|  |
| --- |
| Document filename:  |
| Directorate / Programme | OTS - GPSoC | Project | GPSoC |
| Document Reference | HSCIC-FNT-TO-TAR-0082.02  |
| Project Manager | Shaun Fletcher | Status | Published |
| Owner | Mike Curtis | Version | 1.1 |
| Author | Brendan McEnroe | Version issue date | 14/05/2014 |

CDA Interoperability - MHS Requirements

Document Management

Revision History

|  |  |  |
| --- | --- | --- |
| Version | Date | Summary of Changes |
| 0.1 | May 2011 | 1stdraft |
| 0.2 | July 2011 | 2nd draft |
| 1.0 | 15th Aug 2011 | Approved version |
| 1.1 | 14/5/2014 | Brendan McEnroe – Uplift following supplier engagement |

Reviewers

This document must be reviewed by the following people: author to indicate reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewer name | Title / Responsibility | Date | Version |
| Mike Curtis | Lead Technical Architect GPSoC |  |  |
| Adam Hatherly | Senior Solution Architect |  |  |

Approved by

This document must be approved by the following people: author to indicate approvers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Signature | Title | Date  | Version |
| Mike Curtis |  | Lead Technical Architect GPSoC |  | 1 |
|  |  |  |  |  |

Distribution

This document will be distributed to:

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewer name | Title / Responsibility | Date | Version |
| GPSoC Suppliers |  |  | 1.0 |
|  |  |  |  |

Related Documents:

The table below lists other related documents, which should be understood in the context of this document:

|  |  |  |  |
| --- | --- | --- | --- |
| Ref No | Doc Reference Number | Title | Version |
|  |  |  |  |
|  |  |  |  |

Glossary of Terms

|  |  |  |
| --- | --- | --- |
| Term | Abbreviation | What it stands for |
| CDA | CDA | Clinical Document Architecture – an HL7 standard for the structure (format, content) of clinical documents |
| CDA Document | - | An instance of a clinical document in CDA format |
| CRE Type |  | A Care Record Element categorisation predominantly designed for use with the Summary Care Record held on PSIS but also for more general use |
| Domain Message Specification | DMS | A set of documented requirements related to a specific messaging domain covering a range of messages interactions between systems across that domain. This is the successor to the MIM (Message Implementation Manual) that covered many different domains which reached version 8 – all further developments being spawned off into their own domains to become DMSs. |
| Data Transfer Service | DTS | A Store and Collect mail facility operated by BT and now part of the range of ‘Spine’ services |
| Interoperability Tool-Kit | ITK | Interoperability Tool-Kit – a set of technical standards covering the exchange of messages between the messaging components of systems. |
| Point to Point | P2P | Refers to sending messages directly from one system to another either directly or via an intermediary service such as DTS or TMS – in the case of TMS the message travels through TMS to another end point and not to any central sine service |
| Trading Partner | TP | A system and/or organisation which the host system exchanges messages with. An organisation may have many systems each with their own identifier which equates to a Trading Partner ID. A system (with a single Trading Partner ID) may support multiple organisations. Examples include the 5 character cipher used to identify GP systems and NHAIS systems for NHAIS registration links, 15-char EDI Sender/recipient IDs used in Pathology messaging, a Spine ASID, etc. |
| Trading Partner ID | TP | An identifier for a system to identify itself uniquely within messages it sends and/or receives messages electronically with other systems. |

Document Control:

The controlled copy of this document is maintained in the HSCIC corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

This document is valid from: **14th May 2014**

Contents

[1 Introduction 5](#_Toc387827554)

[1.1 Purpose 5](#_Toc387827555)

[1.2 Audience 5](#_Toc387827556)

[1.3 Document Scope 5](#_Toc387827557)

[1.4 Document Overview 6](#_Toc387827558)

[1.5 Definitions 6](#_Toc387827559)

[2 MHS v Application Responsibility 7](#_Toc387827560)

[3 Message Exchange Requirements 10](#_Toc387827561)

[3.1 Trading Partners Configuration 10](#_Toc387827562)

[3.2 Message Logs & Audit 15](#_Toc387827563)

[3.3 Management Information 17](#_Toc387827564)

[3.4 HL7 Payload Construction & Validation 17](#_Toc387827565)

[3.5 Outbound Message Validation 18](#_Toc387827566)

[3.6 Inbound Message Validation 18](#_Toc387827567)

[3.7 Handling Attachments – Anti-Virus Controls 19](#_Toc387827568)

[3.8 Message/Interaction/Service Patterns 20](#_Toc387827569)

[3.9 ‘Transport’ Channel Requirements 21](#_Toc387827570)

[3.10 Missing/Delayed Application/Business Acknowledgements 27](#_Toc387827571)

[3.11 Retry Behaviour 28](#_Toc387827572)

[3.12 Message Output Control 29](#_Toc387827573)

[Appendix A. DTS Workflow IDs 31](#_Toc387827574)

# Introduction

This document specifies the transport layer ‘interoperability’ requirements for systems sending and receiving CDA documents as illustrated in Figure 1. It covers the interface between the ‘MHS’ and the network and provides a list of high level requirements for systems to send and receive CDA documents over TMS or DTS or using ITK web service messaging standards.

Figure CDA Interoperability Architecture

## Purpose

The purpose of this document is to provide detailed requirements to developers of systems sending CDA documents. It must be read and understood within the context provided by the other documents published in the CDA Interoperability baseline.

## Audience

The intended audience for this document is all suppliers involved in the sending and receiving of messages containing Clinical Documents. It may also be of interest to users of systems provided by these suppliers.

This document should also be read by people developing systems that will receive CDA documents as it provides useful information to assist with the understanding the full point to point business and technical processes.

