NHS Integrated Urgent Care

Technical and Interoperability Standards

Version 0.3

March 2017

when it's less urgent than 999

Version Control

Summary

Document Title	Integrated Urgent Care Technical Standards
Document Status	Draft
Document Version	0.3
Issue Date	16/03/2017
Author	Matt Stibbs

Version

Version	Date	Status
0.1	December 2016	First Draft issued for review
0.2	January 2017	Formatting Updated – John Lucas
0.3	March 2017	Further updates

Approvals

Version	Date	Approver
		Adrian Price

Table of Contents

1. Introduction

These standards were originally issued to support the introduction of NHS 111 – they remain current until specifically superseded by new versions or guidance.

1.1. Purpose

The purpose of this document is to provide an interoperability specification to be used for the exchange of pathways information for transfer of care between the 111 service providers.

1.2. Scope

The scope of this document is to lay down the foundations for specific interoperability and technical interactions between the Integrated Urgent Care organisations and systems.

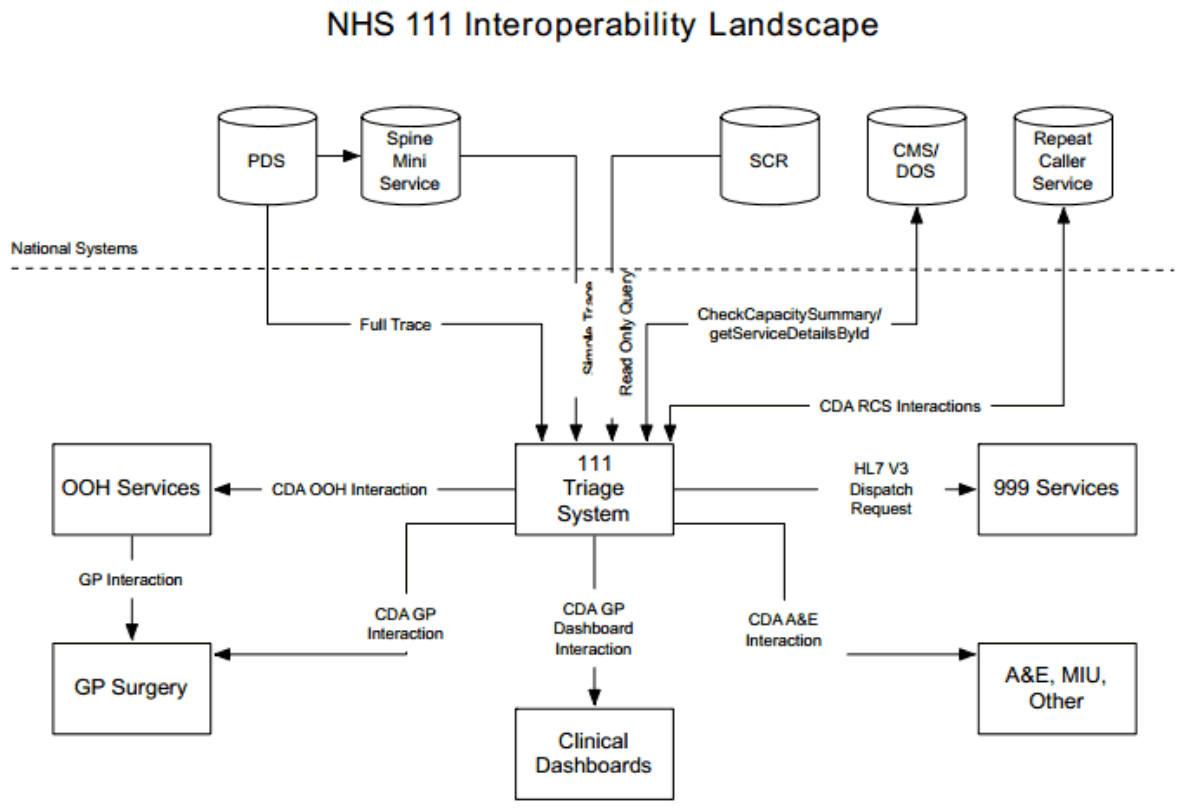
2. Architectural Overview

This section provides a summary view to allow readers a familiarisation with the key aspects which will aid in the understanding of the document contents.

