healthLINK SIX 6
SECURE INFORMATION EXCHANGE

Technical User Guide

Applicable to HMS v6

Version:	1.4
Prepared:	5th January 2004
Updated	5th March 2013
Document:	HealthLink SIX Technical Guide
Authors:	Clifford Wilson, Dan Fraser, Alistair Crawford

Liability Notice: Every effort has been made to ensure that the information in this document, supplied by HealthLink Limited, is accurate and complete. However, as use and interpretation of this document is beyond the control HealthLink Limited, no liability, either direct or consequential, can be entertained by HealthLink Limited, its agents, or its suppliers.

Table of Contents

1.0 INTRODUCTION

2.0 HEALTHLINK SIX

3.0 OTHER SERVICES

4.0 SECURITY

THIS PAGE INTENTIONALLY LEFT BLANK

1.0 Introduction

1.1 Overview – What this document covers

HealthLink provides a suite of services and applications that use Internet enabled technologies to provide effective communication across the health sector. The principal components of these services are the HealthLink Messaging System (HealthLink SIX), and the HealthLink Online Services.

This document details HealthLink SIX and related services from a technical perspective - provided as a reference document for any party using, or intending to use the services provided by HealthLink Ltd.

The majority of the information pertains to the HealthLink SIX software. This document will assist with:

- Integrating PMS software with the HealthLink SIX software
- Integrating Lab systems with the HealthLink SIX software

1.2 HealthLink Service and Support

If you have any questions regarding this guide or regarding the HealthLink Messaging Service, you can contact HealthLink directly for further service and support.

The HealthLink Support Team can be contacted via the following email address:

helpdesk@healthlink.net

HealthLink can be contacted toll-free from Australia and New Zealand on the following toll free lines and between the support hours specified:

New Zealand - 0800 288 887 (press option 2)
8.00 am - **6.00 pm** (New Zealand time)

Australia - 1800 125 036 (press option 2)
8.00 am - **6.00 pm** (All Australian Time Zones)

Customers can also fax toll-free at any time on
0800 288 885 (NZ), or **1800 151 146 (AU)**

We strongly recommend that all customers use the contact details listed above for all support issues rather than contacting individual HealthLink staff-members. This ensures that you get the attention of the first available staff-member, and do not experience delays when individual staff-members are on training courses or on leave.

When contacting the helpdesk by email, fax or telephone, please provide us with the following information:

- The name and version number of the HealthLink software you are using
- The operating system you are using
- If applicable, the details of any change you are wishing to make to the configuration and what effect you are expecting this to have
- The text of any error messages you may have encountered

2.0 HealthLink SIX

2.1 Software Overview – Secure Information eXchange

HealthLink SIX is a secure messaging system that provides real time and store-and-forward Electronic Data Interchange (EDI) in a context specifically tailored to the requirements of Health providers. HealthLink SIX can be run across the internet and can utilise permanent and broadband Internet access technologies including VPN networks. The client uses the same port that is used by web browsers when browsing secure web sites (SSL port, 443), to minimise potential problems negotiating client firewalls and proxy servers.

To customers, HealthLink SIX takes the form of a client application, which makes a secure connection to the HealthLink Electronic Data Interchange (EDI) servers, downloads messages addressed to the customer's EDI account, and uploads messages to be sent to other customers' EDI accounts. The client application is usually set up to make scheduled connections or to run in the background - in many cases it is unseen; for example when running as an NT Service.

The design emphasis of the HealthLink SIX client software is on providing a completely secure, robust, easy-to-use service that is useful for health industry professionals.

Installation

The HealthLink SIX client has been designed to be installed by non-IT specialist practice staff. Country-specific installation requirements are handled by the installation software. The installation program includes the integrated installation/upgrade of required components e.g. Internet Explorer, Java Runtime Environment, loading of certificates into the browser and EDI key stores where applicable. The installation program provides a seamless upgrade from older versions of HMS, maintaining all current directories and configuration options and allowing the site to easily change their connection medium from the HealthLink VPN to the Internet. Multiple EDI accounts can be supported by a single installation of HealthLink SIX.

The messaging GUI (Graphical User Interface) gives details in plain English about the status of the EDI transfer and is updated in real time. Event logs are human and computer-readable and provide information about connections, EDI events and summaries of files exchanged.

2.1.1 Purpose

HealthLink SIX is a secure system that provides real time and store-and-forward Electronic Data Interchange (EDI) services in a context specifically tailored to the requirements of Health providers.

HealthLink SIX is a service. It comprises the following components:

- Use of a Public Key Infrastructure (PKI) for 128 bit end-to-end encryption, sender authentication and non-repudiation.
- Verification of adherence to standard message formats
- Translation of messages to/from other supported formats
- Generic file addressing and transfer for e.g. IPA age/sex register file transfers and PIT message transfer
- Easy installation and day-to-day operation designed for practice staff without specific IT training or knowledge.
- Incorporates a powerful yet easy-to-use configuration utility (GUI)
- Updates are automatically and securely downloaded and configured by the client software as they become available
- Options for scheduled connections, or operation as an NT service.
- Client is written in Java to allow support for multiple platforms. Java installation packages are available for Windows and Mac OS
- Client Software providing connectivity to the HealthLink Online Services
- Messaging Servers – for store-and-forward and real time EDI
- An HL7<>Fax Gateway
- Complete PKI certificate management – from issuing through to revocation and automated certificate renewal
- Full helpdesk support
- Outgoing messages are validated, translated, encrypted and signed
- Incoming messages have their signatures verified, are decrypted, translated and verified

2.1.2 System Requirements

The HealthLink recommended System requirements can be found here:

http://www.healthlink.net/en_NZ/support/software-downloads/

It should be noted that HealthLink software typically integrates with existing EMR software at the practice, typically on the same server. Because of this the system requirements are usually dominated by those of the EMR system.

2.2 Message Formats

2.2.1 Structured Messages

The HealthLink SIX Client application verifies the format of incoming and outgoing messages and is capable of translating messages of the same type (e.g. LABRESULT) from one format to another (e.g. HL7v2.1 to Flat Filev2.3).