## Document Scope

The scope of this document covers the transport level requirements for sending and receiving CDA documents from the point at which the payload (the CDA document) has been created for sending or received for processing by the clinical application. As such it covers:

* The system configuration requirements needed to route a message
* The system configuration requirements relating to the capability of supported clinical application(s)
* The validation requirements for outgoing and inbound messages containing CDA documents
* Specific requirements relating to supported transport channels

## Document Overview

The diagram below illustrates the scope of the baseline documentation defining requirements across the generic CDA interoperability environment with the area covered by this document circled. Suppliers must read associated documentation from this CDA interoperability baseline in order to comply with the overall requirements for CDA interoperability.



Figure 2: CDA Interoperability Documentation Model

## Definitions

Where used in this document set, the keywords MUST, SHOULD and MAY are to be interpreted as follows:

* **MUST**: This word, or the terms "**REQUIRED**" or "**SHALL**", means that the definition is an absolute` requirement of the specification.
* **SHOULD**: This word, or the adjective "**RECOMMENDED**", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications **MUST** be understood and carefully weighed before choosing a different course.
* **MAY**: This word, or the adjective “**OPTIONAL**”, means that an item is truly optional. One implementer may choose to include the item because a particular implementation requires it or because the implementer feels that it enhances the implementation while another implementer may omit the same item. An implementation which does not include a particular option **MUST** be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option **MUST** be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides).

# MHS v Application Responsibility

The roles of Message Handling Systems (MHS) and Clinical Applications are not clearly defined. Whilst there are some requirements that are clearly the responsibility of an MHS (e.g. ebXML header validation, ebXML retries, SOAP validation), there are others that are clearly the responsibility of an Application (e.g. patient record present on system), there are many which could easily be met by either component (e.g. schema validation of an HL7 Payload). Although the architecture diagram makes a distinction between an MHS and an Application the requirements in this document, for the purposes of clarity and simplicity make no distinction between which component of a solution is used to meet a requirement.

The BT External Interface Specification (EIS) document specifies MHS responsibilities and the text below, taken from this document, provides a useful description of the separation of roles.

[EIS Extract – Start]

An MHS node sits in a layered architecture with respect to the health application sending/receiving messages, and the transport stack that supports MHS communications. That is, an application that wishes to send a message to a national service will compose a message compatible with the service interface and call its local MHS to request the message be sent to the service. The MHS will wrap the service message in the required MHS protocol headers and send it to an appropriate transport stack (one that is compatible with the sender) for transmission over a physical network. At the other end, the receiving MHS will obtain an MHS message from the communications stack, strip off its wrapper(s), and pass the message to the service for processing. This layered architecture is shown in Figure 2.2 below.

Health System

 NHS MHS

National Service

 NHS MHS

Network

MHS-MHS

Protocol Interface

Service Message

MHS Message

Sender

Receiver

Network

Protocols

Network

Protocols

HL7 Message and

Protocol Interface

Network Packets

Network Packets

MHS Message

Service Message

Figure 2.2 -Layered Architecture of the MHS.

This specification describes the behaviour of an MHS, and the protocol between the MHS nodes. Also, a binding is provided to lower layer protocols. The definition of the interface between the application and the MHS is out-of-scope for this specification and is an internal concern[[1]](#footnote-1).

Each MHS node implements common behaviour. At an abstract level the MHS provides the following internal services (see Figure 2‑31):

* Header processing. The creation and processing[[2]](#footnote-2) of (ebXML or web service) header elements. This also includes the parsing of header elements, the interaction with contract properties, and the passing of elements to and from the message service interface.
* Message packaging. The building of the ebXML and web service envelopes, including the ebXML SOAP attachment structure.
* Security. No message level security behaviour is required.
* Reliable message processing. Responsible for the delivery and acknowledgement of reliable messages. This component deals with persistence, retries, error notification, and acknowledgement of messages requiring reliable delivery.
* Error handler. Response for the reporting of errors encountered during MHS processing, including errors across the service interface but not including errors occurring within the application.
* Routing. Responsible for making any routing and address mapping decisions required.
* MHS Service Interface. The abstract interface between the MHS and a system that is sending or receiving messages.
* Transport Binding. The abstract interface between the MHS and the various protocol stacks.



Figure 2.3 - MHS Components.

[EIS Extract – End]

# Message Exchange Requirements

## Trading Partners Configuration

The system must support the configuration of Trading Partners, i.e. those organisations and systems with whom this organisation will send or receive clinical documents to/from. At a transport level this will include information such as a ‘network address’ along with other identifiers used to identify a sender or receiver of messages and which network transport is used. At an application or business level, the system will need to record details of which message types the system will receive from sending organisations and which message types the system will send to receiving organisations, including acknowledgements to received messages.

Such information may be manually or automatically configured, e.g. a sending system may dynamically build up a list of Trading Partners to whom they send messages over TMS as message support capability can be determined from SDS.

Under normal conditions a sender and receiver will agree which transport channel to use and thus sending and receiving systems need to be configured to use this channel. Messages may be received over other channels but will need to be flagged as ‘received over unexpected transport’ should this occur as there may be business and/or financial implications for not using the agreed channel. New message types may also be received and these too will need to be flagged as ‘unexpected message type’ (or rejected if the system doesn’t support it).

The requirements in the table specify the configuration requirements for the sending and receiving of CDA documents over the three transport channels within the CDA Interoperability Architecture (See Figure 1).

| **Req ID** | **Requirement Text** | **Status** |
| --- | --- | --- |
| **CM01** | The system **MUST** be able to record the following information about the local system:* ODS code(s) for the Organisation(s) supported by the system
* The UUID of the system[[3]](#footnote-3)
* Trading Partner Identifier(s) for the system/messaging domain(s)[[4]](#footnote-4) (where appropriate)

And/or TMS connectivity* PartyKey(s) used for Spine messaging
* ASID(s) used for Spine messaging

And/or DTS connectivity* DTS Mailbox ID (or multiple IDs if more than one is necessary)