The solution covers the mechanism for the transfer of triage information between the NHS 111 call handling organisations as well as to the various health service providers including ambulance trusts, Out Of Hours (OOH) services and the Repeat Caller Service.

The overall NHS 111 solution allows the call handler to direct for different forms of medical care and to make this available at the most relevant point of care for the patient based on the results of triage. This can be in the form of an ambulance dispatch, referring to OOH / urgent care services or simply providing medical information amongst other outcomes.

This document focuses on the technical elements of information exchange & specifies a standard mechanism to incorporate this implementation. The solution architecture can be seen in the diagram below:



Note: Diagram currently under review and update

3. Functional Messaging Requirements

This section makes extensive reference to ITK Specifications - these can be obtained from the TRUD download service, see: https://isd.digital.nhs.uk

(Further assistance with TRUD may be obtained from the Data Standards and Products Helpdesk at **datastandards@nhs.net)**

The relevant packages on TRUD are:

- **nhs_itkcore** - the ITK core specifications, including web services transport
- **nhs_itkaccreditation** – details of the ITK accreditation process

N**HS 111 Domain Message Specification Version 1.0 RC2:** the 111 messaging payload specifications.

Note: Soon to be superceded by the Integrated Urgent Care Domain Message Specification.

The messaging requirements are shown in the following table:

Ref.	Name	Requirement
MSG.1	Payload specifications	Message payloads **MUST** be conformant with the 111 message definitions These are specified in NHS 111 Version: 1.0; Status: - RC2 Domain Message Specification under NHS MESSAGE SPECIFICATIONS.
MSG.2	ITK Distribution Envelope	Messages **MUST** wrap the 111 message in an ITK Distribution Envelope. Usage of the Distribution Envelope is also specified in **nhs_itkcore**.
MSG.3	ITK Messaging Architecture	All 111 messaging implementations **MUST** be compliant with the ITK Messaging Architecture specification. The document **NPFIT-ELIBR-AREL-DST-0433.01 ITK 2.0 Messaging Architecture v2.0** (see **nhs_itkcore** pack) provides further detail about use of the Distribution Envelope, and other generic aspects of ITK message handling (e.g. versioning, reliable handling). The requirements in this document **MUST** be complied with. (Note that for the purposes of initial 111 go-live then the messaging security requirements (COR-SEC-01 through COR-SEC-05) may be considered to be adequately covered by the approach based on TLS Mutual Authentication that is described in requirement **MSG.6** below).
MSG.4	ITK Web Services Transport	All 111 messaging implementations **MUST** be compliant with the ITK Web Services Transport Specification. The document **NPFIT-ELIBR-AREL-DST-0430.02 ITK 2.0 Web Services Transport Specification v3.0** (see **nhs_itkcore** pack) provides further detail about the ITK web services transport. The requirements in this document **MUST** be complied with, except for the requirements listed below which MAY be omitted for initial 111 go-live:

