS will continue with the upload process, otherwise HIPS will reject the message.

8   If the Filler Field 1 does not contain an AUSEHR key, and no version of this report has been uploaded before, and DoesPCEHRExist was not invoked for this patient within the configured "PcehrExistsReuseIntervalMinutes" period, the DoesPCEHRExist service is invoked to retrieve the advertised or disclosed status of the patient's My Health Record. If the patient's My Health Record is not advertised or disclosed the document is not uploaded.

9   Check the principal result interpreter field of each OBR record for the document author.

    a   If the assigning authority is "AUSHIC" then HIPS will look up and store the HPI-I. If the name has changed or the HPI-I was last validated outside the configured period, and BypassHIService is false, HIPS will validate the HPI-I with the HI Service using the details provided and store the validation date/time and resulting status.

    b   All other assigning authorities we will be treated as local lookups.

        i   If the assigning authority is "AUSHICPR" then skip to step iii.

        ii   Otherwise check that the assigning authority is a valid facility within HIPS.

        iii   Search the hips.HospitalHealthProviderIndividual table with the IDnumberST of the CN for a matching local identifier.

        iv   If no match is found, and the facility is configured for HPI-I exemption, and an OID is configured for the assigning authority code in the CodeSystem table, HIPS will populate the local identifier for the document author / responsible radiologist.

        v   Otherwise if no match is found HIPS will reject the message and send a negative acknowledgment with the reason for rejection.

> vi   If a match is found then retrieve the HPI-I for the individual.
>
> vii Check the deactivated date on the HPI-I and if the observation date time in the OBR record is after the deactivated date then reject the message and send a negative acknowledgement with the reason for rejection.
>
> viii Check the last validated date on the HPI-I and if it is outside of the validity period then invoke ValidateHpii to confirm its validity.
>
> ix   If the "BypassHIService" setting is set to true and no HPI-I has been provided, and the facility is not configured for HPI-I exemption, then reject the message and do not attempt to upload the report.
>
> c   Use the providers identified as the list of document authors and responsible radiologists.

10   Create a *CdaHeaderMetaData* object and populate it with the required CDA header information.

11   Create an *OrderDetails* object and populate it with the order details of the OBR section of the HL7 message.

12   Create a list of *ImagingExamResult* where each test result is created from an OBR and its corresponding OBX.

13   A CdaDocumentDetails object is created using the CdaHeaderMetaData, the patient's primary identifier, OrderDetails, imagingExamResult list and the patient's secondary identifier is used as the requesting hospital MRN.

14   Upload or Supersede the Document to the My Health Record System.

2.2.10.3 Avoiding Excessive Revalidation of HPI-Is

HIPS dynamically stores each HPI-I that it receives via HL7 v2 message, and the HPI-I status that it obtains the first time each HPI-I is validated.

This reduces the response time for all HI service users by not re-validating an HPI-I every time HIPS receives H7v2 ORU messages. In other words, it stops an HI Service overload by caching the HPI-Is.

Revalidation of the HPI-I against the HI Service is done if the HPI-I validation period has expired or a name change has been detected against the stored Health Provider Individual details for that HPI-I.

2.2.10.4 Narrative Support for Multiple Document Authors

The CDA Document Library supports the narrative to allow the multiple author upload. The support for the narrative for multiple authors is integrated into CDA Document Library.

2.2.10.5 Test Result Mapping

The Mapping specification for first and second set of three components in the OBR-4 segment is as follows:

- The HIPS service shall populate the first three components of OBR-4 test result name in the CDA document as a translation of the code where possible.

- The HIPS service shall populate the second three components of OBR-4 test result name in the CDA document as a code where possible, otherwise as free text.

HIPS Core shall extract the OBR details from an HL7v2 message in the following process:

- Extract the first three components and assign them to the translation code of the Test Result object.

- Extract the second three components and assign them to the primary code of the Test Result object.

- If only the first three components have been passed in, then make these the primary code of the Test Result object.

2.2.11 Remove Document from My Health Record System

This service implements a "fire and forget" pattern that adds a request to a queue for removing a document from the associated repository for the document type. The service will return as soon as the item is added to the queue.

2.2.11.1 Business Rules/Functional Business Logic

The remove document operation will have identical patient matching, IHI validation and episode matching logic to the upload or supersede document operation.

2.2.11.2 Cancellation of a Queued Remove Operation

It may be necessary to manually cancel a queued remove operation, if the My Health Record System returns an error message that is documented to have the meaning of system temporarily unavailable, but is actually due to an error in the removal request. This can be done by setting the message state in the MessageQueue record to 3 (failed).

Each time a remove operation is taken off the queue for processing, HIPS checks the current value of the MessageQueueStateID in the MessageQueue record. If the message state is no longer set to 1 (pending) then HIPS will stop processing this operation, and the queue processor will move to the next operation in the queue.

2.2.11.3 Ordering of Queued Operations

If the My Health Record System is temporarily unavailable, the queued remove operation will be placed on a retry queue. The delay between retries and the number of retries are configured when installing the HIPS Queue Consumer.

While one or more operations are on the retry queue, other remove requests can arrive. HIPS will attempt to process these operations immediately as the My Health Record System may now have sufficient capacity to process these requests.

However, it is important to ensure that requests that relate to the same document set are processed in the correct order. Therefore, before a remove operation is taken off the queue for processing, HIPS checks whether there are any earlier pending operations for the same document set. If there are, then HIPS will not proceed to process the current operation until after any earlier operations are completed.

2.2.11.4 Auditing of Document Removal

The additional audit information provided in the "auditInformation" parameter will be stored in the RemoveAudit table.

2.2.11.5 Auditing of System Interactions, Request and Response

After sending the remove document request to the My Health Record system, HIPS will write an audit record into the PcehrAudit table. For all failed interactions with the HI Service and My Health Record system, and also for successful interactions where configured to do so in the

SystemInteractionLogConfiguration table, HIPS will also write an entry to the SystemInteractionLog table containing the full SOAP request and response.

2.2.11.6 Response Classification

Using the configured classifications in the PcehrErrorCode table, which are based on the definitions of the My Health Record System error messages in the Technical Service Specification, each response from the My Health Record System remove document operation will be classified as one of:

- Success

- System Temporarily Unavailable

- Unrecoverable Error

In the case of a success message, the queued operation will be deleted (unless overridden by the configuration setting "QueueConsumer.RemoveOnSuccess") and the ClinicalDocument record will be updated. HIPS will set the DocumentStatus to removed, set the RemovalDate to the current time, and set the RemovalReason to the value provided in the "reason" parameter.

In the case of a message classified as System Temporarily Unavailable, HIPS will retry the remove operation as described previously.

In the case of an unrecoverable error, the queued operation is marked as failed, and the queue processor will move to the next message in the queue.

2.2.12 Get Queued Operation

This service is used to return details of a specific Queued Operation based on its unique identifier.

2.2.12.1 Business Rules/Functional Business Logic

This service is intended for system analysis of pending or failed operation requests from the HIPS operational message queue.

2.2.13 Get Queued Operations

This service is used to return the list of Queued Operations, Uploaded Documents and Document Versions for a particular patient for a specific episode.

2.2.13.1 Business Rules/Functional Business Logic

This service is intended for system analysis of pending or failed operation requests from the HIPS operational message queue.

2.2.14 Search Queued Operations

This service is used to return a list of Queued Operations based on the specified criteria.

2.2.14.1 Business Rules/Functional Business Logic

This service is intended as a simplistic list of pending or failed operation requests from the HIPS operational message queue. Results returned can then be used to perform a request on the more detailed service operations described previously for more detailed analysis.

2.2.15 Search for Provider Individual Details - Synchronous

2.2.15.1 Description

This service is used to search for the Provider Details for an individual in a synchronous process. A provider search can be performed as either an identifier search to validate a known HPI-I, or to retrieve the HPI-I using the registration id (for example the AHPRA number) thus verifying the provider or perform a demographic search to find the provider.

2.2.15.2 Business Rules/Functional Business Logic

1   Following a HPI-I number/registration Id or Demographic HPI-I record search, if the HI Service finds a single match to an HPI-I record which is a 'Resolved' duplicate as a status, the HI Service will return information message (WSE0134) and the primary HPI-I record with search criteria details.

2   HpiiIdentifierQuery:

   a   The hpiiNumber and registrationId and number are conditionally mandatory and thus only one of the two items must be provided for a single search.

   b   The hpioNumber is a mandatory requirement and must be provided for auditing requirements.

   c   The familyName is also a mandatory requirement.

   d   The familyName and givenName must not provide invalid characters. Only alpha and numeric characters, apostrophes, full stops and hyphens are acceptable. Spaces are also acceptable but must not appear immediately before or after apostrophes and hyphens.

   e   When searching by registrationId the search will be case sensitive.