And/or ITK connectivity* URL(s) for ITK web services messaging
* ITK Address(es) (URIs)
* Supported ITK services
 | Must |
| CM01.1 | The system **SHOULD** restrict add, edit and delete any of the above attributes to supplier support staff.Note: This is functionality should be limited to supplier support staff that need access to configure the trading partners. | Should |
| CM01.2 | The system **MUST** make all these attributes available to view to authorised users of the system (e.g. system administrators)Note: Authorised users are system administration users at the practice. | Must |
| CM01.3 | For Spine (TMS) messaging, the system **MUST** only allow the use of one organisation per ASID – it is not allowable for an ASID to be shared by more than one organisation. | Must |
| **CM02** | The system **MUST** be able to record the following information about each Trading Partner:* Trading Partner details
	+ Trading Partner identifier (where appropriate)
	+ Name
	+ Address
	+ Contact details – telephone, email address
	+ ODS code (where applicable)

And/or TMS details:* URL used for Spine messaging
* PartyKey used for Spine messaging
* ASID used for Spine messaging

And/or DTS details* DTS Mailbox ID (or multiple IDs if more than one is necessary)

And/or ITK details* URL for ITK messaging
* ITK Address (URI)
* ITK service name
 | Must |
| CM02.1 | It **SHOULD** be possible for authorised users to add, edit and delete a non-TMS attribute above. | Should |
| CM02.2 | It **MUST NOT** be possible for any user or supplier support staff to amend any TMS attribute above. These values **MUST** be read from the Spine SDS using appropriate LDAP queries. | Must |
| CM02.3 | TMS values retrieved from SDS **SHOULD** be cached locally and refreshed at intervals recommended by the Authority. | Should |
| CM02.4 | The system **MUST** make all these items available to view to authorised users of the system (e.g. system administrators) | Must |
| **CM03** | For each Trading Partner, the system **MUST** be able to record which messages (interactions) can be received from them.Note: Whilst the message definition identifier is common regardless of transport channel, the ‘Interaction ID’ (as used by TMS) is not used, or is different, across non TMS channels such as ITK we service messaging. There is therefore a need for systems to support BOTH message definition identifiers AND interaction identifiers. | Must |
| CM03.1 | For each of these message types supported the system **MUST** be able to record associated interaction identifiers where these are required. These **MUST** include:* For TMS – the Spine ‘Interaction ID’
* For ITK - the ITK ‘interaction id’

For example:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **HL7 Payload ID** | **Interaction Name** | **Interaction ID** |
| TMS | POCD\_MT150001UK06 | Primary Recipient Discharge Report (Version 6.0) | POCD\_IN150001UK06 |
| ITK | POCD\_MT150001UK06 | Primary Recipient Discharge Report (Version 1.0) | urn:nhs-itk:interaction:primaryRecipientDischargeReport-v1-0 |

 | Must |
| CM03.2 | For each of these messages (interactions) the system **MUST** be able to record which transport channel used to receive them from the following list:* TMS
* ITK web service messaging and the corresponding ITK service that will be used
* DTS
 | Must |
| **CM04** | The system **MUST** determine the capability of a receiving system to receive messages over TMS by querying SDS to identify whether the system supports the receipt of the appropriate message interaction ID by checking the ASID (to see if supported) and the associated MHS entry to see if it can be received. (NB The ASID only indicates whether the interaction is supported and does not indicate whether for sending or receiving whereas the MHS only contains interactions that can be received). | Must |
| CM04.1 | Where such interactions are found to be supported, the system **MUST** also retrieve the appropriate ebXML contract properties for that system from SDS. | Must |
| CM04.2 | The system **SHOULD** cache values retrieved from SDS for a maximum of 24 hours to remove the need for SDS lookups for each send event. If caching is supported, the system **MUST** provide a mechanism to refresh the cache in case it is out of date. The refresh maybe performed by supplier support staff if a SDS entry is known to have changed in the last 24 Hrs. | Should |
| **CM05** | For each Trading Partner, the system **MUST** be able to record which messages (interaction) types can be sent to them. These SHOULD be identified by InteractionID as specified in the MIM/DMS. | Must |
| CM05.1 | For each of these messages (interaction) type the system **MUST** be able to record which transport channel is used to send messages to them from the following list:* TMS
* ITK web service messaging and the corresponding ITK service that will be used (e.g. SendCDAdocument v2.0)
* DTS
 | Must |
| CM05.2 | For each of these messages (interactions) types the system **MUST** be able to record the default (agreed) transport channel to be used | Must |
| CM05.3 | Systems **MAY** support the sending of messages over non-default transport channels in exceptional situations, (e.g. default channel is unavailable, to support testing of new communications). NB. Suppliers who intend to support this functionality need to provide clear details of how this will operate. | May |
| **CM06** | The system **MUST** allow inbound messages to be received from unrecognised senders.  | Must |
| CM06.1 | When the system receives a message from an unrecognised sender, the system:* **SHOULD,**  either automatically, or via user confirmation, create a new Trading Partner record using details from the received message, and
* **MUST** flag the message as ‘received from an unrecognised sender’

(See ‘CDA Interoperability Receiver Requirements’ for further requirements). | Must/Should |
| **CM07** | The system **MUST** allow unrecognised or unsupported HL7 CDA documents (i.e. message interactions) to be received from recognised Trading Partners and from unrecognised Trading Partners (subject to the configuration setting (CM06)) or over non-default transport channels.Note: An unrecognised CDA document will be able to be processed, albeit with some limitations, by the system as part of the general CDA handling requirements specified in the ‘CDA Document Receiver Requirements’ document. | Must |
| **CM08** | The system **MUST** provide appropriate access controls to configuration data, e.g. restrict view and update access to such data according to a users RBAC profile. | Must |