The following formats are currently supported by HealthLink SIX:

- ACC M40/M47 CLAIMS: Flat File and EDIFACT New Zealand
- LABRESULT: Flat File and New Zealand HL7 (v2.1)
- LABORDERS and LABRESULTS: New Zealand HL7 (v2.4)
- HBL-CLAIM / HEALTHPAC: Maternity Providers Claims Flat File and New Zealand HL7 (v2.3)
- REFERRAL, STATUS AND DISCHARGE (RSD): Flat File and New Zealand HL7 (v2.3)
- REFERRAL, STATUS AND DISCHARGE (RSD): New Zealand HL7 (v2.4)
- PIT / BROADCAST: Pathology Linecode messaging for Australia
- DIABETES: IPA Project reporting Flat File New Zealand
- DIABETES2: XML reporting specification New Zealand
- GP2GP: transport wrapper for CDA and attachments New Zealand HL7 (v2.4)
- HCONNECT: HL7 Health Connect Message Type in Australia
- HDOCS: HealthDocs XML wrapper for attachments New Zealand
- HDOC eMS: Canadian XML wrapper for CDA or PDF
- LAB2RESULT2: HL7 (v2.3.1) in Australia
- LAB2RESULT2: laborders and labresults HL7 (v2.4) in Australia
- NSWEHR: Electronic Health Record messaging HL7 (v2.4) in Australia
- RSDAU: HL7 (v2.3.1) in Australia
- RSDAU: HL7 (v2.4) in Australia
- NIR : National Immunisation Register messaging New Zealand HL7 (v2.4)
- GMS/IMMS : General Medical Services & Immunisation Claims HL7 (v2.3)
- MDM: SMD transport wrapper for CDA HL7 (v2.3.1) in Australia
- HDOC eMS: Canadian XML wrapper for CDA or PDF

Additional message types and message translations can be created and rapidly deployed to a set of HealthLink SIX installations or to all HealthLink SIX client installations.

The currently supported structured messages and formats for New Zealand are:

Type	Definition Jar	Supported Formats	Primary Format(s)	Supported Mappings
RSD	RSD_Definitions	Flat Filev2.3 Flat Filev2.3.1 HL7v2.3 PIT	HL7v2.3	FFv2.3 > HL7v2.3 FFv2.3.1 > HL7v2.3 HL7v2.3 > FFv2.3.1 HL7v2.3 > FFv2.3 HL7v2.3 > PIT
LAB	LAB_Definitions	Flat Filev2.1 HL7v2.1 HL7v2.2	HL7v2.1	FFv2.1 > HL7v2.1 HL7v2.1 > HL7v2.2 HL7v2.2 > HL7v2.1 HL7v2.1 > FFv2.1
HBL	HBL_Definitions	Flat Filev2.3 HL7v2.3	HL7v2.3 HL7v2.3 (Mat88)	FFv2.3 > HL7v2.3 HL7v2.3 > FFv2.3
KIDZNET	KIDZNET_Definitions	FFv1.22	FFv1.22 (Kidslink) FFv1.22 (Kidznet)	None
ACC	ACC_Definitions	EDIFACTvD-97a FFvD-97a	EDIFACTvD-97a	EDIFACTvD-97a > FFvD-97a FFvD-97a > EDIFACTvD-97a
Diabetes	DIABETES_Definitions	FF1.4b	FF1.4b	None
HEPB	HEPB_Definitions	FFv2.3.1 HL7v2.3.1	HL7v2.3.1	FFv2.3.1 > HL7v2.3.1 HL7v2.3.1 > FFv2.3.1
MEDDOCS	MEDDOCS_Definitions	FFv1.0	FFv1.0	None
GPSURV	GPSURV_Definitions	FFv1.8 FFv1.9a	FFv1.8 (GPSURV CSV) FFv1.9a (GPSURV)	None
XML	XML_Definitions	XMLv1.0 XMLvD-97a XMLvD0-8	XMLv1.0 (Transfer) XMLvD0-8 (Commented)	EDIFACTvD-97a > XMLvD-97a XMLvD-97a > EDIFACTvD-97a
NIR	nir_definitions	HL7 v2.4	HL7 v2.4	None
GMG	hbl_definitions.jar	HL7 v2.3	HL7 v2.3	None
IMMS	hbl_definitions.jar	HL7 v2.3	HL7 v2.3	None

The currently supported structured messages and formats for Australia are:

Type	Definition Jar	Supported Formats	Primary Format(s)	Supported Mappings
HCONNECT	HCONNECT_Definitions	HL7v2.3.1	HL7v2.3.1	None
LAB2	LAB2_Definitions	HL7v2.3.1 HL7 v2.4	HL7v2.3.1	Yes for incoming to PIT/PDF
RSDAU	RSD_Definitions	HL7 v2.3.1 HL7 2.4	HL7v2.3.1	Yes for incoming to PIT/PDF
MDM	LAB2_Definitions	HL7 v2.3.1	HL7 v2.3.1	None

2.2.2 Generic Messages

Messages that do not conform to any of the above formats can be sent as generic, "unstructured" messages. These messages are sent without any message validation, message parsing, or message translation/mapping between formats. This generic message type is used in both NZ and Australia – for MIMS updates and IPA/PHO files in NZ, and for the legacy formatted PIT laboratory result delivery in Australia.

In order to improve the use of EDI all new file types will be implemented as structured messages.

A number of options are available for addressing generic files. These are described in detail in section 2.2.3; The Message Spec Interface.

2.2.2.1 Generic Message Transport Level Acknowledgement Messages

By default, the HealthLink SIX client is configured to request an acknowledgement message be generated and sent by the HealthLink SIX client receiving the generic file. The transport level acknowledgement is confirmation that the recipient has successfully downloaded the file. It does not confirm that the file has been loaded into their practice management system.

The acknowledgement message consists of two records separated by a carriage return (0x0A) character. The description is as follows:

Record Identifier	Record Name
MSG_HDR	Message Header
MSG_ACK	Message Acknowledgement

A record is composed of multiple fields. The fields are of variable length and delimited by a vertical bar character (“|”).