3   hpiiDemographicQuery:

   a   The hpioNumber is a mandatory requirement and must be provided for auditing requirements.

   b   The familyName is a mandatory requirement.

   c   The familyName and givenName must not provide invalid characters. Only alpha and numeric characters, apostrophes, full stops and hyphens are acceptable. Spaces are also acceptable but must not appear immediately before or after apostrophes and hyphens.

   d   The dateOfBirth is a mandatory requirement.

   e   The sex is a mandatory requirement.

   f   The australianAddress and internationalAddress are conditionally mandatory and thus only one of the two items must be provided for a single search.

      i   If the australianAddress is provided then the following are mandatory:

         ■ streetName

         ■ suburb

         ■ postcode

         ■ state

      ii   If the internationalAddress is provided then the following is mandatory:

         ■ country

2.2.16 Search for Provider Individual Details – Asynchronous

2.2.16.1 Description

This service is used to search for the Provider Details for an individual in an asynchronous process.

2.2.16.2 Business Rules/Functional Business Logic

1   All rules for the HpiiIdentifierQuery and HpiiDemographicSearch apply for all validation and search requests.

2   HpiiBatchSubmit:

   a   Asynchronous batch searching allows Participating Organisations to perform up to 50 search requests per message. A badlyFormedMsg will be returned in the response file when the batch file size is greater than 50 requests.

3   HpiiBatchRetrieve

   a   The HPI-I Service will only permit the requestor of the HPI-I batch search to retrieve the details of the HPI-I batch search. The HI Service will validate the requestor for the services: and a not authorised error will be returned when the requestor is invalid – error WSE9050.

   b   The HPI-I Service will hold the completed search results for a period of exactly 14 calendar days from the date the batch request has reached a COMPLETED status. The results will be deleted after the timeframe has elapsed for searches when the status of the batch request is 'Completed', 'Retrieved' or 'Error'.

2.2.17 Gain Access to My Health Record

2.2.17.1 Description

This function is used when a health provider organisation (HPO) wants to gain access to an individual's My Health Record for subsequent viewing and/or downloading information from the My Health Record System.

This can be performed:

- With an Access Code

- Without an Access Code, or

- With Emergency Access.

A call to the "IsPcehrAdvertised" method described in this guide will return the following information about whether an access code is required for the individual's My Health Record:

- Null – thus meaning that the individual has not registered for My Health Record, or has chosen to hide the existence of his/her My Health Record. The individual may give advice of My Health Record existence and may or may not provide an access code.

- With Code – thus meaning that a code must be provided to gain access.

- Without Code – thus meaning that access is open and no Record Access Code is required. The patient may advise of a Limited Document Access Code to grant restricted access.

- Access Granted – thus meaning that access has been granted and no code is required unless the patient advises of a change to access level and provides an access code.

As an individual can change their access at any time and so a call to the "IsPcehrAdvertised" method should be performed before each call to the gain access function.

NOTE: The "AccessCodeRequired" for an individual is stored in the HIPS "HealthProviderOrganisationPatient" table after "IsPcehrAdvertised" has been called. However, since this is a transactional system and other calls may already be updating the "AccessCodeRequired" in another thread, it is essential that a call to the "IsPcehrAdvertised" is performed to ensure the current state of "AccessCodeRequired" is understood.

2.2.17.2 Business Rules/Functional Business Logic

The following business rules have been derived from the Australian Digital Health Agency diagram entitled "Accessing & Viewing the PCEHR", and reproduced below:
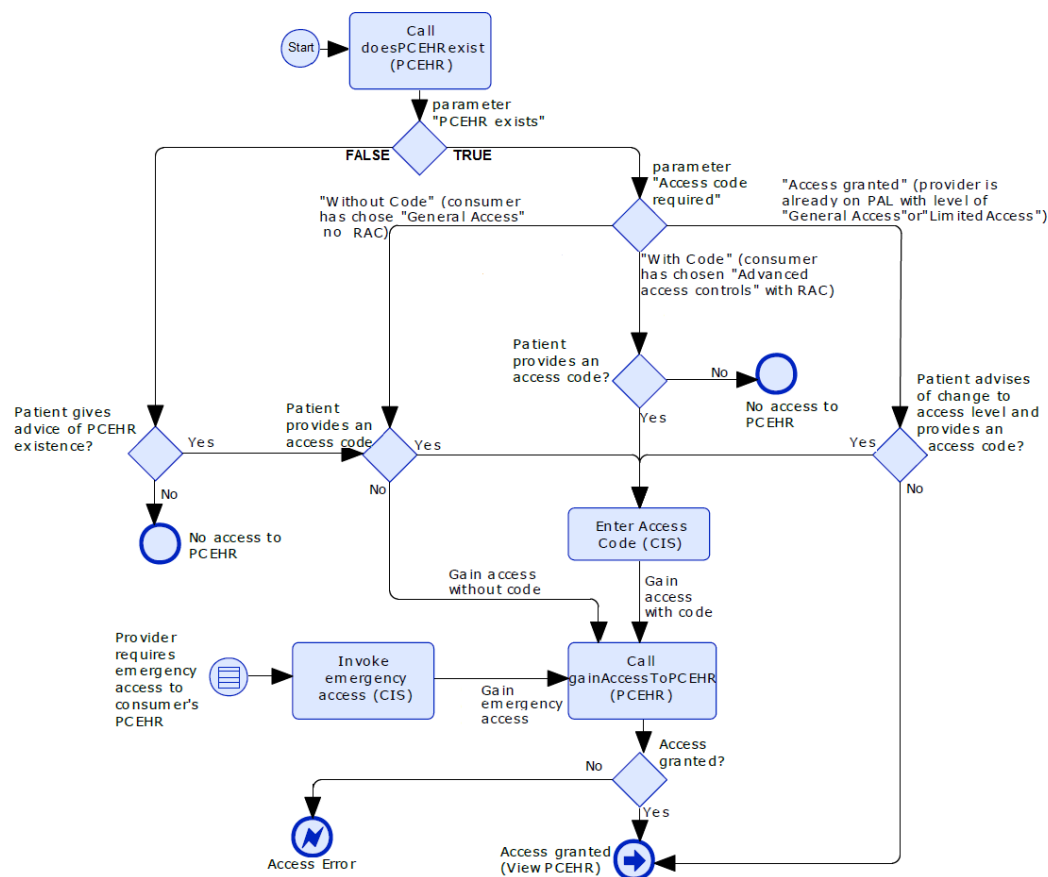

Figure 2 - Gain Access Business Logic Diagram from Australian Digital Health Agency

The derived business logic is:

1   The IHI number must be verified and must be added to the My Health Record System header. HIPS will ensure that a verified IHI is used.

2   With the verified IHI number:

a   If Access Type for the individual's My Health Record is "WithCode" then the "AccessType" of the patient must be added into "GainPCEHRAccess">"PCEHRRecord">"AuthorisationDetail" object. This can be either as "AccessCode" or "EmergencyAccess"

   i If the "AccessType" is set to "AccessCode" then the individual's My Health Record access code must be added to the GainPCEHRAccess">"PCEHRRecord">"AuthorisationDetail">"AccessCode" field.

 b If Access Type for the individual's My Health Record is "WithoutCode" and the individual has not given the provider an access code, and the provider does not choose to assert emergency access, then the "GainPCEHRAccess">"PCEHRRecord">"AuthorisationDetail" object will be set to NULL. If the individual has given the provider an access code or the provider chooses to assert emergency access, then the "AccessType" of the patient must be added into "GainPCEHRAccess">"PCEHRRecord">"AuthorisationDetail" object.

 c If Access Type for the individual's My Health Record is "AccessGranted" and the individual has not given the provider an access code, and the provider does not choose to assert emergency access, then "GainPCEHRAccess" would not need to be actioned. If the individual has given the provider an access code or the provider chooses to assert emergency access, then "GainPCEHRAccess" must be actioned and the "AccessType" of the patient must be added into "GainPCEHRAccess">"PCEHRRecord">"AuthorisationDetail" object.

 d If the parameter "PCEHR Exists" is false and therefore the Access Type for the individual's My Health Record is "null":

   i If the provider requires emergency access to the My Health Record then the AccessType of EmergencyAccess must be added into the GainPCEHRAccess.

   ii Otherwise if the individual has not advised of My Health Record existence then no access is possible and the GainPCEHRAccess must not be actioned.

   iii Otherwise if the individual has advised of My Health Record existence but has not provided an access code, then GainPcehrAccess must be actioned and the AuthorisationDetail object will be set to NULL.

   iv Otherwise if the individual has provided an access code then GainPcehrAccess must be actioned and the AccessType of AccessCode must be added into the GainPCEHRAccess > PCEHRRecord > AuthorisationDetail object.