## Message Logs & Audit

| **Req ID** | **Requirement Text** | **Status** |
| --- | --- | --- |
| **CM10** | The system **MUST** record in a ‘message log’ the following fields:1. An indication of whether the messages was sent or received
2. Date and time sent/received (NOT the date/time within a CDA document or ‘wrapper’)
3. Transport Channel/Method (i.e. TMS, DTS, ITK)[[5]](#footnote-5)
4. Transport Channel Identifier (e.g. TMS ASID, DTS Mailbox, ITK Address)
5. Trading Partner ID (where present)
6. Trading Partner Status (recognised, unrecognised)
7. Message/Interaction type Identifier
8. \*Message/Transmission ID (e.g. TMS message GUID)
9. Interaction status (i.e. supported, not supported)
10. Transport Channel Receipt Status (awaiting, success or error)
11. Application/Business Acknowledgement status (awaiting, success, error) where appropriate
12. \*Application/Business Acknowledgement Message/Transmission identifier (e.g. UUID from appropriate TMS/ITK wrapper or DTS control file)
13. Date and time send/received for the Application/Business Acknowledgement (where appropriate)
14. Error Code and Description received (where applicable)
15. Message size (including any attachments) in bytes
 | Must |
| CM10.1 | The Trading Partner (TP) Status field **MUST** indicate whether the TP was unrecognised. | Must |
| CM10.2 | The Interaction Status field **MUST** indicate whether the message (interaction) was unsupported. | Must |
| CM10.3 | It **SHOULD** be possible to order the message log by any of the fields listed above (except those marked with an \*). | Should |
| CM10.4 | It **SHOULD** be possible to filter the message log by any of fields 1 to 11 above (except those marked with an \*). | Should |
| CM10.5 | It **SHOULD** be possible filter the message log by any of fields 1 to 11 above and then to order by any field (except those marked with an \*). | Should |
| CM10.6 | It **MUST** be possible to view any selected message (including acknowledgements/responses). This **MUST** include any supported embedded object (e.g. PDF file). Note : Defined in CDA Documents - Attachment Types - NPFIT-FNT-TO-TAR-0095.02. | Must |
| CM10.7 | It **MUST** be possible to print any selected message (including acknowledgements/responses). This **MUST** include any supported embedded object (e.g. PDF file). Note : Defined in CDA Documents - Attachment Types - NPFIT-FNT-TO-TAR-0095.02. | Must |
| CM10.8 | Message timestamps (i.e. the timestamp visible to MHS’s and Transport Channels to determine message persistence, retry behaviour, etc) **MUST** use UTC (Coordinated Universal Time – aka GMT in the UK) | Must |
| **CM11** | It **SHOULD** be possible to produce summary reports for viewing on screen and for printing which show aggregated counts of messages by user selection of:* Date/time
* Trading Partners
* Interaction types

See Management Information section for further reporting requirements. | Should |
| **CM12** | Messages **MUST** be retained within the system in accordance with the NHS Data Retention Policy. Note : Retention Policy defined in Information Governance Requirements for ESP and GPSoC Systems NPFIT-FNT-TO-TIN- 0427.10. | Must |
| **CM13** | It **MUST** be possible to view a list of messages waiting to be sent, to an end point. Note: This will be of use where the end point is not available to receive messages and message may be pending and backed up. This process will also show messages queued up due to throttling by the suppliers system. | Must |
| CM13.1 | The waiting to be sent view **SHOULD** show the same attributes as stated in CM10.  | Should |
| **CM14** | The system **SHOULD** indicate the next connection time for each transport channel. If fixed connections times are not supported and the system ‘connects’ at fixed intervals of time the system SHOULD display the connection frequency and SHOULD display the last connection time. | Should |
| CM14.1 | The system **SHOULD** provide a ‘Send/receive now’ option for each transport channel for all, or selected messages, as soon as possible rather than wait until the next scheduled send time, if the transport mechanism utilises a scheduling approach. | Should |
| **CM15** | The system MUST provide appropriate access controls to ‘message log’ and ‘audit’ data, e.g. restrict view and update access to such data according to a users RBAC profile.  | Must |

## Management Information

There is no existing system across the NHS estate that can monitor electronic clinical information flows and no transport level infrastructure components that can provide a holistic view on CDA messaging. The requirements within this section require the MHS components of systems to collate and submit information about CDA documents sent and received by the system.

| **Req ID** | **Requirement Text** | **Status** |
| --- | --- | --- |
| **CM16** | Sending and Receiving systems **MUST** support all requirements documented in the ‘CDA Interoperability – Management Information’ document. (FileCM Ref NPFIT-FNT-TO-TAR-0092.04) | Must |

## HL7 Payload Construction & Validation

It is Authority policy to require sending systems to validate CDA Documents against the appropriate schemas before sending a document although not all systems will necessarily have had this requirement tested and so schema compliance cannot be assumed to have been undertaken by the sender. Receiver systems should therefore undertake schema validation of all received CDA documents.

| **Req ID** | **Requirement Text** | **Status** |
| --- | --- | --- |
| **CM20** | A sending system MUST provide a means to assure the validity of the HL7 CDA document payload before sending. Detailed requirements about how to validate the payload are contained in ‘Technical Guidance for Implementation of Templated CDA Domains’ (see Baseline Index) Note: This validity maybe technical sign off of the CDA construction process. | Must |
| CM20.1 | If this validation fails the sending system **MUST**:* NOT send the message
* Log the error in the message or application logs as appropriate
* Proactively notify the sender (or an administrator) that the document has not been sent so that arrangements can be made to send the information by other means if necessary.
 | Must |
| **CM21** | A receiving system **SHOULD** validate HL7 CDA documents received against the relevant schemas (see ‘Technical Guidance for Implementation of Templated CDA Domains’). If any errors are detected the system **MUST** respond according to the message interaction pattern (see MIM,DMS as appropriate), e.g. by sending an Application/Business Acknowledgement with appropriate error codes (See Point to Point Error Codes NPFIT-FNT-TO-TAR-0083.02). | Should |
| CM21.1 | If this validation fails the receiving system **MUST**:* NOT pass the CDA document to the local clinical application for user processing
* Log the error in the message or application logs as appropriate
* Proactively notify a user (e.g. system administrator users at the practice) that the received document has failed validation.
 | Must |