The MSG_HDR record will have the following contents:

Seq	MAX Len	Format	Reqd/ Optn	Field name
		XX_XXX	reqd	Record Identifier, MSG_HDR
	4	(14)	reqd	The original sender who is recipient of this acknowledgement message.
		XXXX_XXX	reqd	Message type IMS_ACK – IMS acknowledgement AETNA_ACK – AETNA acknowledgement BROAD_ACK – Broadcast acknowledgement
		99	reqd	Message version (001)
	0	(30)	reqd	Sending facility The name of the sender
	0	(30)	reqd	Receiving facility The name of the recipient
	4	YYYMMDDH HMMSS	reqd	Date/time of message format YYYYMMDDHHMMSS

The MSG_ACK record will have the following contents:

Seq	MAX Len	Format	Reqd/ Optn	Field name
		XX_XXX	reqd	Record Identifier, MSG_ACK

		(2)	reqd	Acknowledgement Code [AA, AR]
				AA = Application Accept
				AR = Application Reject

	27	(127)	reqd	The original file name being acknowledged
	55	(255)	optn	Error Text

Below is a sample acknowledgement message:

```
MSG_HDR|auck_gp|IMS_ACK|001|ims|auck_gp|19990121153912
MSG_ACK|AA|The original filename.txt
```

The name of the acknowledgement file will be the same as the name of the data file, but with an ‘ack’ extension. For example, the sender will receive the acknowledgement ‘abc.ack’ for the original data file sent as ‘abc.txt’.

Example - Sending file to hlknetse, from sectst03 – filename mike.txt

MSG_HDR|hlknetse|PIT_ACK|001|sectst03|hlknetse|20021121094344
MSG_ACK|AA|mike.ack

2.2.3 The MessageSpec Interface

Through the MessageSpec Interface, HealthLink SIX provides the user with a number of options and a great deal of control regarding the format and specifications of messages sent and received.

2.2.3.1 MessageSpec Options

A number of options are available for each message type. These options are specified separately for each different type of message. To access these options, select the message specification to configure from the upper panel of the MessageSpec interface, and click on the “Options” tab.

Request Acknowledgement Messages?

Select “Yes” to request HealthLink message-level acknowledgements for messages sent by this client. Please note that this has no effect on application-level acknowledgements, e.g. laboratory acknowledgements generated by Practice Management Systems.

Compress Outgoing Messages?

Select “Yes” to enable compression on outgoing messages of this type. Messages are decompressed automatically by the recipient HealthLink Messaging client. Compressing messages reduces the amount of data that has to be transferred and therefore lowers connection times.

Prefix Senders EDI Account to filename?

Select “Yes” to add the EDI account name of the sender to the beginning of the filename of all incoming files of this type. For example, a file named result1.edi from a sender with EDI account name testlab would be renamed as (testlab)result1.edi when this option is enabled.

Archive Ingoing/Outgoing Messages?

Select “Yes” to archive the ingoing/outgoing files sent/received through HealthLink. This is recommended if the user wishes to keep a record of all files sent/received. The user can also specify the number of days that the files remain archived on your system.

2.2.3.2 MessageSpec Message Stores

File Base Interface

This interface allows the user to specify which directories on the local system will be used to interface HealthLink SIX with third-party software e.g. a Practice Management System (PMS) or Laboratory Information System (LIS). Files that are to be sent or received by HealthLink SIX reside in these directories until either processed by the HealthLink SIX client or imported by the PMS or LIS.

To access this interface, select the message specification to configure from the upper panel of the MessageSpec interface in the Advanced Options, and click on the “Message Stores” tab below. Then choose “File Based” radio button.

The user can select “Edit/More” button to pop up “Message Directories” dialog for modifying message directory options.

Outgoing Message Directory and Error Directory

Files of this message type that are to be processed and sent by HealthLink SIX should be placed in this directory. Files rejected by HealthLink SIX during message processing are stored in the error directory.

Incoming Message Directory and Error Directory

Files received and de-processed by HMS are stored here. Files rejected by HealthLink SIX during message de-processing are stored in the error directory.

Acknowledgement Directory and Error Directory

The acknowledgement directory is used if the user wishes to keep incoming acknowledgements for this message type in a separate directory to the regular incoming messages of this type. If it is required to keep incoming acknowledgements that have been rejected by HealthLink SIX separate from other rejected incoming messages of this type, the directory to use for rejected acknowledgements is specified as the acknowledgement error directory.

Archive Directories

Incoming and Outgoing files for archiving (if archiving is selected for this message type) are stored in this directory.

MDM in LAB2 Directories

For Australia MDM message, there is a radio button “Use LABRESULT2 Folder” in “Message Directories” popup to indicate where MDM message should be delivered in the directories configured for LAB2.

Web Service Interface

This interface allows the user to specify which web service urls that third-party software e.g. PMS or LIS is listening on for importing incoming messages. To access this interface, select the message specification to configure from the upper panel of the MessageSpec interface in the Advanced Options, and click on the “Message Stores” tab below. Then choose “Symmetric Web Service” radio button.

The user will then need to select “Edit/More” to change the incoming web service urls.

Outgoing message from PMS or LIS to the local HMS Client MessageExchange Web Service Endpoint “[http://localhost:5099/ hmswsv1_2/MessageExchange](http://localhost:5099/hmswsv1_2/MessageExchange)” will be processed and sent to message recipient. And message from outgoing directory will also be processed and sent to message recipient.

All error and archive messages will still be configured as “File Based”.

Incoming Message Web Service URL

Messages received and de-processed by HMS Client are going to send to this MessageExchange web service endpoint instead of being stored in the corresponding incoming message directories.

Acknowledgement Message Web Service URL

Acknowledgements received and de-processed by HMS Client are going to send to this MessageExchange web service endpoint.

2.2.3.3 MessageSpec Processor

HealthLink SIX allows users to receive messages in a variety of formats using a number of advanced features. The configurations for these features are available through this interface.

To reach this interface, select the message type to configure from the upper panel of the MessageSpec interface, and click on the “Processor” tab below.

Application Type allows the user to specify a different name for this type of message on the HealthLink SIX network. We recommend that this not be changed from the Message Specification name - to avoid confusion. The exceptions to this recommendation are any Message Specifications that are set up by default when the HealthLink SIX client software is installed; some of these have different Message Type names for backwards compatibility reasons.