2.2.18 Document List – Registry Stored Query (ITI-18)

2.2.18.1 Description

This function is used to retrieve a list of documents from the My Health Record System repository. There are several standard overloaded GetDocumentList methods for simple queries; if a more complex query is required then the GetDocumentList that uses the DocumentQuery object should be used. This is also described as the getDocumentList() function.

Zero or more listed documents can be returned from this function.

2.2.18.2 Business Rules/Functional Business Logic

1 The IHI number must be verified and must be added to the My Health Record System header. All calls must use the IHI value.

2 If the count of the list of documents from a successful repository request is zero (0) then a GetDocumentListRespone object will still be returned; however, the DocumentList attribute will have a null or empty list.

3   For the methods that use the CreationTimeStart, CreationTimeEnd, ServiceTimeStart and ServiceTimeEnd; they are all optional parameters. If null values are passed, then the query request will not include those parameters.

4   CreationTimeStart, CreationTimeEnd, ServiceTimeStart and ServiceTimeEnd parameters have a minimum precision value of a second.

5   Entering a value for the parameter for the ServiceTimeStart will enter a query against the ServiceStartTimeFrom to return all documents whose ServiceStartTime is after this value entered.

6   Entering a value for the parameter for the ServiceTimeEnd will enter a query against the ServiceStopTimeTo to return all documents whose ServiceStopTime is before this value entered.

7   Using the DocumentQuery object the DocumentClassCode, DocumentStatus, FormatCode, HealthCareFaciltyType and PracticeSettingTypes are all ILists and thus can have one or more values passed in.

2.2.19   Download Document - Retrieve Document Set (ITI-43)

2.2.19.1 Description

This function is used to retrieve a single XDS document element. ("DEXS-T 19" & "DEXS-T 21" from "PCEHR Document Exchange Service IHE XDS-b Technical Service Specification v1.3"). This is also described as the getDocument() function.

2.2.19.2 Business Rules/Functional Business Logic

1   Only a single document is returned from each call.

2   The returned document is unpacked and unencrypted as a CDA document along with any attachment files included in the package.

3   If the Save Document flag in the Document Request parameter is set, then HIPS will save a copy of the downloaded document in the Downloaded Document table in the local database.

4   If the consumer's IHI, date of birth, sex or family name in the downloaded document does not match the relevant stored information for the patient, a Demographic Mismatch Warning will be returned in the HIPS response. It is recommended that a user-facing application displaying the document makes this warning visible to the user.

2.2.20   Change History View

2.2.20.1 Description

This function is used to retrieve a list of all versions of a document from the My Health Record System repository, that are previous or subsequent versions of to a single identified document instance. The documents that are returned are the historical documents from a document tree.

2.2.20.2 Business Rules/Functional Business Logic

1   The IHI number must be verified and must be added to the My Health Record System header. All calls must use the IHI value.

2   The unique document ID, which is passed to this method, can be any of the unique document IDs that are within the historical document tree. Thus, no matter which unique document ID is passed all historical documents from the set will be returned.

2.2.21 Get View

2.2.21.1 Description

This function is used to access a My Health Record System view service, using the parameters that are defined for the view service, and receive the results as a CDA document.

This version of HIPS supports Prescription and Dispense View and Medicare Overview, however, the web service interface is designed to be extended to support any My Health Record System view service that returns a CDA document and is available via the 'GetView' interface.

2.2.21.2 Business Rules/Functional Business Logic

1   The patient must be identified with a verified IHI number. HIPS will ensure that the IHI number is verified and added to the My Health Record System header. All calls must use the IHI value.

2   The "user" object which is passed to this method must contain the name, role and identifier of the person responsible for the action, who is typically the interactive user of the clinical system. If the HPI-I of the person is known, the Role must be "ProviderIndividual" and the HPI-I must be provided.

3   The "parameters" object which is passed to this method must be an instance of "PrescriptionAndDispenseViewRequest" or "MedicareOverviewRequest" which are the only concrete subclasses of the abstract base class 'ViewParametersBase' in this version of HIPS.

2.2.22 Get Health Record Overview

2.2.22.1 Description

This function is used to retrieve Patient's Health Record Overview. The intended purpose of the HRO is as an overview of the patient information retrieved from the national My Health Record System.

2.2.22.2 Business Rules/Functional Business Logic

1   The patient must be identified with a verified IHI number. HIPS will ensure that the IHI number is verified and added to the My Health Record System header. All calls must use the IHI value.

2   The "user" object which is passed to this method must contain the name, role and identifier of the person responsible for the action, who is typically the interactive user of the clinical system. If the HPI-I of the person is known, the Role must be "ProviderIndividual" and the HPI-I must be provided.

3   The HIPS Core invokes the GetView from the My Health Record B2B Gateway Service.

4   The HRO View is returned and includes the patient profile, new documents list, recent documents list and the most recent Shared Health Summary in atomic format.

2.2.23 Get Pathology Report View

2.2.23.1 Description

This function is used to retrieve a patient's Pathology Report View (PRV). The intended purpose of the PRV is to aggregate and display in an effective manner a summary of pathology tests from pathology reports stored in the My Health Record system.

2.2.23.2 Business Rules/Functional Business Logic

1   The patient must be identified with a verified IHI number. HIPS will ensure that the IHI number is verified and added to the My Health Record System header. All calls must use the IHI value.

2   The "user" object which is passed to this method must contain the name, role and identifier of the person responsible for the action, who is typically the interactive user of the clinical system. If the HPI-I of the person is known, the Role must be "ProviderIndividual" and the HPI-I must be provided.

3   The HIPS Core invokes the GetView from the My Health Record B2B Gateway Service.

4   The HIPS Core returns the PRV mapped to response objects.

2.2.24   Get Diagnostic Imaging Report View

2.2.24.1 Description

This function is used to retrieve a patient's Diagnostic Imaging Report View. The intended purpose of the DIRV is to aggregate and display in an effective manner a summary of diagnostic imaging examinations from diagnostic imaging reports stored in the My Health Record system.

2.2.24.2 Business Rules/Functional Business Logic

1   The patient must be identified with a verified IHI number. HIPS will ensure that the IHI number is verified and added to the My Health Record system header. All calls must use the IHI value.

2   The "user" object which is passed to this method must contain the name, role and identifier of the person responsible for the action, who is typically the interactive user of the clinical system. If the HPI-I of the person is known, the Role must be "ProviderIndividual" and the HPI-I must be provided.

3   The HIPS Core invokes the GetView from the My Health Record B2B Gateway Service.

4   The HIPS Core returns the DIRV mapped to response objects.

2.2.25   Register Patients in Hospital

2.2.25.1 Description

This function is used to register patients in a health facility/hospital. The request will include the patient information that is required to register a patient in a health facility/hospital including MRN, Demographics, and optionally IHI.

2.2.25.2 Business Rules/Functional Business Logic

1   The "user" object which is passed to this method must contain the name, role and identifier of the person responsible for the action, who is typically the interactive user of the clinical system. Any errors that occur during the operation will be logged with the user's identity.

2   If an IHI has been provided it must have a last validated date supplied.

3   Invoke the FindOrCreatePatient to retrieve or create the patient master, hospital and hospital patient objects from the MRN, Demographics and IHI provided.

4   Based on the results:

a   If the "BypassHiService" setting is false then

ⅰ   If a new patient master was created then invoke RegisterPatient on the PatientRegistration class to attempt to find the patient's IHI.

ⅱ   If there was an existing patient master but a new hospital patient record was created, then invoke RevalidateIhi on PatientIhiValidation class to check for duplicate patients and confirm the IHI for this facility.

b   Otherwise invoke UpdatePatient on the PatientDemographicUpdate class to update the patient's details.

c   If an IHI was found, then invoke PcehrExists on the DoesPcehrExist class to check the current My Health Record status of the patient.

2.2.26   List Patients in Hospital

2.2.26.1 Description

This function is used to access a list of current patients in a healthcare facility. The list can be filtered to include patients with or without a My Health Record, with or without an IHI, and to include inpatients who were discharged within a specified number of days, patients who had other episode types within a specified number of days, and pre-admit patients who are expected to be admitted within a specified number of days.

2.2.26.2 Business Rules/Functional Business Logic

1   The "user" object which is passed to this method must contain the name, role and identifier of the person responsible for the action, who is typically the interactive user of the clinical system. Although this function does not access the HI Service or My Health Record System, any errors that occur during the operation will be logged with the user's identity.

2   The facility code (HospitalCode) and code system code (HospitalCodeSystem) are passed to this method to identify the healthcare facility.

3   While there may be several episodes that fall within the specified numbers of days, only one record is returned for each episode type and patient in the facility, with the details from the matching episode of each type whose date is closest to now.