## Outbound Message Validation

Sending systems are required to perform validation checks on outbound messages before sending them. This section deals with the validation of the non-HL7 elements of a message containing a CDA document.

| **Req ID** | **Requirement Text** | **Status** |
| --- | --- | --- |
| **CM30** | The system **MUST** validate the HL7 payload wrapper (e.g. ITK Distribution Envelope, HL7 Control Act, etc) against the appropriate schema. | Must |
| **CM31** | The system **MUST** validate all outbound messages containing CDA documents against the appropriate specifications. (e.g. ebXML, SOAP, WSDL) | Must |
| **CM32** | If either of the above validation steps fail the system **MUST**:* NOT send the message
* Notify the user that the Message construction and send failed
* Log the error in the message logs
* Notify the sender (suppliers system administrator) that the document has not been sent
 | Must |

## Inbound Message Validation

The following requirements are in addition to normal MHS validation requirements inherent in the network communication protocols (e.g. HTTP, ebXML, SOAP) undertaken by the MHS.

| **Req ID** | **Requirement Text** | **Status** |
| --- | --- | --- |
| **CM35** | When the ‘Allow inbound messages from unrecognised senders’ setting is ON the system **MUST** attempt to process the received message and pass it on to the associated clinical application. | Must |
| CM35.1 | The system **MUST** flag the document as ‘Received from unrecognised sender’ (i.e. Trading Partner). | Must |
| CM35.2 | The system **SHOULD** perform appropriate CDA schema validation on the received file, either specific interaction based schema validation where one exists or generic CDA validation where not. | Should |
| **CM36** | When the ‘Allow inbound messages from unrecognised senders’ setting is OFF, the system **MUST** return an appropriate negative Application/Business Acknowledgement message to the sender indicating that the system is unable to process the message (e.g. using a error response code indicating “unrecognised sender” – See ‘Point to Point Error Codes’) and make appropriate entries in the receiving system message logs.Note: With regard to CM06 this requirement is to allow the control of switching between allowing unrecognised to recognised senders. | Must |
| **CM37** | If the message received contains an unrecognised HL7 CDA Document message/interaction type the system **MUST** attempt to process the document as normal.  | Must |
| CM37.1 | The system SHOULD perform CDA validation on the received file to ensure it is structurally correct. | Should |
| CM37.1 | The system **MUST** flag any unrecognised received CDA Document interaction as ‘Unrecognised Document type’. | Must |
| CM37.2 | The system **MUST** provide a function to render the contents of an unrecognised CDA Document to an authorised user (see CDA Receiver Requirements for more detailed requirements) | Must |
| **CM38** | The system **MUST** perform ‘duplicate message’ checks on all received messages.  | Must |
| CM38.1 | If the message ID is a duplicate (e.g. a TMS message GUID, an ITK Tracking ID) the system **MUST**:* NOT forward the message to the host clinical application
* Log the error in the message logs
 | Must |

## Handling Attachments – Anti-Virus Controls

It is important that any received attachment is checked by appropriate anti-virus software prior to being passed through to the clinical application for user processing. This is a complex area as supplier systems are not always responsible for Anti-virus and other malware checking and there may be different approaches needed to ensure all received files are checked.

| **Req ID** | **Requirement Text** | **Status** |
| --- | --- | --- |
| **CM40** | Where the supplier/system is responsible for AV/Malware checking, the system **MUST** ensure that appropriate checking of attachment is undertaken by the AV software. | Must |
| **CM41** | If the supplier/system is not responsible for AV/Malware checking, the system **MUST** process attachments in such a way that it is checked by local AV software, e.g. most AV software will operate at operating system level and will check a new file being placed onto disk and therefore it would be appropriate to write the file to disk for checking prior to forwarding on the attachment for user processing; or if the local AV software has an API that allows an attachment to be programmatically passed to it for checking, this should be done, etc. | Must |
| CM41.1 | If a virus is found by the Receiving system’s AV software, the Receiving system **MUST** return an appropriate negative Application/Business Acknowledgement message to the sender indicating that the system is unable to process the message (e.g. using an error response code indicating “Anti-virus check failed” – See ‘Point to Point Error Codes’) and make appropriate entries in the receiving system message logs. | Must |

## Message/Interaction/Service Patterns

All message interactions containing CDA documents specified in the MIM/DMS have an associated interaction or service pattern as illustrated in the ‘Interaction Diagrams’ section of each MIM/DMS domain. In the current releases these are identical. Sending and receiving systems must adhere to the pattern(s) associated with each CDA document type and must use the same transport channel for each ‘conversation’ e.g. a CDA Document received over DTS must have the acknowledgement(ITK ‘Business Acknowledgement’ message) returned over DTS.

For example, the Discharge pattern includes the sending of either a Primary Recipient Discharge Report or a Copy Recipient Discharge Report to a Receiving system which then responds with an Application/Business Acknowledgement. The sender may also send a Nullify Discharge Report which is also responded to with an Application/Business Acknowledgement.

Note: Replacement and Nullification versions of documents are linked to their previous versions via the ‘SetID’ attribute of the ClinicalDocument. CDA Documents may also be linked via the use of ‘EncompassingEncounter’ (see MIM/DMS for further details).

| **Req ID** | **Requirement Text** | **Status** |
| --- | --- | --- |
| **CM45** | All sending and receiving systems **MUST** support the domain interaction patterns as specified in the MIM/DMS, i.e. the appropriate message interaction(s) while acting as a sender/originator or receiver. | Must |
| CM45.1 | A sending system **MUST** support the ‘xxx Originating System’ role as defined in the appropriate MIM/DMS | Must |
| CM45.2 | A receiving system **MUST** support the ‘xxx Receiving System’ role as defined in the appropriate MIM/DMS | Must |
| CM46 | A system to system ‘conversation’ (exchange of interactions within a domain, e.g. send discharge, return acknowledgement/response) **MUST** occur on a single transport channel, i.e. it is not permissible to receive a CDA document over TMS and to return the acknowledgement over DTS. | Must |

##  ‘Transport’ Channel Requirements

All sending and receiving systems must support the message/interactions patterns required over any transports channel, e.g. TMS, DTS or ITK web service messaging; that is to say that the sending and receiving of messages must be independent of the network transport.