The message specification should also be configured to be either a Generic or Structured message file. Generic files are not parsed or validated by HealthLink SIX, nor can they be mapped (translated) from one format to another.

2.2.3.4 Generic File Processors

Unlike structured messages, HealthLink SIX cannot retrieve the recipients EDI account from the receiving facility field of the structured message (HL7/FF/EDIFACT/XML), as the message format is not specified.

The HealthLink SIX Client has a number of different processors for addressing these generic messages. These different processors can retrieve the EDI account name from the file, the filename or by knowing which directory the file is being sent from. Each of these options is discussed with examples as below.

Recipient Embedded in File

This processor requires all messages to be placed in a single folder, and the messages are addressed based on specific and consistent format/content within each file. The processor looks for a predefined start and finish delimiter within each file, and expects to find the recipients HealthLink EDI account between the start and finish delimiter.

Note : - The HealthLink EDI account usually conforms to an 8 alpha character code depicting the recipient practice. For example, Sander Medical Centre might be issued an EDI account of 'sandermc'

The default setup for this, is to set the start delimiter equal to HLK#, and the finish delimiter equal to # Therefore, the client expects to check through the content of the message and find a string similar to HLK#ediaccount# (where ediaccount denotes the recipients EDI account). The start and finish delimiter can be configured as required (including the use of carriage returns). The user has the option of removing the start delimiter, EDI account and finish delimiter from the contents of the file using this message processor.

Recipient Embedded in Filename:

This processor requires all files to be placed into a single folder, and the messages are addressed to the recipients EDI account based on the filename.

This processor can be configured in a number of ways:

Remove End Enumeration Digits

The default setup for the Recipient Embedded in Filename, is to remove the end Enumeration digits from the filename. This means that HealthLink expects to have a file of name format ediaccountXXX.ext, where ediaccount denotes the recipients 8 character HealthLink EDI Account - XXX is a string of numeric characters of varying length - and .extis the file extension. The client will remove the extension, remove the numeric characters and then address the message to the remaining characters - in this case 'ediaccount'

Remove the Last X Characters

With this option, the user can specify to remove the last X number of characters (where X denotes a user specified numeric value) from the right hand side of the filename (excluding the file extension), to address the file.

With a filename of format ediaccountXX.ext, and configuring the client to remove the last 2 characters, the processor will remove the extension, then remove the last 2 characters, and will address the message to 'ediaccount'

Use the first X Characters

With this option, the user can specify that the client use only the first X number of characters (where X denotes a user specified numeric value), from the left hand side of the filename, to address the file. With a filename format of ediaccountxxxxxxx.ext, and configuring the client to use the first 10 characters, the processor will take the first 10 characters and address the file in this case to 'ediaccount'.

Using the Filename Recipient Map

An additional feature for the Recipient Embedded in Filename processor is to use the filename-recipient map. This mapping file allows the user to specify sequences of alpha/numeric characters to be aliased to valid HealthLink EDI accounts - the user will need to configure the filename-recipient map for all the users aliases and the users EDI Accounts that the user are sending to before you begin sending messages. This processor is particularly useful if the users LIS addresses files using a doctors ID – which can be mapped to a sites EDI Account.

Please note –

- This filename-recipient map aliasing can be used in any of the configurations above that use the EDI account embedded in filename.

- The alias and EDI account fields are case insensitive.

When using the processor to remove the end enumeration digits, the user may have a filename in the following format: aliasXXX.ext. The processor would remove the extension, remove the end XXX string of numeric characters; leaving the 'alias'. The client automatically checks the filename-recipient map to see if there is an EDI account that it has been aliased to, and will address the file according to the mapping. If no entry is found in the map file then the file is addressed using the 'alias'.

Single Recipient

This processor requires files to be placed into a different directory/folder for each recipient.

A new Message Type is created for each recipient, where the Message Type name is the recipients EDI account name. For each recipient, a new Message Type must be added and configured to send to the correct recipient. Files intended for each recipient EDI account should be placed in the corresponding folder.

If the user wishes to send to Sander Medical Centre, (with EDI account sandermc), the user would need to create a Message Type called SANDERMC, with single recipient, 'sandermc'. All messages for Sander Medical Centre would need to be placed in the outgoing SANDERMC directory within the HealthLink SIX messaging folders.

Use the Filename as the Message Control ID:

The user can choose to use the filename as part of the Unique MessageID Number. This assists with keeping records of the exact files sent through the system.

2.3 HealthLink SIX Directory and Program Files

2.3.1 HealthLink SIX Messaging Directory Layout

The default messaging directory structure created during the installation of HealthLink SIX is “C:\HLINK”. A number of sub-directories are created under the HLINK directory. The exact directory structure is determined by the location selected during installation (New Zealand or Australia) and by the version of HLK SIX being installed.

Please note that the actual directories used are controlled by the configuration of HLK SIX via the Advanced Options UI.

2.3.1.1 New Zealand Installation

Folder	Subfolders	Purpose
FF_in	ACC, BROADCST, CMDHBICS, GPSERVE, DIABETIES, GPSURV, HBL, HEPB, IMS, KIDSLINK, KINDZNET, LAB, MEDDOCS, MIMMS, NHCL, NHCLAIM, RSD, CBG_QUERY, CBG_RESEARCH	Files received in a Flat File format are stored in the appropriate folder after processing. They are then imported to a PMS/LIS system for viewing
FF_out	ACC, BROADCST, CMDHBICS, GPSERVE, DIABETIES, GPSURV, HBL, HEPB, IMS, KIDSLINK, KINDZNET, LAB, MEDDOCS, MIMMS, NHCL, NHCLAIM, RSD, CBG_QUERY, CBG_RESEARCH	Files created in Flat File format within a PMS/LIS are placed here waiting to be processed and sent the next time HLK SIX is run
HL7_in	HBL, HEALTHPAC, HEPB, LAB, REFERRAL, GMS, IMMS, NIR, GP2GP, LAB24NZ, RSD02NZ	Files received in a HL7 format are stored in the appropriate folder after processing. They are then imported to a PMS system for viewing
HL7_out	HBL, HEALTHPAC, HEPB, LAB, REFERRAL, GMS, IMMS, NIR, GP2GP, LAB24NZ, RSD02NZ	Files created in HL7 format within a PMS/LIS and placed here waiting to be processed and sent
LOG		Contains all logs relating to the Healthlink Messaging Client. E.g. error and event logs
other_in	Fax, HLK_HELP, HLK_INST , HLK_REJECTED	Messages sent via the HLK fax service and acknowledgements for files sent to HealthLink support are placed here after processing