4   Matching patients are either:

a   current inpatients from ADT A01 admit messages with patient class "I" for inpatient, or

b   recently discharged inpatients from ADT A03 discharge messages with class "I", or

c   recently serviced patients from ADT messages with patient class other than "I" or "P", or

d   future pre-admits from ADT-A05 pre-admit messages or other ADT messages with patient class of "P" for pre-admit.

2.2.27   List Patients Episodes in Hospital

2.2.27.1 Description

This function is used to access a list of admitted or discharged episodes for a specific patient in a hospital. The list can be filtered to include patients who were discharged within a specified number of days as well as include all the documents for a single document type for the patient.

2.2.27.2 Business Rules/Functional Business Logic

1   The "user" object which is passed to this method must contain the name, role and identifier of the person responsible for the action, who is typically the interactive user of the clinical

system. Although this function does not access the HI Service or My Health Record System, any errors that occur during the operation will be logged with the user's identity.

2   The hospital code, the "hospitalCodeSystem" object, which is passed to this method acts to scope the hospital code.

3   There may be several episodes that fall within the specified number of days since discharge and these will be included as well as currently admitted episodes.

4   Matching patients are either current inpatients (as created by an ADT-A01 message) or recently discharged inpatients (as created by an ADT-A03 message).

2.2.28   Local Health Providers

These methods are intended to be used to allow health facilities to view a list of health providers which are part of their health organisation network, allowing the health facilities to add, edit or deactivate a provider within their health organisation network.

2.2.28.1 List Local Providers

The ListLocalProviderRequest will return a ListLocalProviderResponse containing a list of local health providers that are in the local HIPS datastore, within the health organisation network, including:

- LocalProviderCode: a unique code assigned to the local health provider by the HIPS

- FullName: the health provider's full name

- Active: true if the local health provider has not been deactivated, false otherwise

- Hpii: the HPI-I of the local provider, if stored in the HIPS datastore

- HpiiStatus: the current status of the local provider's HPI-I, if stored in the HIPS datastore

- LocalProviderIdentifiers: a list of the local provider's identifiers if they have local identifiers for the health facilities stored in the HIPS datastore.

2.2.28.2 Add or Edit Local Provider

Adds or edits a local provider. If a HPI-I is provided or the name of the provider has changed, then the HPI-I will be validated against the HI service.

2.2.28.3 Deactivate Local Provider

Deactivates or removes deactivation on a local health provider.

NOTE: The deactivation is a local deactivation only and is separate to a HPI-I status of deactivated that is controlled via the HI Service.

2.2.29   Assisted Registration

2.2.29.1 Description

Assisted Registration was built to allow the fast and easy registration of patients into the My Health Record system.

2.2.29.2 Business Rules/Functional Business Logic

The Assisted Registration Service in HIPS implements the following business rules:

- Provide the ability to register adults (over 14 years of age) and dependents (under 18 years of age) with the My Health Record System.

- Maintain an audit log of successful registrations. If the verification method is response, then the return code must be masked or encrypted in the log.

- Allow all Identity Verification Methods to be used.

- Provide a list of patients with an IHI but without a My Health Record System using a simple data protocol.

- Allow patient registration based on the identifiers from the list and the patient's assertions. When using identifiers other than a verified IHI the associated IHI should have been verified within the previous 24 hours or HIPS should re-verify the IHI.

- Allow patient registration based on a Verified IHI and the patient's assertions.

- Allow patient registration based on a patient's demographics and assertions.

- Allow IHI validation to occur within HIPS prior to sending the registration request to the My Health Record System when using patient demographics.

- Allow the registration request to be sent to the My Health Record System without IHI validation when using patient demographics.

- Must meet all NOC and CCD mandatory tests.

2.2.29.3 Functional Validations

The following errors may be generated due to functional validations of the registration request. In the table below, RP refers to the "RegisterPatient" service that is for assisting an individual to register for their own My Health Record System, while RD refers to the "RegisterDependant" service that is for assisting a parent to register for their child's My Health Record System.

HIPS Error Message	Applies to
Individual's details must be provided.	RP & RD
The Indigenous Status must be provided.	RP & RD
The Evidence of Identity Type must be provided.	RP & RD
No given name provided.	RP & RD
No family name provided.[1]	RP & RD
Cannot have future dated date of birth. [1]	RP & RD
Date of birth cannot be more than 140 years ago.[1]	RP & RD
Must include a Medicare or DVA number. [1]	RP & RD
Medicare number is incorrect. [1]	RP & RD
Medicare IRN must be a number between 1 and 9. [1]	RP & RD
Representative details must be provided.	RD only

---

[1] Prefixed with "Representative: " or "Patient: " to indicate which person's demographics were invalid.

HIPS Error Message	Applies to
Consent form {0} with size {1}B exceeds the 200,000B limit for uploading to My Health Record System.	RP & RD
Filename contains path separator characters.	RP & RD
Consent form {0} has an invalid filename.	RP & RD
Consent form {0} is not a supported type for uploading to My Health Record System.	RP & RD
Must provide a response for ACIR documents consent.	RP & RD
Must provide a response for AODR documents consent.	RP & RD
Must provide a response for MBS documents consent.	RP & RD
Must provide a response for MBS Past Assimilation documents consent.	RP & RD
Must provide a response for PBS documents consent.	RP & RD
Must provide a response for PBS Past Assimilation documents consent.	RP & RD
The latest terms and conditions have not been accepted.	RP & RD
IVC Correspondence Channel has not been specified.	RP & RD
Mobile phone number is required for IVC SMS correspondence.	RP & RD
Invalid mobile phone number.	RP & RD
Email address is required for IVC email correspondence.	RP & RD
Invalid email address.	RP & RD
Representative declaration is required for assisted registration.	RD only
Dependant cannot be older than 18 years.	RD only
There cannot be less than a 14 year age gap between the dependant and the representative.	RD only
The representatives Medicare number must be provided.	RD only
The dependant and the representative must be on the same Medicare card.	RD only
An individual cannot be less than 14 years old.	RP only

2.2.30   Contracted Service Provider (CSP) Usage

2.2.30.1 CSP for HI Service

The 'CSP for HI Service' configuration option (HiCsp) changes how HIPS invokes the HI Service when requested by a health provider organisation to search or validate IHI or HPI-I numbers.

For HPOs that provide their Medicare site certificate to the operator of HIPS, the standard invocation logic will apply. The HPI-O of the accessing organisation is not required and not permitted in the SOAP header because the HI Service determines the accessing organisation's identity based on the certificate that is presented.

For HPOs that do not provide their Medicare site certificate to the operator of HIPS, but instead nominate to Medicare that the operator of HIPS is their Contracted Service Provider (CSP), altered invocation logic applies. DHS issue a CSP certificate to the operator of HIPS and this certificate is stored as the certificate to be used by HIPS when invoking the HI Service for this HPO. In this case, the HPI-O of the accessing organisation is included in the SOAP header on each invocation of the HI Service. This is configured by populating the HiCertSerial with the CSP certificate serial number and setting the HiCsp column to true in the HealthProviderOrganisation table.

2.2.30.2 CSP for My Health Record System

The CSP for My Health Record System configuration option (PcehrCsp) changes how HIPS invokes the My Health Record System B2B Gateway when requested by a health provider organisation to access the My Health Record of a patient.

For HPOs that provide their NASH certificate to the operator of HIPS, the standard invocation logic will apply. The client system type "CIS" is presented in the SOAP header on each invocation.

For HPOs that do not provide their NASH certificate to the operator of HIPS, but instead nominate to DHS that the operator of HIPS is their Contracted Service Provider (CSP), altered invocation logic applies. DHS issue a NASH PKI Certificate for Supporting Organisations to the operator of HIPS and this certificate is stored as the certificate to be used by HIPS when invoking the My Health Record System B2B Gateway for this HPO. In this case, the client system type "CSP" is presented in the SOAP header on each invocation. This is configured by populating the PcehrCertSerial with the CSP certificate serial number and setting the PcehrCsp column to true in the HealthProviderOrganisation table.

2.2.31   Multi-Tenant for IHI

The 'Multi-Tenant for IHI' modifies how HIPS manages the assignment of an IHI number to each patient record, in the context of multiple Health Provider Organisations (HPO) using the one instance of HIPS.

HIPS has a concept of networks, where organisations that have a common seed organisation can belong to the same network. These are configured in the HealthProviderOrganisationNetwork table within HIPS. HIPS must have at least one network configured.

For HPOs that belong to one network when an IHI is obtained by a network organisation, it is stored against the shared patient record and is available for use by any other network organisation during the configured period. This aligns with existing practice in a network of public hospital facilities.

For HPOs that do not belong to the same network, the IHI will be obtained and stored separately for each seed organisation in HIPS. The IHI that is obtained by one organisation will not be available for use by organisations that are in different networks. When organisations in other networks request the IHI or attempt to access the My Health Record System, HIPS will perform a new search of the HI Service to obtain the IHI for the new organisation. This ensures that the HI Service audit log records a disclosure of the IHI to the new organisation.