Although there are different ‘wrappers’ required for different transport channels, the CDA document payload is unaffected by the transport and the MHS is required to wrap/unwrap the payload using the appropriate wrapper and transmit/receive according to the appropriate network protocols for the channel being used.

Systems should only send one CDA document (plus any attachments) per message/transmission/file and only one Application/Business Acknowledgement (where sent) per message/transmission/file.

All systems must adhere to the individual network transport requirements supported as specified by the providers of each, namely:

* TMS – BT Spine – as specified in the External Interface Specification (and associated documents) (See Baseline Index for latest version)
* DTS – BT Spine – as specified in the DTS specifications (see Baseline Index for documentation URL)
* ITK v2 – NHS CFH - as specified in the ITK specifications (see Baseline Index for documentation URL)

### Message Wrappers

CDA Documents sent via TMS are wrapped differently to those sent using ITK web service messaging or DTS. The DMS documentation provides detailed requirements on the use of the different wrappers involved. The diagrams illustrate the main differences between the various wrappers used.



Figure 3.1 – TMS ebXML Message with wrappers



Figure 3.2 – TMS Web Services Message with wrappers

### TMS Implementation Profile for CDA Documents

When a system is sending or receiving messages over TMS the requirements in this section must be adhered to.

| **Req ID** | **Requirement Text** | **Status** |
| --- | --- | --- |
| **CM50** | When sending or receiving over TMS the system **MUST** adhere to all the applicable requirements contained in the relevant External Interface Specification (EIS) published by BT from time to time, in a timescale as required by the Authority (e.g. usually when the requirement goes ‘live’) (see CDA Interoperability Baseline for latest version) . | Must |
| CM50.1 | The applicable sections of the EIS containing requirements which **MUST** be met are:* Part 2 – MHS
* Part 3 – Message Interaction Map
* Part 5 – SDS
* Part A - Appendix
* Part B – Errors
* Part C – Validation
 | Must |
| CM50.2 | When sending CDA messages to TMS the system **MUST** **NOT** breach any TMS constraints (i.e. maximum message size, maximum number of attachments, appropriate TMS service, and appropriate interaction service name). | Must |
| CM50.3 | If the TMS returns an error, the Sending system **MUST** update the status of the sent message and log the error code and error description in the message log. | Must |

### ITK Implementation Profile for CDA Documents

When a system is sending or receiving messages using ITK web service messaging standards the requirements in this section must be adhered to.

The system needs to make use of certain ITK settings to ensure the minimum level of tracking and error detecting is achieved. For example, the ITK Infrastructure Acknowledgement message must be used to provide transport level acknowledgements and the ITK Business Acknowledgement message must be used instead of the TMS Application Acknowledgement.

Note that the ITK v2 messaging standards also include the option to use DTS. Where a system is ITK messaging compliant and is using DTS as its transport mechanism it must adhere to the DTS requirements contained in the ITK documentation.

| **Req ID** | **Requirement Text** | **Status** |
| --- | --- | --- |
| **CM55** | When sending or receiving using ITK web service messaging standards the system **MUST** adhere to all the applicable requirements contained in the relevant ITK web service messaging requirements published by NHS CFH periodically, in a timescale as required by the Authority (see CDA Interoperability Baseline for latest version). | Must |
| CM55.1 | The system **MUST** support the following ITK standards:* Transmission using secure web services (i.e. TLS over SOAP 1.1)
* The ITK v2 Distribution envelope
* The ITK v2 Addressing schema
* The ITK v2 Router mode and End-Point mode
* The following ITK services
	+ SendCDADocument-v2-0
	+ SendDocument
 | Must |
| **CM56** | A sending system **MUST** only send one CDA Document per ITK transmission (i.e. one CDA document within a single ITK Distribution Envelope). NB. If the interaction agreement allows the inclusion of attachments outside of the CDA document then these MUST be included within the same ITK Distribution Envelope. | Must |
| **CM57** | CDA Documents **MUST** be sent using the ITK v2 web services standard for messaging. | Must |
| **CM58** | Sending systems **MUST** support the use of the ITK v2 Distribution Envelope as details in the ITK v2 specifications when sending a CDA Document. In particular, in order to facilitate safe clinical communication of CDA Documents between participating systems certain attributes need to be used in particular ways, these are detailed below. | Must |
| CM58.1 | The ‘Handling Specification’ attribute **MUST** contain the following key value pairs:* key attribute = ‘urn:nhs:itk:ns:201005:ackrequested’ ’’ and value attribute=‘=‘true’
* Key attribute =‘urn:nhs-itk:ns:201005:interaction’ and value attribute=<Interaction ID of the message>
 | Must |
| CM58.2 | The ‘service’ attribute **MUST** be ‘SendCDAdocument-v2-0’ when sending CDA Documents. | Must |
| CM58.3 | The ‘Sender Address’ **MUST** contain the ITK address (URI). | Must |
| CM58.4 | The ‘Tracking ID’ **MUST** be a UUID and this **SHOULD NOT** be the same as the HL7 ‘ClinicalDocument.ID’ within the CDA Document. | Must |
| **CM59** | When returning an Business Acknowledgement, Receiving systems **MUST** use the ‘Tracking ID’ from the ITK Distribution Envelope as the identifier of the message being acknowledged in the MessageRef ID attribute and MUST set the ‘service’ attribute of the Distribution Envelope to ‘SendBusinessAck-v1-0’. Note: It is not necessary to set ‘ackrequested’ when returning an Business Acknowledgement | Must |
| **CM60** | When a system using DTS as an ITK transport mechanism it **MUST** adhere to the DTS requirements contained in the ITK v2 documentation. | Must |
| **CM61** | The system **MUST** use the latest version of the DTS Client within 6 months of it being published and made available by BT. | Must |
| CM61.1 | The system **MUST** comply with any new DTS implementation requirements (i.e. the way in which the DTS service is used, configuration file settings, etc) associated with a new version of the DTS Client | Must |

### DTS Implementation Profile for CDA Documents

When a system is sending or receiving messages using the Data Transfer Service (DTS) and is not ITK compliant, the requirements in this section must be adhered to. This does require the use of the ITK Distribution Envelope as the ‘wrapper’ for the message to provide consistency in architecture across multiple transports

The system needs to make use of certain settings across the DTS service to ensure the minimum level of tracking and error detecting is achieved. These requirements are detailed in the table below.