other_out	Fax, HLK_HELP, HLK_INSTALL, HLK_REJECTED	Acknowledgements for fax messages and files to be sent to HealthLink support are stored waiting to be processed and sent
Receive	Error	Contains all the received messages that are waiting to be de-processed. All incoming messages are de-processed , which involves decrypting and checking of messages to ensure they meet the correct format before placing them in the correct FF_in or HL7_in subfolder. Any messages that are of an unknown message type are placed in the error subfolder
Send	Error	Stores all processed messages that are waiting to be sent. Outgoing messages are taken from the appropriate FF_out or HL7_out folders and processed, which involves checking the messages to ensure they meet the correct format, compressing, encrypting and signing the message. If for any reason the message cannot be sent, such as being unable to read/retrieve the message, the message will be placed in the error subdirectory. If a message validation error or encryption/decryption error occurs, the message will be placed into the corresponding message rejected folder.

2.3.1.2 Australian Installation

Folder	**Subfolders**	**Purpose**
BROADCST_in	Archive	No longer being used
BROADCST_out	Archive	No longer being used
FF_in	BROADCST, LAB, MEDDOCS, RSD	Files received in a Flat File format are stored in the appropriate folder after processing. They are then imported to a PMS/LIS system for viewing **NOTE:** PIT messages for WA are put in the FF_in\BROADCST folder
FF_out	BROADCST, LAB, MEDDOCS, RSD	Files created in Flat File format within a PMS/LIS are placed here waiting to be processed and sent **NOTE:** PIT messages for WA are put in the FF_in\BROADCST folder
HL7_in	HCONNECT, LAB, LAB2, HIRAD REFERRAL, HIRAD, MDM01AU, RSDAU, NSWEHR	Files received in a HL7 format are stored in the appropriate folder after processing. They are then imported to a PMS/LIS system for viewing
HL7_out	HCONNECT, LAB, LAB2, HIRAD	Files created in HL7 format within a PMS/LIS and placed here waiting to be

	REFERRAL, HIRAD, MDM01AU, RSDAU, NSWEHR	processed and sent
LOG		Contains all logs relating to the HealthLink Messaging Client. E.g. error and event logs
other_in	Fax, HLK_HELP, HLK_INST, HLK_REJECTED, QLDH01RSD	Messages sent via HLK fax service and acknowledgements for files sent to HealthLink support are placed here after processing
other_out	Fax, HLK_HELP, HLK_INST, HLK_REJECTED, QLDH01RSD	Acknowledgements for fax messages and files to be sent to HealthLink support are stored waiting to be processed and sent
PIT_in	Archive, Rejected	Files in a PIT format are downloaded to this folder. They are encrypted as normal during the sending process. As they are a generic message they do not require the same checking process as a Flat File or HL7 message. Messages can be stored in the archive subfolder by enabling this function in the HMS advanced options
PIT_out	Archive, Rejected	Files in a PIT format are sent from here. As they are a generic message they do not require the same checking process as a Flat File or HL7 message. Pit files are encrypted during the sending process. Messages can be stored in the archive subfolder by enabling this function in the HMS advanced options
Receive	Error	Contains all the received messages that are waiting to be de-processed. All incoming messages are de-processed , which involves decrypting and checking of messages to ensure they meet the correct format before placing them in the correct FF_in or HL7_in subfolder. Any messages that are of an unknown message type are placed in the error subfolder
Send	Error	Stores all processed messages that are waiting to be sent. Outgoing messages are taken from the appropriate FF_out or HL7_out folders and processed, which involves checking the messages to ensure they meet the correct format, compressing, encrypting and signing the message. If for any reason the message cannot be sent, such as being unable to read/retrieve the message, the message will be placed in the error subdirectory. If a message validation error or encryption/decryption error occurs, the

		message will be placed into the corresponding message rejected folder.

2.3.1.3 Multiple Accounts Messaging Directories.

Where multiple EDI Accounts are installed using a single installation of HMS SIX the first account installed will use the HLINK messaging directory structure outlined above. Each subsequent account will have its own full set of messaging directors created below the HLINK directory using the EDI Account name.

For example, we install three EDI Accounts in the following order: EDI1, EDI2, EDI3

The messaging directories for EDI1 will be, by default, C:\HLINK\ etc

The messaging directories for EDI2 will be C:\HLINK\EDI2\ etc

The messaging directories for EDI3 will be C:\HLINK\EDI3\ etc

2.3.2 Program Files

Folder	Purpose
HealthLink SIX Client Software/Jars	Contains the HMS application as well as updateable definitions that define structured messages for validation services.
HealthLink SIX Client Software/Jre	Contains the Java Run time engine used by the HMS client (self-contained).
HealthLink SIX Client Software/Security	Holds certificate and security information needed for HMS to connect and encrypt and decrypt messages
HealthLink SIX Client Software/.install4J	Contains the information required to uninstall HMS.
HealthLink SIX Client Software /admin	Log files, performance file, profile uploading
HealthLink SIX Client Software /Licenses	Component libraries licenses
HealthLink SIX Client Software /updates	For HMS client software updates
\\hlkvm-smdejbca\c$\Program Files (x86)\Healthlink\HealthLink Quantum/hmsonline	HMS online (synchronous) web service, online forms and proxy functionality.

2.3.2 Configuration File

The HMS client comes with a file ‘hms_config.xml’ Which contains the locations of the all the directories that are in use. This can enable an interfacing EMR to parse and automatically configure input directories to scan and output directories to use for sending. Further details of this file are in the “HMS Interface File Technical Documentation” please contact our Vendor team for a copy.