2.2.32   Package and Unpackage CDA document

This service was, prior to this version, used by the P2P module to package a CDA document for sending via the SMD. All validation is done as part of the P2P module before the CDA Packaging is invoked.

A successful response indicates the document has been sent to the SMD service successfully. The SMD component will attempt to send the message and any errors are handled in this component.

The Unpackage CDA Document service was used by the P2P module to unpack a CDA document that has been sent via the SMD Component.

The service result is sent back as the Unpackage CDA Document response.

The CDA document must be in the specified business format otherwise an exception will be raised. The Certificate must be a valid X509 Certificate otherwise an exception will be raised.

Once the CDA document is unpacked the Get CDA Content Service can be called which returns the CDA document content.

2.2.33   Validate Sending and Receiving Patient

This Validate Sending Patient service was, prior to this version, used by the P2P module to validate the IHI information when sending an ehealth message via the SMD.

The Validate Receiving Patient Service was used by the P2P module to validate the IHI information when an ehealth message is received via the SMD.

The response for both services return the MRN, State Patient Id and Validated IHI for the patient.

2.2.34   Reference Services

The following items in the HIPS database are considered reference data and are cached in memory for faster access.

Schema Item	Tables	Information Represented
Hospital	Hospital HealthProviderOrganisation HospitalAddress, Address HospitalContact, Contact HospitalCode, CodeSystem	Name, Authorised Employee, Logo Image HPI-O, Certificate Serial Numbers Hospital Addresses Hospital Contact Methods (e.g. Phone, Fax) Hospital Codes
Title	Title	Name Titles (Dr, Ms, Mr, etc.)
Suffix	Suffix	Name Suffixes (Senior, Junior, etc.)
Sex	Sex	Sex Codes and Descriptions
Country	Country	Country Codes and Descriptions
State	State	Australian State Codes and Descriptions
EpisodeType	EpisodeType	Episode Type Codes and Descriptions
CodeSystem	CodeSystem	Coding Systems and Namespaces
HospitalCode	HospitalCode CodeSystem	HospitalCode These codes are used to look up a hospital.

Schema Item	Tables	Information Represented
AddressType	AddressType	Address Types (Home, Temporary, Business, Mailing, etc.)
EpisodeLifecycle	EpisodeLifecycle	Episode Lifecycle Statuses (Pre-admit, Admitted, Discharged, Cancelled, etc.)
DocumentType	DocumentType	Document Types (Discharge Summary, etc.)
DocumentFormat	DocumentFormat CodeSystem	Document Format Codes/Template IDs For example, the format code "1.2.36.1.2001.1006.1.20000.16" represents the validation rules for "PCEHR Release 3 Discharge Summary Level 3A", with the relaxation of display name for mode of separation.
MedicareExclusion	MedicareExclusion	Certain values that are populated by PAS systems in the MedicareNumber field, which indicate that the person is ineligible for Medicare benefits or that the Medicare number is unknown.
ResponseChannel	RegistrationResponseChannel	Registration response codes for Assisted Registration.
DocumentConsentType	RegistrationConsentType	Registration document consent code for Assisted Registration.
IndigenousStatusType	IndigenousStatusType	Indigenous status codes for Assisted Registration.
IDEvidenceType	RegistrationIdentityEvedenceType	Identity evidence method codes for Assisted Registration.

2.2.34.1 Reload Reference Data

This method instructs HIPS to reload all reference data from the database. The system administrator can invoke this method after making a change to reference data in the HIPS database, instead of restarting the HIPS application server.

This service only affects cached reference data in the HIPS Core Web component and not in the queue consumer or alert monitor components. Reference data cached in the latter components can only be refreshed by restarting the corresponding Windows service.

2.2.34.2 Get Hospital Details

This method returns a set of information about a specified hospital, which is useful for the generation of a CDA document from that hospital.

2.2.35 Common Schemas

2.2.35.1 User Details

The user is included as a parameter on all calls to HIPS in order to assert the authorisation role under which any calls to the HI Service or My Health Record System should take place.

2.2.35.2 HIPS Response

This object is used to wrap up a response status indicator, error code, description and details that are returned from HIPS to calling systems.

2.3 Database Resource Access Layer

The HIPS Core database contains certain information about hospital patients that is relevant and required for the My Health Record System connectivity in HIPS.

The key requirements for this design were:

- Each hospital belongs to a Health Provider Organisation (HPO) with an HPI-O.

- A disclosure of My Health Record can be stored for each HPO that a patient visits.

- A withdrawal of consent to upload documents can be stored for each episode.

An overview of the data model is given below:
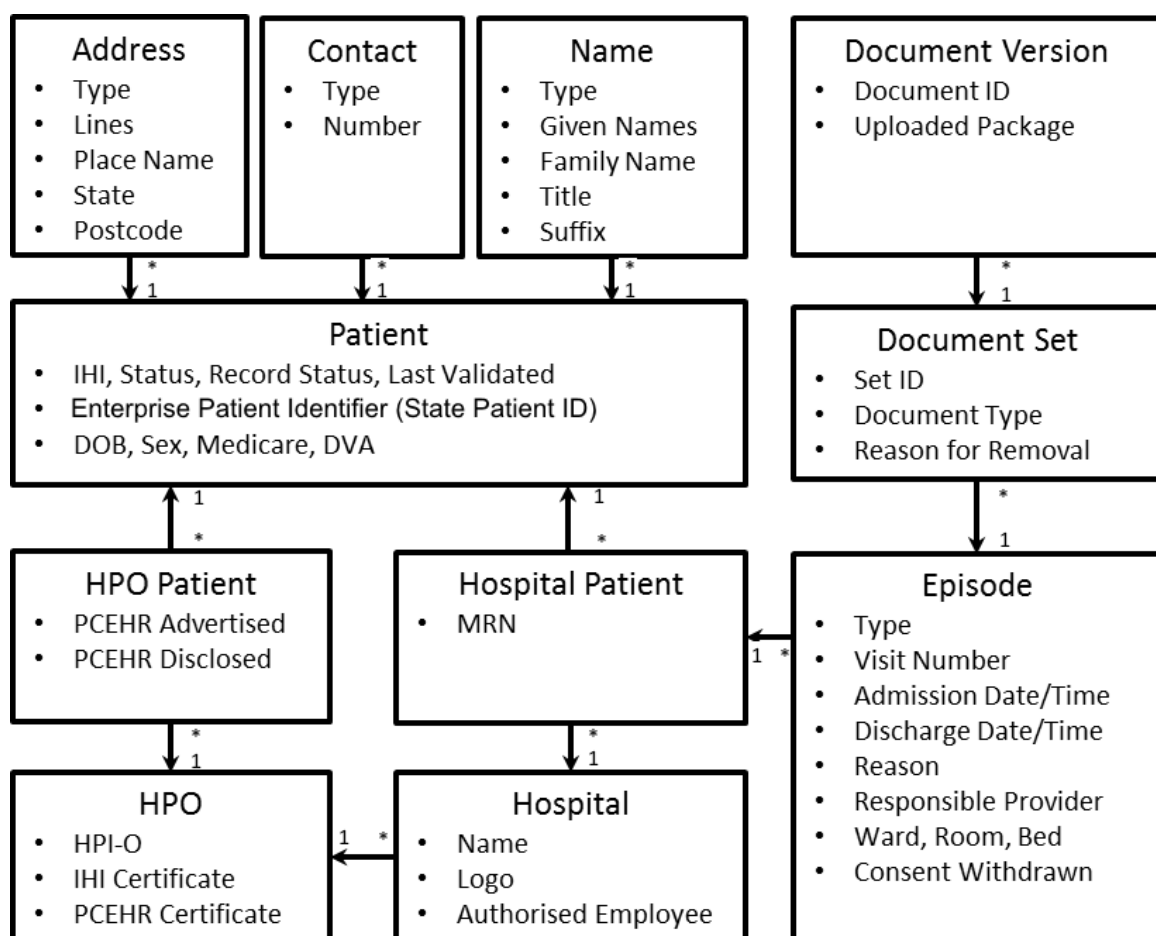
Figure 3 - Data model

2.3.1   HealthProviderOrganisationPatient Table

After HIPS calls the My Health Record System's "doesPCEHRExist" service method, the result is stored in the HPO Patient table, "HealthProviderOrganisationPatient".