Note that the ITK v2 messaging standards also include the option to use DTS. Where a system is ITK compliant and is using DTS as its transport mechanism it must adhere to the DTS requirements contained in the ITK documentation. The requirements in the table below must be followed for non-ITK compliant systems using DTS.

| **Req ID** | **Requirement Text** | **Status** |
| --- | --- | --- |
| **CM65** | When sending or receiving over DTS the system **MUST** adhere to all the applicable (see DTS Implementation Profile below) requirements contained in the relevant DTS requirements (see CDA Interoperability Baseline for latest version) published by the Authority periodically, in a timescale as required by the Authority.  | Must |
| CM65.1 | The DTS Client **MUST** be configured according to the DTS Implementation Profile (see below) | Must |
| **CM66** | The system **MUST** use the latest version of the DTS Client within 6 months of it being published and made available by the Authority. | Must |
| CM66.1 | The system **MUST** comply with any new DTS implementation requirements (i.e. the way in which the DTS service is used, configuration file settings, etc) associated with a new version of the DTS Client | Must |
| **CM67** | A sending system **MUST** only include one CDA Document within a file sent over DTS. NB. DTS does not explicitly support associated or linked documents and thus has no in-built mechanism to handle attachments. The sending of attachments outside of a CDA Document over DTS is not covered by these requirements. | Must |
| **CM68** | Sending systems **MUST** support the use of the following DTS settings in order to facilitate safe clinical communication between participating systems as detailed below | Must |
| CM68.1 | The ‘PollMode’ setting **MUST** be set to ‘Reverse’ – it **MUST** **NOT** be set to ‘Upload’ or ‘Download’ when sending or receiving files containing CDA documents | Must |
| CM68.2 | The ‘SaveSent’ setting **MUST** be set to ‘Y’ unless the system saves copies of files before passing to DTS in which case the setting may be set to ‘N’. | Must |
| CM68.3 | The system **MUST** use the ‘ServerRetry’ setting to force the DTS client to retry sending files to the DTS server unless the system provides alternative retry facilities. | Must |
| CM68.4 | The system **MUST** use the ‘TransferReport’ setting set to ‘Y’ in order to detect successful transfer to the DTS Server. | Must |
| CM68.5 | Files sent over DTS are encrypted and therefore the system **SHOULD** **NOT** use the ‘encrypt’ setting unless there are good business reasons for doing so and arrangements are in place between the sender and receiver to enable decryption to take place. | Should |
| CM68.6 | The system **SHOULD** set the ‘Compress’ setting to ‘Y’ unless there are good business reasons for not doing so (e.g. the content is already compressed or encrypted by agreement between sender and receiver). | Should |
| **CM69** | The system **MUST** detect and process any errors reported by DTS by interrogating ‘Report Control Files’ as and when they are generated. | Must |
| **CM70** | The system **MUST** allow approved users (e.g. system administrators) to view the DTS Client Log file. | Must |
| **CM71** | The system **SHOULD** **NOT** send files containing CDA Documents to eSMTP recipients. | Should |
| **CM72** | The DTS Client **SHOULD** be configured to periodically poll the DTS server to ensure that outgoing files are sent in a timely manner and inbound files are received in a timely manner. The DTS Client **SHOULD** **NOT** be placed into ‘shutdown’ or ‘pause’ modes unless this is for justifiable business reasons, e.g. upgrades, backups. | Should |
| **CM73** | Sending systems **MUST** use the ITK v2 Distribution Envelope when sending a CDA Document over DTS.  | Must |
| CM73.1 | Sending systems **MUST** support the following attributes of the ITK Distribution Envelope:* Handling Specification (**MUST** contain the interaction ID associated with the CDA Document)
* Sender Address (**MUST** contain the senders DTS mailbox ID)
* Tracking ID (**MUST** be a unique ‘message’ identifier and **SHOULD NOT** be the HL7 ‘ClinicalDocument.ID’)

(See previous section on ITK for further details.) | Must |
| **CM74** | Receiving systems **MUST** be able to process a CDA Document received over DTS whether it has an ITK Distribution Envelop or not (i.e. no ‘wrapper’ at all). | Must |
| CM74.1 | Receiving systems **MUST** support the use of the ITK Distribution Envelope when received via DTS. In particular this applies to the handling of the values contained in the following attributes:* Service which contains the ITK service – in this case ‘SendCDADocument-v2-0’
* Handling Specification (contains InteractionID and whether an Infrastructure Acknowledgement is required)
* Sender Address (contains the senders DTS mailbox ID)
* Tracking ID (used as the unique ‘message’ identifier)
 | Must |
| **CM75** | Sending systems **MUST** populate the DTS WorkflowID in the Control File. (see Appendix A) | Must |
| **CM76** | Sending systems **MUST** populate the ‘LocalID’ attribute in the Control File with the ITK Distribution Envelope ‘Tracking ID’. | Must |

## Missing/Delayed Application/Business Acknowledgements

Circumstances may arise where an expected Application/Business Acknowledgement either fails to be returned by the recipient system or is returned later than expected. Sending systems need to detect missing or late Application/Business Acknowledgement and to allow messages to be resent if business needs dictate. Systems therefore need to support a range of configuration settings to support these scenarios.