2.4 Features and Functionality

2.4.1 Connection Options

HealthLink SIX can connect to the messaging servers in one of three different ways:

- LAN – Over a permanent Internet connection available to your Local Area Network
- VPN – By making a dial-up connection to the HealthLink VPN

To view the connection method you are using, select “Global Settings” from the “Configuration” menu within Advanced Options and then click on the “Connection” tab.

2.4.1.1 Using the connection Tester

You can also check your connection to the three URLs that HealthLink SIX utilises by running the connection tester.

Running this test will prompt a resolution of the URLs to the IP Addresses and then try connecting to them. You can see the results individually from each IP address and determine if there is a problem connecting to any address.

2.4.1.2 Http Proxy Negotiation

It is possible to connect to HealthLink via a Proxy Server.

To set this up you will need to tick the option “use Proxy Server” and specify the IP Address and the port number of the host. If your proxy requires authentication and is Base64 encoded, you can still connect to HealthLink by specifying your username and password in the fields below. Other authentication methods are not supported. However, for some proxies you can work through authentication issues e.g. if you are using Microsoft's ISA server you can install HLK SIX on another computer on your network, along with the ISA firewall client.

Please note: The connection tester will not run when you choose to connect via a Proxy Server.

2.4.2 System Directories

To view or change the directories used internally by the HealthLink Messaging System, select “User Settings” from the “Configuration” menu within Advanced Options and click on the “System Directories” tab.

To make changes to the values of these fields, either type in a new value or click the “...” buttons to browse to a directory.

Please note: These directories are for internal use by the HealthLink SIX client and under normal circumstances users will not interact directly with these directories. In particular, these directories should not be confused

with the sending and receiving directories specified through the MessageSpec interface (see Section 2.3.2 for details of this).

2.4.3 Modes of Operation

2.4.3.1 The HealthLink Scheduler

HealthLink SIX can be configured to run continuously on your computer and to connect and exchange messages automatically as often as every 30 minutes. This means that you can launch the HealthLink SIX application once and then leave it to connect at scheduled times until you decide to close the application.

To enable this feature, select “Global Settings” from the “Configuration” menu within the Advanced Options Interface. This screen opens by default when you launch HealthLink SIX Advanced Options.

Click the “Scheduler” tab, and change “Mode of Operation” to Unattended.

You should also consider changing the values for the other fields:

Start Time - the time of day to make the first connection.

Stop Time - the time of day after which no more connections are to be made.

Sleep Period - the number of hours and minutes to wait between consecutive connections.

Close Period - the number of minutes and seconds to leave the HealthLink SIX Window open after the application has been closed.

Exclude Saturdays and Sundays - allows you to limit connections to week days.

2.4.3.2 Scheduling Batch/Executables

The built-in scheduler allows the user to run .bat or .exe files before and/or after a connection has been run.

From the Scheduler tab, you can browse to find the selected commands, or type the commands in manually as shown below:

Please Note – The batch files/executables must not require user intervention such as confirmations or button presses to continue, otherwise the HealthLink SIX client cannot run (as it will be waiting for the batch file prompt to be answered).

2.4.3.3 Running HealthLink Messaging System as an NT Service

Please note: this functionality exists only under Microsoft Windows NT, 2000, XP and 2003 Server. NT Services will not run under other operating systems.

HealthLink SIX can be configured to run as an NT Service, to allow continuous operation independently of whether there is a user logged into Windows.

This can be configured under the NT Service tab within the Advanced Options. You will need to specify the EDI accounts that will be logged on and then install and start the service.

By default the service will be installed under the local system account and may not have privileges and rights that the current user does for diallers, passwords and network access. You can choose to run the service under a specific Windows user account. You will need to know the domain name (if applicable), username and password.

2.4.3.4 System Tray Icon for NT Service

When you install HealthLink SIX as an NT Service, you will have a system tray icon installed from which you can: force the client to run, stop, or uninstall the service. By right-clicking on the icon you also have access to the error and event logs.

There are system tray icons, depending on the current state of the service:

This icon indicates that the service has been installed, but is not started. Right-click on the service icon and choose to start the service.

... This icon indicates that the service is installed and running successfully.

... This icon shows when HMS is running a connection to the servers

... This icon indicates that the last time HealthLink SIX tried to connect, it failed. If this icon is displayed, please refer to your log to determine what the cause of the connection failure was and contact the helpdesk for assistance if required.

2.4.3.5 Running HealthLink Messaging System in Unattended (Auto Login)

Please note: this functionality exists only under Microsoft Windows NT, 2000, XP and 2003 Server. Unattended Auto Login will not run under other operating systems.

Unattended Mode using Auto logon runs using the same schedule as if it was running as a NT service but the computer needs to remain logged on at all times to ensure the clients as per the scheduled times.

If the computer is restarted or logged off for any reason it will automatically restart and login without the need to enter a connection password.

This mode is only recommended if a user account is required to access a network drive for exchanging messages between HMS and the EMR. If the NT service mode is used when a network drive is in use for exchanging messages, then there are sometimes problems if the password expiry cannot be disabled on the service account - interrupting the service.

2.4.3.6 System Tray icons for Unattended (Auto Login)

An icon like this one will appear in the system tray, the client will also be minimised to the system tray.

If the HMS client fails to connect at the schedules time the icon will appear with a red flashing centre.

2.4.3.7 Restricted Files

HealthLink SIX gives you the power to select the types of files (using file extensions) that can be sent and received through the HealthLink SIX client. This is very important for generic file transfer and the default restricted file extensions have been selected to stop files that could potentially carry computer viruses. These include files such as executables and scripts.

If the name or extension of an incoming or outgoing file indicates that the file may contain harmful code, the file is moved to a “rejected” folder and renamed to prevent execution.

To add another file mask to the list, click the “Add” button. File masks may also be edited or removed by clicking on the appropriate buttons.

2.4.4 Logging and Archiving

All connections, file transfers and errors encountered in verification, translation or transmission detailed in human and machine-readable log files at the client end.

2.4.4.1 Logging Options

HealthLink SIX allows the user to configure some aspects of the application logging from the Advanced Options. This includes:

Log File Size

The size in (kb) the log file will grow to before being backed-up or overwritten.

Number of Backups

The number of rolled-over logs that the client will keep (of size specified above) before the client permanently deletes the oldest backup.