Ref.	Name	Requirement
		The following requirements may be excepted for initial 111 go-live as they are not relevant as they relate to messaging patterns that are not currently needed by 111: • ****WS-PAT-02****- Toolkit Web Services **MUST** use the Asynchronous Invocation style for Pattern 1 services where this is specified; • **WS-PAT-03** - Toolkit Web Services **MUST** use the Synchronous Invocation Pattern for Pattern 2 services; • **WS-PAT-04** - The SimpleMessageResponse **MUST** contain simple acknowledgement of a Pattern 2 request. The following requirements are security related, and may be excepted for initial 111 go-live, as an alternative, simplified, security approach has been defined for 111 (see MSG.6 below): • **WS-SEC-03** - Toolkit Implementations **MUST** sign the message timestamp; • **WS-SEC-07** - Toolkit Implementations **MUST** be able to authenticate a requestor's identity; • **WS-SEC-08** - Toolkit Implementations **MUST** be able to authorise a service request, based on the Service and the Requestor's identity; • **WS-DSC-15** - The timestamp element of the SOAP Header **MUST** be signed; • **WS-DSC-05** - Canonicalization method **MUST** be present in the signature; • **WS-DSC-06** - PKI certificates **MUST** be used for message signing; • **WS-DSC-17** - PKI certificates **MUST** be from a recognised CA; • **WS-DSC-18** - Toolkit middleware and applications **MUST** preinstall all CA root certificates that are listed in the Microsoft Trusted Root Certificate Store; • **WS-DSC-19** - Toolkit middleware and applications **MUST** preinstall the NHS CA Root Certificate; • **WS-DSC-20** - Toolkit middleware and applications MAY preinstall the Root Certificate from other CAs that they choose to trust; • **WS-DSC-21** - Toolkit middleware and applications **MUST** verify the certificate Thumbprint against an approved list; • **WS-DSC-09** - Detached signatures SHOULD be used if XML Signature is utilised; • **WS-DSC-10** - KeyInfo element **MUST** use SecurityTokenReference;

Ref.	Name	Requirement
		• **WS-DSC-14** - The X509 certificate **MUST** be included in the BinarySecurityToken element.
MSG.5	Full ITK Compliance	All IUC messaging implementations SHOULD gain full "ITK Application" Accreditation, including support for the IUC messaging payload bundle. In practice this will involve, in addition to the above, implementing the remaining requirements in the "**itk_core**" pack – see **"**NPFIT-ELIBR-AREL-DST-0422.02 ITK 2.0 Specifications Overview v2.0****" for details of the additional ITK requirements modules that are relevant to this.
MSG.6	Security based on TLS Mutual Authentication	The IUC service requires "any-to-any" connections between nodes: call handlers and service providers. Connections are made under the direction of information in the Directory of Services (DoS). The size of the handler and provider population, and the requirement to be able to add handlers and providers with a minimum of disruption, argues against reliance on firewalls to restrict connection access. To use firewalls, would require significant reconfiguration across the estate each time a handler or provider is added. An alternative is to open a single firewall port on each 111 node and rely on certificates and mutually-authenticated TLS to secure connections. This works by requiring that all 111 nodes have a certificate which is identifiable, and trustworthy as, belonging to an authorised 111 node. On receipt, a connection will only be accepted if it is secured with a certificate that is trustworthy as being from another 111 node. Sites are configured to use this simply by installing the certificate authority certificates, in their platform. **Port 1880 must be used by all parties for 111 messaging.** Such trustworthiness is assured by the "policy" which guards the issuing of a certificate to an IUC organisation. At the time of initial rollout, there is no such established policy which completely assures the identity of a 111 node – delivery of that policy is dependent on a PKI project with a longer delivery timescale than NHS 111. As an interim, Spine certificates will be used. Spine certificates are signed by a nationally-recognised Certificate Authority, and protected by a policy which identifies sites for connection to Spine. On their own, Spine certificates do not identify a site as a 111 node. However, to create a Spine certificate the Fully Qualified Domain Name (FQDN) and associated IP address of the site must be provided, and the policy enforces this. Therefore, by controlling access to an aspect of the FQDN, the 111 programme ensures that the certificate issued by Spine, identifies the holder as a 111 node. This will be done by placing all 111 nodes under the subdomain "oneoneone.nhs.uk" – control of that subdomain provides the additional 111-specific policy around the issuing of Spine certificates that makes a 111-specific certificate trustworthy as such. On receipt of a connection request, an NHS 111 endpoint will only accept the connection if it is secured by a Spine-issued certificate that has a CN containing an FQDN of the form nodename.oneoneone.nhs.uk. In more detail these checks comprise of: • Full certificate path validation and revocation check by both client and server (client and server stated in the context of the TLS