| **Req. ID** | **Requirement Text** | **Rating** |
| --- | --- | --- |
| **CM80** | Sending system **MUST** provide a configuration setting for recording the maximum waiting time for the return of an Application/Business Acknowledgement message for each outbound message where an Application/Business Acknowledgement is expected to be returned by the recipient.Note: A global default setting MUST be provided for all trading partners with the ability to define a local configuration timeout for an individual trading partner. | Must |
| CM80.1 | When the message is sent over TMS the maximum waiting time **MUST** be equal or greater than the ebXML (maxretries X retryinterval) calculated value.Note: A global default setting MUST be provided for all trading partners with the ability to define a local configuration timeout for an individual trading partner. | Must |
| CM80.2 | When the message is sent using ITK web services or over DTS the maximum waiting period **SHOULD** be user configurable and **MUST NOT** be null. The system MAY provide separate max wait values for each transport channel. | Should/Must |
| **CM81** | The MHS / Application **MUST** monitor sent messages awaiting Application/Business Acknowledgements and **MUST**:* flag any message which has not had the Application Acknowledgement/Business Acknowledgement returned and the maximum waiting time has been exceeded as ‘Ack overdue’ (or equivalent)
* remove the flag if the Application/Business Acknowledgement arrives late and flag as ‘Ack late’ (or equivalent)
* generate a notification to an appropriate practice system administrator
 | Must |
| **CM82** | The system **MUST** provide a facility for an appropriate user to resend a message that is flagged as ‘Ack overdue’ (or equivalent).This facility can either be provided within the MHS and/or within the clinical application. The timer for the 'Ack' MUST be reset and the details that the message has been resent. | Must |
| CM82.1 | When a message is resent the system **MUST** update any required message attributes with new values, e.g. if a message is resent via TMS it will require a new message GUID and a new timestamp. | Must |

## Retry Behaviour

Messages sent via TMS using an asynchronous channel will use the ebXML standard and the local MHS will be required to adhere to the ebXML contract properties determining retry behaviour, e.g. the maximum number of retries to attempt and the interval between each retry. The ITK web service messaging standards do not include any retry behaviour and the DTS service does not include any retry behaviour either.

The previous section on handling missing or late Application/Business Acknowledgement covers manual resends of messages which haven’t had an Application/Business Acknowledgement received within the expected time. This section deals with automated retry behaviour at the MHS level.

| Req. ID | Requirement Text | Rating |
| --- | --- | --- |
| **CM85** | For messages sent using the ebXML standard the system **MUST** behave, with respect to retries, to the ebXML contract properties in use between the sender and the receiver. | Must |
| CM85.1 | When sending such messages over TMS the ebXML contract properties **MUST** be retrieved from SDS. Such values may be cached in accordance with the Authorities current guidance. | Must |
| **CM86** | For messages sent containing CDA Documents sent using other standards (i.e. not ebXML) such as web services, the system **MUST** support retry behaviour when the MHS has been unable to send the message (i.e. no transport channel response has been received) | Must |
| CM86.1 | The system **MUST** support the following configurations settings per outbound message type per transport channel:* Maximum number of retries (integer data type) – the number of further attempts to send a message following initial failure
* Retry interval (integer data type) plus units– the gap in seconds/minutes/hours between each retry

Note 1: For example, this means the system must be capable of recording different values for messages sent over DTS from messages sent using ITK web service messaging.Note 2: TMS messaging also has a persist duration setting that is used by MHSs to determine when to delete the message – this behaviour is not explicitly required for non-TMS messaging but systems may implement this behaviour over other channels if required.’ (See ‘Message Logs and Audit’ section for data retention requirements). | Must |
| CM86.2 | The MHS **MUST** monitor the transmission for transport channel responses and upon reaching the retry interval with no response received **MUST** send the message again, reset the timer and wait for a response again, repeating the process until the maximum number of retries has been reached. | Must |

## Message Output Control

Circumstances may arise where the MHS has a large number of messages to send, e.g. following service downtime, and the transport channels that a backlog of messages are going to sent over may be limited in the number of messages it can handle per time period. In order to prevent overloading the transport channel, systems must have a limiter in place for each outbound transport channel.

| Req. ID | Requirement Text | Rating |
| --- | --- | --- |
| **CM90** | For each supported transport channel the system **MUST** support a setting for maximum messages (Integer data types) per time period (seconds/minutes/hours) setting. Note: This is to protect the end point, sending system and services from overload in batch process and recovery from failure catchup. | Must |
| CM90.1 | When sending messages the system **MUST** not exceed the maximum number of messages per time period applicable to the transport channel being used. | Must |
| CM90.2 | When sending messages, the system **SHOULD** spread them out over the time period. | Should |

1. DTS Workflow IDs

All CDA-based messages sent over DTS are required to have the ‘workflow ID’ attribute of the control file populated.

A full list of Workflow IDs to use when using DTS will be published by the Spine DTS Programme and will be available on the DTS website.

1. Note that error codes are passed between the MHS and the application. However, these are included in the EIS to ease implementation as an appendix only. Logically they are still within the MIM domain. [↑](#footnote-ref-1)
2. Processing of the header on receipt of a message SHOULD involve removal of the header prior to passing to the next layer. [↑](#footnote-ref-2)
3. This must be a one-time only generated UUID used to identify the clinical system – that is the system which at a business level is generating or consuming CDA documents. It is used within Management Information to uniquely identify the instance of the clinical system generating the reports. [↑](#footnote-ref-3)
4. Note that a system may have multiple Trading Partner (TP) identifiers for different types of messaging/domains, e.g. EIDFACT sender/recipient 15 digit IDs for Pathology Messaging, NHAIS registration links ID, CDS 15-digit S/R ID, etc. For most CDA messaging the TP ID is the ASID if sent over TMS the ITK address if using ITK or the DTS Mailbox ID if using DTS – in these cases an additional TP ID is unlikely to be required. [↑](#footnote-ref-4)
5. Systems MAY support ‘Other’ if messages can also be received by other means. [↑](#footnote-ref-5)