As an example, if Size were set to 200kb and Number were set to 3, HealthLink SIX would allow the log to grow to 200kb in size before archiving it, and would keep three log archives (a total of approx. 800 kb).

2.4.4.2 Sending Log Files to HealthLink Support

To assist our users and support team in troubleshooting messaging issues, HealthLink SIX contains functionality to easily and securely send log files to the helpdesk team over the HealthLink EDI network.

This feature is available via the utilities menu in the advanced options where a list of current log files and profiles can be selected to be packaged, compressed and sent to the ‘hlksuprt’ EDI account at HealthLink on the next successful connection.

In most cases the event.txt, error.txt, user.profile and system.profile files will be requested by the helpdesk staff, though the HealthLink support provider will assist in determining which files are required.

The Log File Sender will prepare a package of files which will be sent to HealthLink Support the next time the HealthLink SIX client connects to the HealthLink EDI network.

The rejected file sender uses the **HLK_HELP** MessageSpec type for file transfer.

Please note: This utility will not assist when the problem is connection related. Please contact HealthLink Support by phone or by email if you are having problems, before sending log files. Our support team cannot respond to unsolicited log files that are received.

2.4.4.3 Printing Log Files

HealthLink SIX users occasionally need to send log files to the Support team by fax. HealthLink SIX can simplify the process of printing out the last few days’ worth of log entries.

The log file printer is found in the Utilities menu in the Advanced Options. Each log file can be individually selected and viewed within the viewing pane. A specific timeframe in weeks/days/months can be selected to be viewed and the applicable log content printed – Using the default printer.

2.4.5 Sending Rejected Files to HealthLink Support

To assist our users and support team in troubleshooting message formatting issues, HealthLink SIX contains functionality to send files that have been rejected due to formatting problems to the HealthLink Support team over the secure HealthLink EDI network.

This feature is available from the Utilities menu of the Advanced Options. By simply clicking on the Package button, a copy of all rejected incoming and outgoing files will be compressed and packaged in preparation for transmission to the Support Team. This packaged file will be sent on the next successful connection through to the ‘hlksuprt’ EDI account for the HealthLink team to look at.

The rejected file sender uses the HLK_REJECTED MessageSpec type for file transfer.

Please contact HealthLink Support by phone or by email if you suspect that you are having message formatting problems, before sending your rejected files. Our support team cannot respond to unsolicited files that are received.

2.4.6 Support for Multiple Accounts on a Single Installation

Multiple EDI Accounts can connect to HealthLink via a single HealthLink SIX client installation. The maximum number of accounts that can connect from a single installation is 10, and requests for multiple accounts on one installation are considered on an individual basis.

Adding additional accounts is done via the User Settings menu in the Advanced Options. When creating additional users it is recommended to copy the existing profile settings (and is specified by default) to retain all currently available message types for the new account. Once the account has been added and the EDI account and Password entered, the keys will need to be installed for this user using the Security Tool under the Utilities Menu.

From this interface changes can be made to the EDI Account name and password as required.

2.4.7 Certificate Details

You can check the details of your current certificates by clicking on the certificate details tab from “Utilities” drop down menu->”Security Tool”. You will be required to enter your passphrase before any certificate information is displayed. Once the correct passphrase has been entered you will be able to check details such as the certificate issuer, certificate serial number, date issued, and expiry date.

2.5 The User Interface

The user interface gives information in plain English detailing connecting, file transfer and file processing information. The details in the application window are all recorded in the event.txt file which can be accessed from the link to the HealthLink SIX log on the desktop, for post connection investigation/checking.

The sequence of events reflected in the user interface are:

- HealthLink SIX establishes a secure, authenticated connection to our EDI services using the connection specified during the installation (multiple URLs).

- All outgoing messages are processed (including parsing and translation where applicable). For structured messages all sending facility fields are updated, where required, to the EDI Account name of the user who is actually sending the files. Negative acknowledgement is generated and saved in its corresponding incoming directory for message that fail validation or wrongly addressed. Oversize message will not be delivered and get moved to its corresponding outgoing rejected directory.

- The required public keys are downloaded (these are currently cached for 3 hours by default) and the messages encrypted.

- The message is signed using the sender's private key and sent to the EDI Servers.

- All incoming messages are retrieved by the HealthLink SIX client.

- The required public keys are downloaded and the signature verified.

- The files are decrypted using the sites private key.

- The incoming files are processed and written to the respective incoming directories. Negative acknowledgements are generated and sent for messages that fail validation.

- Meta-data about the connection and files transferred are written to the HealthLink EDI database in real time.

2.6 URLs and Connection Information

All outbound connections are established on port 443 for Internet connections.

Type	Internet URL
NZ Primary	connections.hms.nz1www1.healthlink.net
	edi.hms.nz1www1.healthlink.net
	quantum.hms.nz1www1.healthlink.net
AU Primary	connections.hms.au1www1.healthlink.net
	edi.hms.au1www1.healthlink.net
	quantum.hms.au1www1.healthlink.net
CA Primary	
	edi.hms.ca1www1.healthlink.net
	quantum.hms.ca1www1.healthlink.net

Please contact HealthLink Ltd if you need to connect to HealthLink over the HealthLink Frame Relay or the Health Intranet.

3.0 Other Services

3.1 HealthLink Online Services

3.1.1 Purpose

HealthLink's range of secure online services comprise of a number of web-based applications, accessed through a web browser. The applications include monitoring tools for each customer’s own EDI activities, as well as other resources such as a Provider Directory and integrated EDI and Online disease management projects.

New services are being added constantly. Currently available applications include:

- HealthLink User Online – tools that monitor EDI traffic sent to or from a customer’s EDI account and track acknowledgements received for transmitted messages.

- Provider Directory – a dynamic, cross-referenced list of local health providers, facilities, organisations and services.

- NHI Lookup – a service that returns the National Health Index number for New Zealand residents.

- Disease management applications for HealthLink disease management projects e.g. HepB Free

- Online forms and the HISO/Aduro interfaces for EMR data exchange

- SMD Australian Secure Message Delivery

3.1.2 Requirements

The HealthLink Online Services are accessed using a Browser such as Microsoft Internet Explorer 7+ or Firefox

3.1.3 URLs

HealthLink User Online is accessed using different URLs depending on your method of connection, as can be seen below.