The HealthProviderOrganisationPatient table will have the following columns:

Column	Type	Description
HealthProviderOrganisationId	int	The HPO to which this record relates.
PatientMasterId	int	The patient to which this record relates.
PcehrAdvertised	nullable bit	The value that the My Health Record System last indicated to this HPO as to whether the My Health Record for this patient exists.
AccessCodeRequiredId	int	The value that the My Health Record System last indicated to this HPO as to whether access to this patient's My Health Record is granted and whether a code is required for this HPO to gain access: -1: Unknown 0: With Code 1: Without Code 2: Access Granted
PcehrDisclosed	bit	Whether the patient has disclosed the existence of his/her My Health Record System to this HPO. The patient is known to be participating in the My Health Record if the patient has disclosed the existence of a My Health Record.
DateCreated	datetime	The date and time when the record for this HPO and patient was created.
UserCreated	varchar(256)	The domain and login of the user identified by the source system as responsible for the action that triggered the creation of this record.
DateModified	datetime	The date and time when the record was last modified.

Column	Type	Description
UserModified	varchar(256)	The domain and login of the user identified by the source system as responsible for the action that last modified this record.
PcehrExistsTimestamp	datetime	The date and time when HIPS last invoked the "doesPCEHRExist" service of the My Health Record system to refresh the information stored in this record.

2.3.2 Queuing Data Model

After each request to UploadOrSupersedeDocument, UploadDischargeSummaryLevel1A, UploadOrRemovePathology, UploadOrRemoveImaging or Remove has been validated, a record of the queued operation with "Pending" status will be added to the "MessageQueue" table in the HIPS Core database as illustrated below.

Normal processing is to delete these records of the queued operations once the operation has successfully completed, and so the table will contain only pending operations and failures. HIPS has a configuration item to allow successful operations to be retained for testing or operational purposes.

The configuration item "QueueConsumer.RemoveOnSuccess" will default to true. If this configuration item is true, then the record of the queued item will be deleted after successful processing.

If the queued operation is successful, and above configuration item is set to false, then the MessageQueueStateID column will be updated to Success, and the record will remain in the MessageQueue table.

If the queued operation is unsuccessful, then the MessageQueueStateID column will be updated to Failure, the SOAP request and response will be populated into the Request and Response columns of the SystemInteractionLog table, and any additional error information including a HIPS exception or stack trace will be populated into the SystemEventLog table.
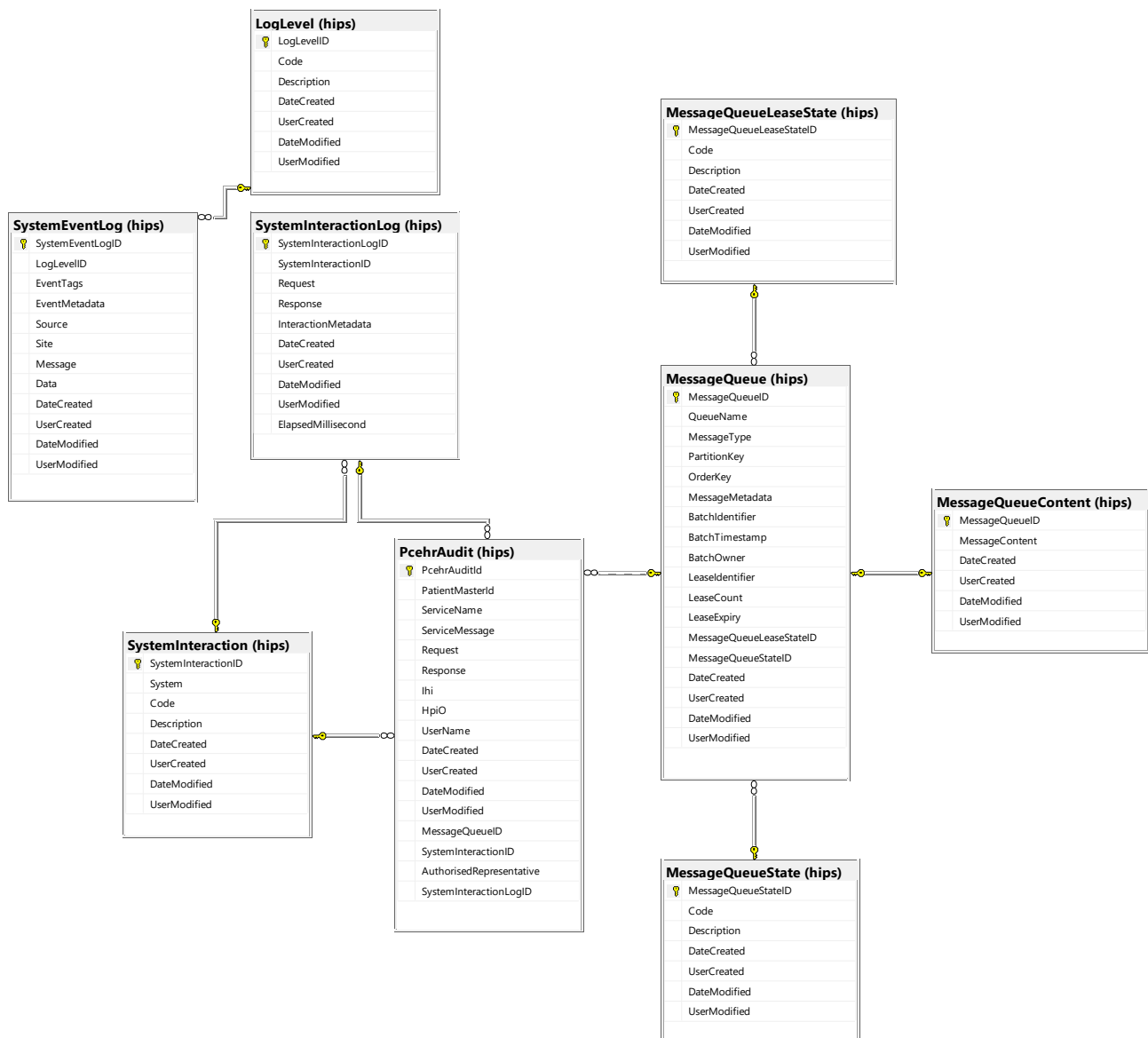
Figure 4 - Queuing Data Model

The sections below further describe the key tables in the queuing data model.

MessageQueue (hips)

Column Name	Condensed Type	Nullable	Description
MessageQueueID	int	No	PK. Unique identifier of the record. Unique identifier of the queued message.
QueueName	varchar(100)	No	Name of the logical queue into which the message has been queued.
MessageType	varchar(100)	No	Identifier for the type of queued message.
PartitionKey	varchar(500)	Yes	Key value used for partitioning messages.
OrderKey	varchar(500)	Yes	Key value used for ordering messages within their partition.
MessageMetadata	xml	Yes	Metadata related to the message.
BatchIdentifier	uniqueidentifier	Yes	Unique identifier of a batch within which a set of queued messages has been acquired for processing.
BatchTimestamp	datetime2(7)	Yes	Timestamp of the batch within which a set of queued messages has been acquired for processing.
BatchOwner	varchar(500)	Yes	Identifier of the owner of the batch (e.g. HIPS background processing consumer identifier).
LeaseIdentifier	uniqueidentifier	Yes	Unique identifier of a lease obtained on a specific message for processing.
LeaseCount	int	No	Number of sequential leases that have been obtained on this message.
LeaseExpiry	datetime2(7)	Yes	Date and time at which the current message lease will expire.
MessageQueueLeaseStateID	int	No	FK (MessageQueueLeaseState). Unique identifier of the associated MessageQueueLeaseState record. State of the current messa
MessageQueueStateID	int	No	FK (MessageQueueState). Unique identifier of the associated MessageQueueState record. State of the message in the message
DateCreated	datetime	No	Date and time the record was created.
UserCreated	varchar(256)	No	Identity of the user that created the record.
DateModified	datetime	No	Date and time the record was last modified.
UserModified	varchar(256)	No	Identity of the user that last modified the record.

Figure 5 – MessageQueue

MessageQueueContent (hips)

Column Name	Condensed Type	Nullable	Description
MessageQueueID	int	No	PK. Unique identifier of the record. Unique identifier of the queued message.
MessageContent	varbinary(MAX)	No	BLOB content of the queued message itself.
DateCreated	datetime	No	Date and time the record was created.
UserCreated	varchar(256)	No	Identity of the user that created the record.
DateModified	datetime	No	Date and time the record was last modified.
UserModified	varchar(256)	No	Identity of the user that last modified the record.