Ref.	Name	Requirement
		Protocol but in essence, both parties perform verification and validation of the certificates presented by the other party); • Check the validity of the dates within the certificates presented; • Check that the certificate being presented is one which has been issued to a 111 node (i.e. has a CN containing an FQDN of the form nodename.oneoneone.nhs.uk); • Check the issuer of the presented certificate and that should include checking of Authority Key ID and Subject Key ID. *Note: that using the FQDN to provide additional identification for a 111 endpoint is a tactical solution and MAY be subject to changes in future policy regarding DNS or use of the 111 services. For example use of the FQDN check might become redundant at such time as 111 security policy is handled via the processes that protect issuance of certificates against a specific 111 sub CA. To avoid undue impact on deployed systems, vendors **MUST** allow the FQDN checks to be configured such that they can be "turned off" without the need to deploy changed code.*
MSG.7	Direct, synchronous connection	To be able to fulfil the requirements for 111 messaging the following properties of the interaction must exist: • The interface **MUST** be synchronous from the perspective of an HTTPS connection. The request and response are communicated over the same HTTPS connection and the user must be conscious of the message response in real time. The service caller and provider **MUST NOT** communicate via a third-party intermediary.
MSG.8	Endpoint Addressing	Messages to service providers (e.g. Out of Hours, Ambulance) will be addressed to the service provider's endpoint for receiving 111 messages. This service provider endpoint **MUST** be as retrieved from the 111 Directory of Service (DoS). The endpoint of the DoS API **MUST** be a configurable item. Messages to the Repeat Caller Database will be addressed to a single well-known endpoint. The Repeat Caller Database endpoint **MUST** be a configurable item.

4. Non-functional Requirements

The requirements in the following table are expected to be implemented by all suppliers involved in the NHS 111 pilots. This list is likely to grow during the development of the NHS 111 pilot solution:

Ref.	Name	Requirement
NFR.1	Flexible Architecture	The system SHOULD be designed flexibly, so as to accommodate change. The systems and interfaces comprising the NHS Care Record Services will change over time, as new policies and functionality are introduced, and the operational environment evolves. This will require that suppliers are able to modify, activate and deactivate system and user interfaces, and the operational behaviour of the system, or parts thereof.
NFR.2	Support for Multiple Versions of Message Definitions	The system **MUST** be designed in such a way as to support multiple versions of message definitions as receiver and sender of NHS 111 messages to and from other suppliers/organisations.
NFR.3	Availability	The Availability of the system **MUST** be appropriate for the environment in which it is being deployed, taking into consideration its intended usage. The method for calculating the target Availability of the system **MUST** be defined, and the required target Availability **MUST** be documented. The actual Availability of the system **MUST** be monitored. Failure to meet the required target Availability of the system **MUST** be addressed through service improvements.
NFR.4	Open Standards	Suppliers SHOULD adopt Open Standards wherever possible for the development, testing and deployment of accredited systems that will connect to any of the Spine Services. Across the NHS, Open Standards will be applied where applicable, and suppliers are likely to accommodate change most easily if they have adhered to this requirement.
NFR.5	Response Times	The system **MUST** enable users to work efficiently. System design must take account of the user experience and ensure that the introduction of NHS 111 functionality enhances, rather than degrades, the user experience. Systems should make use of appropriate current technology and best practice, and take into consideration the expected response time characteristics of using web services.

5. Directory of Services (DoS)

The Urgent and Emergency Care Directory of Services (also known as the Pathways DoS) is a centrally-hosted and locally-populated directory of services involved in or related to the delivery of NHS Urgent & Emergency Care.