Connection	URL	Protocol
NZ Internet	secure.healthlink.net	HTTPS
NZ VPN	extranet.healthlink.net	HTTPS
AU Internet	secure.healthlink.net	HTTPS
AU VPN	extranet.healthlink.net	HTTPS

4.0 Security

4.1 Security Overview

HealthLink Messaging System uses end-to-end 128-bit PKI encryption for EDI. X509 v3 compliant certificates are used to:

HealthLink SIX EDI:

Uses end-to-end 128-bit encryption (Public / Private Key) for EDI

- Data is encrypted using the DESede (Triple DES) algorithm in CBC mode with PKCS #5 padding, using 192 bit session keys. The session keys are encrypted using the RSA algorithm in ECB mode with PKCS #1 padding. The encrypted data is signed using SHA1 with RSA. Separate keys are used for signing and encryption. Private keys are held on the user's local machine in a PKCS #12 format encrypted and password-protected file. Public keys are held on a central HealthLink server.

Uses x509 v3 compliant certificates to:

- Encrypt the message so that only the intended recipient can view the contents of the message

- Authenticate the sender and verify the integrity of the message using a digital signature

- Authenticate users logging onto the network and control access to applications (EDI and Online services)

- Identify the HealthLink EDI and Web Servers

- Encrypt the payload so that only the intended recipient can view the contents of the message

Provides 128-bit SSL between the client and the online applications

Provides extensive message tracking and management tools

HealthLink Online Services:

- Operate using an internationally recognised server certificate – to prove the identity of our site and provide 128bit SSL. Our client side software installation upgrades the client to IE5.5 to allow 128 bit SSL connections to our web servers.

- Require a client certificate to access the login page. This proves the identity of the client allowing us to limit access to the Online Services through the use of digital signatures.

The HealthLink servers are located on site in a secure temperature controlled server room. This room is always locked and has a monitored alarm system with restricted access available to very few individuals. All servers require login/password identification.

All HealthLink servers are connected to an uninterruptible power supplys (UPS) and run a RAID array (mirrored hard drives) for redundancy. All data is backed and stored securely offsite. All data on the backups are encrypted.

HealthLink maintains an offsite backup of each of the essential servers in an equally secure environment. These are synchronised on a nightly basis with the live servers.

All HealthLink servers and staff workstations run anti-virus software with the latest virus definitions.

4.2 The HealthLink CA and RA

HealthLink offers Certification Authority (CA) and Registration Authority (RA) PKI services for HealthLink SIX Client. Certificates issued by HealthLink trusted third party CAs can also be supported by import process.

4.2.1 HealthLink Certificate Profile

Here is the current HealthLink Certificate Profile which will be revised before the end of year 2014:

- Key usage for signing and encryption
- Extended key usage for client authentication (TLS)
- Signature algorithm SHA128
- RSA key size 1024 bits

4.2.2 CSR Triggers and Processes

Certificate Signing Requests are generated and sent by the HealthLink SIX Client when new certificates are required.

This is generally an automated procedure carried out without the user having to do anything. The exception is the “One Time Password for Request New Keys” function.

There are 3 triggers that set this process into action:

One Time Password for Request New Keys

This would be done during the fresh installation of the HealthLink SIX client, or where the site is concerned that the keys have been compromised. For example, disk lost or stolen, passphrase given to someone else.

User will be prompted for a onetime password given to the user by HealthLink during installation. Two new key pairs (cipher and signature) will be generated locally and used for generating two CSRs.

The two CSRs (cipher and signature) are then sent to the HealthLink RA server along with the onetime password. If the HealthLink RA server accepts the onetime password, it will process the two CSRs and send back the two newly signed certificates in the response.

The new certificates and the corresponding private keys will be saved into the 'security' folder under the HealthLink SIX Program File folder for the site's EDI account. When the new certificates are successfully stored, two certificate activation requests will be sent to the HealthLink RA server for making the new certificates to be the current active certificates of the site's EDI account. From this point on these new keys will be used for signing and decryption and this normally happens during the next scheduled connection.

Expiring Certificates

4 weeks before the current certificate expire, a CSR is generated along with signature signed with the current signing key of the site's EDI account and sent to the HealthLink RA server. If the HealthLink RA server successfully verifies signature, it will process the CSR and send back the newly signed certificate in the response. When the new certificate is successfully stored locally, a certificate activation request will be sent to the HealthLink RA server for making the new certificate to be the current active certificate of the site's EDI account. From this point on the new key will be used for PKI.

3rd Party Certificates are about to expire

4 weeks prior to third party certificate expiring a message is written to HealthLink SIX logs and warning of impending expiry appears in HealthLink SIX client window.

1 week before third party certificate is due to expire (if they have not had new ones installed) a HealthLink CSR is sent to HealthLink to ensure continued connectivity for the site. This process is the same as the process for HealthLink certificates described above.

4.2.3 Third Party Key Certificate Import

The process for key/certificate import is as below:

1. Import the 3rd party certificates from the Advanced Options -> "Utilities" Menu->"Security Tool" Item->"Key Import" Tab. The 3rd party private key will be stored locally as .import file in the security directory. The corresponding certificate (which contains public key only) will be put into a certificate registering request along with the signature signed with the current signing key of the site's EDI account and sent to HealthLink RA server for approval.

2. HealthLink RA server will verify the request signature and validate the 3rd party certificate embedded in the request. Only certificates which are issued by

HealthLink trusted Certificate Authorities (CAs) and within certificate validity period will be accepted by HealthLink RA server. The accepted 3rd party certificate will be store on the server and then monitored by HealthLink RA server for revocation and expiry.

3 The response will be sent back synchronously to the site’s HMS installation after successfully importing certificate into HealthLink RA server. HMS Client software will then replace the current key store with newly imported key store and back up the old key store.

4 Upon successful current key store replacement, a certificate activation request will be sent to the HealthLink RA server for making the new certificate to be the current active certificate of the site’s EDI account. From this point on the new key will be used for PKI, and this normally happens during the next scheduled connection.