Figure 6 – MessageQueueContent

Figure 7 - PcehrAudit

Figure 8 - SystemEventLog

2.3.3 Clinical Document Data Model

Documents that are successfully uploaded, superseded or removed will be stored within the HIPS Core database in the data model illustrated below.
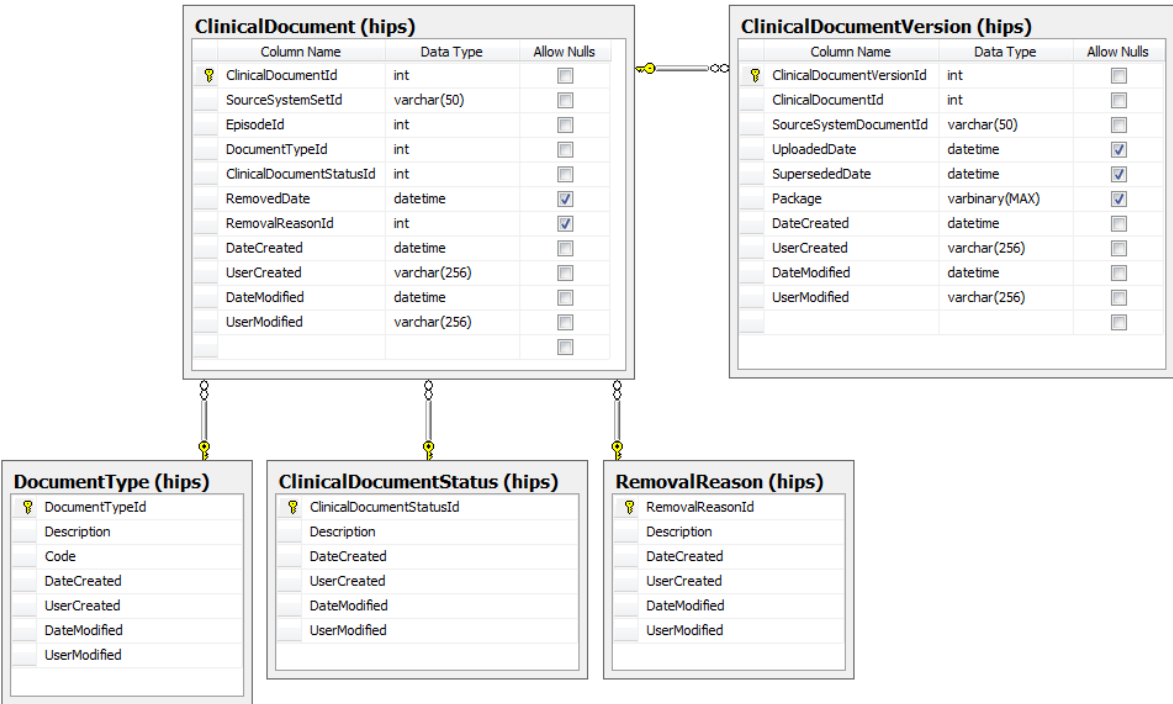
Figure 9 - Clinical Document Data Model

All versions of a document that are uploaded to My Health Record System by HIPS will be associated with an episode, which is associated with a patient in a certain hospital, which is associated with the patient master record and the hospital record. The HIPS Core database model makes this hierarchy explicit, and assigns identifiers at each level.
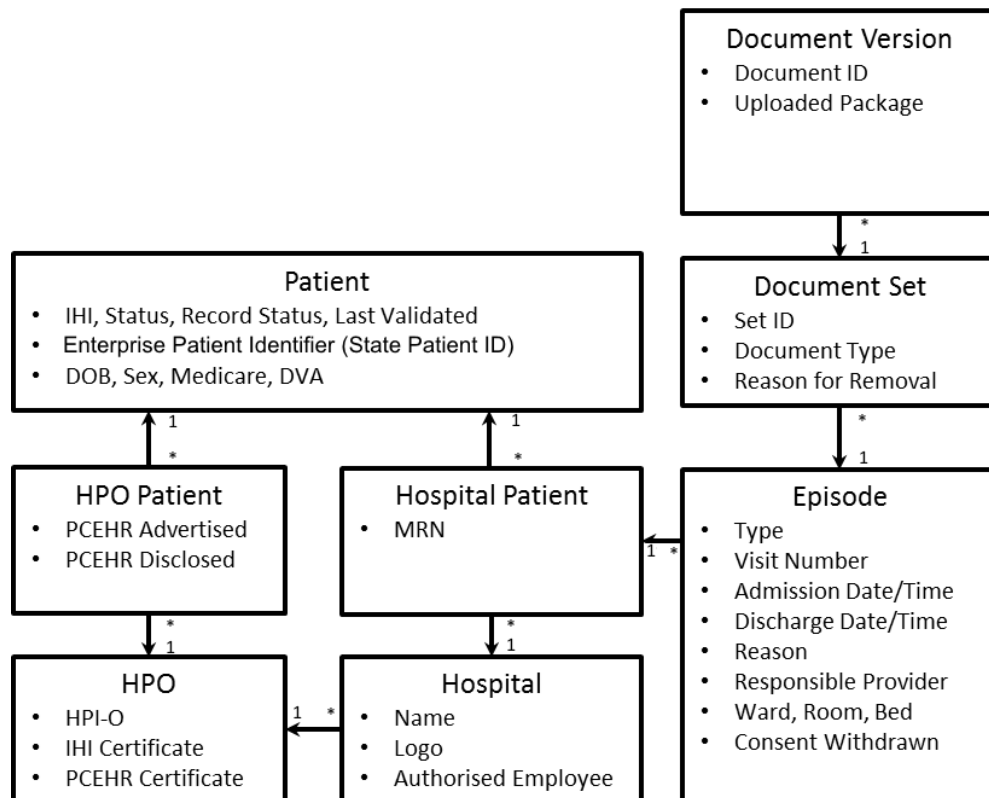
Figure 10 - Data Store model

2.3.3.1 ClinicalDocument Table

The "ClinicalDocument" table stores the information that relates to the overall document.

Column	Type	Description
ClinicalDocumentId	int	Auto-incrementing primary key.
SourceSystemSetId	varchar(50)	The source system's unique identifier of the overall document, which must not change between versions of the same document. This is populated from the "root" and "extension" attributes of the "setId" element of the CDA document, separated by ^ (caret).
EpisodeId	int	The episode to which this document relates. The hospital and patient are identified via this link to the episode.
DocumentTypeId	int	The type of document, such as discharge summary or event summary. This is populated from the "code" element of the CDA document.

Column	Type	Description
ClinicalDocumentStatusId	int	The overall document status: 1: Active 2: Removed
RemovedDate	datetime (nullable)	If currently removed, the date and time when the document was last removed. This will be reset to null if a new version of a removed document is uploaded.
RemovalReasonId	int	If currently removed, the reason for removal: -1: Not Removed 1: Withdrawn 2: Elect to Remove 3: Incorrect Identity This will be reset to -1 if a new version of a removed document is uploaded.
DateCreated	datetime	The date and time when the clinical document was first uploaded.
UserCreated	varchar(256)	The domain and login of the user identified by the source system as responsible for the upload.
DateModified	datetime	The date and time when the clinical document was last uploaded or removed.
UserModified	varchar(256)	The domain and login of the user identified by the source system as responsible for the action.

2.3.3.2   ClinicalDocumentVersion Table

The "ClinicalDocumentVersion" table stores the information that relates to an individual version of the document.

Column	Type	Description
ClinicalDocumentVersionId	int	Auto-incrementing primary key.
ClinicalDocumentId	int	The clinical document that this is a version of.

Column	Type	Description
SourceSystemDocumentId	varchar(50)	The source system's unique identifier of the document instance, which will change between versions of the same document. This is populated from the "root" and "extension" attributes of the "id" element of the CDA document, separated by ^ (caret).
UploadedDate	datetime	The date and time when this version was uploaded.
SupersededDate	datetime (null)	If this version has been superseded by a later version, the date and time when this version was superseded.
Package	varbinary(max)	The CDA package ZIP file that was uploaded.
DateCreated	datetime	The date and time when this clinical document version was uploaded.
UserCreated	varchar(256)	The domain and login of the user identified by the source system as responsible for the upload.
DateModified	datetime	The date and time when this clinical document version was uploaded or superseded.
UserModified	varchar(256)	The domain and login of the user identified by the source system as responsible for the most recent upload or supersede action on this version.

3   HIPS Monitoring Tool

The HIPS Monitoring Tool was built for Application Support Teams to allow them to act proactively with regards to any alerts that HIPS provides.

It provides:

- Alerts about current issues.

- Near real-time information about the current state of connections and messages.

- Basic statistics about patients, IHI lookups and My Health Record lookups.

- Views of the connections and general errors in the system.

3.1   General Features

The following general features will be available:

- Monitoring data is automatically refreshed every 2 minutes.

- Refresh button will perform an immediate refresh of the monitoring data.

- Show and Hide Errors button toggles the error tab display.

- Snooze button will silence known alerts for 30 minutes.

- Any unacknowledged issues at time of snooze will still be displayed.

3.2   System Tray Alert Icons

The system tray alert icons are designed to alert the user to HIPS issues when the HIPS monitoring tool is minimised. The alerts appear in the bottom right of the user's taskbar.

Green	Healthy	
Orange	Possible issues	
Red	Active issues	

Active issues will display Pop-up Messages from the Status Tray:


Figure 11 - Alert

Approved for external use

3.3 Status Display

The status display shows the current status of the HIPS system based on predefined values and minimums.