It underpins the workflow within the Urgent & Emergency Care system and fulfils several roles:

1. Provides a core list of clinical services and associated service information (e.g. service demographic criteria and service access information)

2. Holds information about the clinical services provided, and any referral criteria (e.g. specific sexes, age ranges, and clinical conditions)

3. Performs complex search filtering and prioritisation of services to return appropriate service lists to users (e.g. national and local service preferences)

4. Holds endpoint information to route messaging between different services (e.g. NHS 111 call-centre to Out of Hours GP)

Ref.	Name	Requirement
DOS.1	DoS is the official source for UEC service data	The Directory of Services shall be used by any system wishing to direct patients between services within Urgent & Emergency Care.
DOS.2	Caching of results must not lead to stale data	Systems querying the DoS shall always return current service information to users, which requires DoS searches to be real-time via the API or equivalent method guaranteeing the most recent version of the information. Caching may be used to assist with performance of end-user systems – where this is used end-user systems must ensure that this does not result in out-of-date information being provided to users.

6. Permission to View in ITK Messaging

The Summary Care Record and other local shared records are regularly used by Urgent & Emergency Care Services when providing care to patients. In almost all cases the consent to view these records is given by the patient at the time of the encounter (i.e. the clinician looking after the patient will ask the patient for permission to view their medical records).

This is often referred to as **'Permission to View'** or **'PTV'**.

The nature of the Integrated Urgent Care system is such that there are often multiple organisations involved in a single encounter for a patient. Patient experience is compromised if every organisation involved in that encounter needs repeats the same request for consent to view their medical records.

6.1. Sharing Permission to View

To provide a better experience for both patients and clinicians, it should only be necessary to ask the patient for their permission to view their medical records once at the beginning of their encounter.

If the patient needs to interact with other Urgent & Emergency Care services during their encounter, their consent should be automatically communicated between those services alongside the rest of their encounter information.

6.2. How is Permission to View shared?

The Integrated Urgent Care Domain Message Specification (previously NHS 111 Domain Message Specification) specifies a coded-section to be included in ITK messages which allows a referring organisation (e.g. an NHS 111 telephony service) to communicate a patient's Permission To View consent to a receiving organisation (e.g. an out of hours GP service, a clinical assessment service (CAS), an ambulance service).

6.3. Integrating with existing Summary Care Record workflow

It is important that including the Permission to View details in messages does not compromise the existing Summary Care Record workflow in the clinical system – this workflow will have been assured as part of the Summary Care Record Common Assurance Process (CAP).

If you are not sure how to integrate the “Permission to View” ITK functionality into your existing assured Summary Care Record workflow, you should contact the Summary Care Record team.

6.4. Use with other medical record viewers

Use of the Permission To View coding for shared records other than the Summary Care Record must be reviewed and approved by the appropriate responsible officers within those organisations concerned.

7. Messaging Endpoints

7.1. Locating Messaging Endpoint Information

The Directory of Services (DOS) is the official endpoint registry for messaging endpoints for use within Urgent & Emergency Care. It can only hold endpoint records for those clinical services that are configured on the DoS.

The endpoint details support the routing of patients and their encounters through the Integrated Urgent Care system by specifying how and where the clinical systems should transfer patient encounter information to other clinical services.

7.2. Querying Endpoint Details

The DoS API has a SOAP method called 'ServiceDetailsById' - this allows a system to submit a DOS Service ID (10 digits) or Organisational Data Service (ODS) Code and receive back details of any messaging endpoints that are configured for that service.

Endpoint details are structured as a prioritised list of endpoints with various attributes defining how those endpoints can be used.

The following table details each attribute that is stored against an 'endpoint' entry:

Attribute	Description
Priority / Order	The priority / order is used to 'sort' the entire list of endpoints for a single service.
Transport	The transport type for an endpoint defines the transport method used for getting information to that endpoint (e.g. ITK, Email, Phone).
Endpoint Address	The endpoint address is the actual address identifier that the information will be sent to for that service.
Interaction	The interaction value denotes which ITK interaction should be used for the transmission of the information.
Format	The endpoint format defines the format in which the information should be represented (e.g. CDA, HTML, PDF).
Business Scenario	The business scenario defines the situation in which a particular endpoint should be used. Currently this can be **Primary** or **Copy**.
Compressed	The compressed flag is used for ITK messages and defines whether or not the endpoint can accept compressed ITK messages. Where the value is **True**, ITK messages should be sent with compression enabled. Where the value is **False** or not present, ITK messages should be sent uncompressed.
Business Scenario	Description
Primary	This should be used when information is being shared for the purpose of a primary referral of an active encounter.
Copy	This should be used when information is being communicated **for information only** either during or after an active encounter (e.g. Post Event Message to a patient's GP surgery).