Each status will be displayed with a graphic that depicts its current state:

Green	Healthy	
Orange	Possible issues	
Red	Active issues	

3.4 Thresholds

3.4.1 IHI Lookup percentage connection failures

Percentage of IHI Connection Failures in last 60 minutes, alert based on the **percentage**.

< 20	Green Healthy
> 20 but < 50	Orange Alert
>= 50	Red Alert

This is based on a count of all IHI alerts divided by a count of all unique IHI's, where:

- Unique IHIs: Count of all IHI records in the Patient Master IHI table

- IHI alerts: Count of all IHI alerts records in the Monitoring Syslog view for IHI connection errors over the last 60 minutes.

3.4.2 Average IHI Lookup time

Average amount of time (in seconds) that the IHI lookup takes to response, alert based on **duration in seconds**.

< 10	Green Healthy
> 10 but < 20	Orange Alert
>= 20	Red Alert

This retrieves the time difference between the "creation" date time that is added to the HI service request and the date time recorded as Date Created for the IHI Lookup Audit after a response has been received from the HI service.

3.4.3 My Health Record percentage connection failures

Percentage of My Health Record Connection Failures in last 60 minutes, alert based on the **percentage**.

< 20	Green Healthy
> 20 but < 50	Orange Alert
>= 50	Red Alert

This is based on a count of My Health Record request failures divided by a count of My Health Record requests over the last 60 minutes, where:

- My Health Record requests: Count of audit records in the PCEHR Audit table

- My Health Record request failures: Count of all records in the Monitoring Syslog view for My Health Record failures.

3.4.4   Average My Health Record Lookup time

Average amount of time (in seconds) that the service takes to respond from a 'DoesPCEHRExist' request. Alert based on duration in **seconds**.

< 10	Green Healthy
> 10 but < 20	Orange Alert
>= 20	Red Alert

This retrieves the time difference between the "creation" date time that is added to the My Health Record service request and the date time recorded as Date Created for the My Health Record Audit after a response has been received from the My Health Record service.

3.4.5   PAS Messages in the last 10 minutes

Number of PAS messages received successfully in the last 10 minutes, alert based on the **count of messages**.

> 0	Green Healthy
= 0	Red Alert

Provides a count of messages in the HL7MessageLog table from the last 10 minutes.

3.4.6   HIPS errors in the last 8 hours

Number of HIPS Errors in the last 8 hours, alert based on the **count of errors**.

= 0	Green Healthy
>= 1 but < 5	Orange Alert
>= 5	Red Alert

Provides a count of errors recorded in the Monitoring Syslog view for HIPS errors.

3.4.7 My Health Record items in a Pending state

Number of My Health Record Documents that are pending upload to the My Health Record System, alert based on minutes waiting in the message queue.

< 10	Green Healthy
> 10 but < 20	Orange Alert
>= 20	Red Alert

3.4.8 My Health Record failed items in the last 7 days

Number of My Health Record Documents that have failed upload to the My Health Record System in the last 7 days, alert based on the count of failed uploads.

= 0	Green Healthy
> 0	Red Alert

3.5 Statistics

Basic statistics will be displayed to give a quick overview of the number of patients in the system and their IHI and My Health Record status.

The following statistics will be displayed:

- PAS Messages Processed: Number of successful ADT messages processed from go live.

- Unique Patients: Number of unique patients stored within HIPS.

- IHIs Found: Number of Valid IHI numbers matched from the Unique Patients. Added is % of IHIs Found to Unique Patients.

- CDA Documents Uploaded: Number of documents successfully uploaded to the My Health Record.

- My Health Records Advertised: Number of identified My Health Records advertised from Unique Patients with an IHI. If a patient has an advertised My Health Record with at least 1 HPI-O, then it calculated as being advertised; however, if a patient is registered with multiple HPI-Os, then it is only recorded once. Added is the ratio of My Health Records Advertised to IHIs Found.

3.6 Error Tabs

The Error Tabs provide detailed information about any errors that have occurred within the HIPS system.

The following tabs will be provided:

- HIPS Errors

- HIPS Information

- Merge Information

- IHI Connection Errors

- IHI Information

- IHI Status

- My Health Record Connection Errors

- My Health Record Information

- My Health Record Upload Errors

- MSMQ Information

- Background Processor

- My Health Record Uploaded Documents

3.6.1 System Errors and Information

The following tabs display errors or information from the System Error Log:

- HIPS Errors

- HIPS Information

- Merge Information

- IHI Connection Errors

- IHI Information

- My Health Record Connection Errors

- My Health Record Information

- MSMQ Information

- Background Processor

Each error or information record contains a log number that is linked to a tab via the Monitor Tab Message table. This table is maintained as part of HIPS releases and should not be changed during implementation.

Fields displayed are:

- Message

- Exception Message

- Date Created

- Log Message

3.6.2 IHI Status

This tab displays information about each patient that has an IHI Status in error or needing resolution. The Registered Given Name and Family Name are provided. These names may not match the current CIS name of the patient but are the names used to retrieve the IHI from Medicare.

As these records can be updated the Date Modified is displayed rather than the date created to provide the correct timeframe of the errors.

Fields displayed are:

- IHI Status

- IHI Status ID

- MRN

- Hospital

- Registered Given Name

- Registered Family Name

- Date Modified

3.6.3   My Health Record Upload Errors

This displays any errors that occurred when uploading a document to the My Health Record System. By double clicking on a specific row the user can save a zip file containing the CDA package that was uploaded to the My Health Record System. In the case of validation errors this can then be run through the offline validator to provide additional details about the errors.

Fields displayed are:

- MRN

- IHI

- IHI Status

- Hospital

- Episode Admission Date

- Patient Master Id

- Episode Id

- PCEHR Message Queue Id

- Date Created

- Error Details

3.6.4   My Health Record Upload Documents

This tab displays details about documents uploaded over the last 7 days. It retrieves this information from the Clinical Document table and associated tables.

Fields displayed are:

- Upload Date Time

- Source Document ID

- Document Type

- Sender Name

- Facility

- MRN

- Visit Number

- Admission Date Time

- Discharge Date Time

Acronyms

Acronym	Description
ADT	Admission, Discharge, Transfer. Class of HL7 message types. ADT is also an Application Code used in MSH.3 and MSH.5
CDA	Clinical Document Architecture
CIS	Clinical Information System
CSP	Contracted Service Provider
DHS	Department of Human Services
EMPI	Enterprise Master Patient Index
ESB	Enterprise Service Bus, an integration hub for routing and transforming messages within and between healthcare facilities.
HI	healthcare identifier
HL7	Health Level Seven
HPO	Healthcare Provider Organisation
HRO	health record overview
IHI	individual healthcare identifier
IHTSDO	International Health Terminology Standards Development Organisation
IRN	Medicare card individual reference number
LHN	Local Health Network
MBS	Medicare Benefits Schedule
MRN	Medical Record Number
MSMQ	Microsoft Message Queue (or Queueing)
NASH	National Authentication Service for Healthcare
NIO	National Infrastructure Operator
OBR	Observation Request segment of HL7 messages
OBX	Observation Result Segment of the HL7 message. Is used to transmit a single observation or observation fragment.
OID	object identifier
OPD	Outpatient Department

Acronym	Description
ORC	Common Order Segment of an HL7 message. Is used to transmit fields that are common to all orders.
ORU	Unsolicited transmission of an observation message. R01 event.
PAS	Patient Administration System
PBS	Pharmaceutical Benefits Scheme
PCEHR	Formerly, personally controlled electronic health (eHealth) record, now My Health record.
PMI	Patient Master Index
PRV	Pathology Report View
RIS	Radiology Information System
SMD	Secure Message Delivery
SNOMED	Systematized Nomenclature of Medicine
SOAP	Simple Object Access Protocol

Glossary

Term	Meaning
Medical Record Number (MRN)	This number is stored in HospitalPatient.Mrn and is the primary identifier used to find the existing patient records in the HIPS database. Identified by the code "MR" in PID-3.
	Ideally one MRN is allocated by the hospital for each patient, though it is common to temporarily allocate a new MRN for emergency patients until their identity is confirmed. These temporary MRNs should be merged back to the original MRN for the patient using an A36 Merge MRN message.
Observation Request	Segment of an HL7 message, used to transmit information specific to an order for a diagnostic study or observation, physical exam, or assessment.
Outpatient Department	Often used to describe an informal class of HL7 message types, such as appointment/booking/scheduling messages. OPD is also an Application Code used in MSH.3 and MSH.5.
Patient Master Index (PMI)	Often used to describe an informal class of HL7 ADT messages – includes updates to patient demographics and merge/unmerge message types. PMI is also an Application Code used in MSH.3 and MSH.5.