7.3. Email Endpoints

Where email is used for Transfer of Care messages (sending CDA messages via email instead of ITK), there is a specific list of email domains which should be supported; attempts to send person identifiable data (PID) to any other domain should be blocked by the sending system.

The official list of acceptable domains for transferring person identifiable data (PID) is available on the HSCIC (NHS Digital) website here: HSCIC - Sending secure email

It is possible that this list may change in the future. It is recommended that system suppliers should make it easy to update the list of valid email domains in customer systems so as to avoid having to deploy new product releases if the list changes in the future.

Systems using email to send urgent care messages should also conform to the "Secure email standard" also detailed on the HSCIC - Sending secure email page.

7.4. ServiceDetailsById Webservice

The ServiceDetailsById function is part of the Pathways DOS API - the definition can be found here: https://www.pathwaysdos.nhs.uk/app/api/webservices?wsdl=1.3

A request to the ServiceDetailsById API requires the following mandatory information:

Item	Description
Service ID	The identifier of the service for which details are required - can be either a DoS Service ID or an ODS code

The response from the ServiceByDetailsId API provides a list of 0 or more 'endpoints' each containing the following information:

7.4.1. Endpoint Ordering

Upon retrieving a complete list of endpoints from the webservice, the consuming system should then order the returned list in ascending order using the Order attribute for each endpoint.

Where there are multiple endpoints which meet certain criteria (e.g. Primary business scenario) the system uses the order to identify which endpoint should be attempted first (Order 1), and which should be used as a backup (Order 2).

7.4.2. Endpoint Value Concatenated String

The endpoint value is a concatenated string of endpoint attributes which are separated by a custom delimiter of \|

The structure of the concatenated string is as follows:

Endpoint Address \| Interaction \| Format \| Business Scenario \| Compressed?

Examples:

http://SampleHostname/SendCDADocument\|urn:nhs-itk:interaction:primaryOutOfHoursRecipientNHS111CDADocument-v2-0\|CDA\|Primary\|Compressed

email.address@nhs.net\|urn:nhs-itk:interaction:primaryEmergencyDepartmentRecipientNHS111CDADocument-v2-0\|PDF\|Primary\|Compressed

email.address@nhs.net\|urn:nhs-itk:interaction:primaryEmergencyDepartmentRecipientNHS111CDADocument-v2-0\|PDF\|Primary\|

8. Spine SSL Certificates

8.1. Renewing Spine SSL Certificates

Spine SSL Certificates (also known as ITK certificates or 111 certificates) provide the security and identification element of existing Integrated Urgent Care interoperability.

They are used to support Mutual Authentication between two communicating systems.

Live services operate using spine certificates issued to system endpoints on the oneoneone.nhs.uk NHS sub-domain.

These certificates are issued centrally by NHS Digital.

New certificates can be obtained by contacting the Deployment Issue Resolution team on dir@nhs.net.

8.2. Certificate expiry

When you are issued with ITK certificates, they are automatically issued with an expiry date. This expiry date is the last point in time at which that certificate will be valid.

Once a certificate expires it can no longer be used to make a secure connection - this would result in interoperability failing.

To ensure that your service is not interrupted by an expiring certificate, you must make sure you **renew your certificate** before the expiry date.

8.3. Renewing certificates

Certificates can be renewed at any point - you do not have to wait until the expiry date is close or passed.

If a certificate is issued with an expiry date that is 2 years away, it is advisable that you aim to renew that certificate 6 months before it expires. This gives you plenty of time to go through the renewal process and deal with any issues that may arise.

8.4. Monitoring certificates

Monitoring certificates is the responsibility of the organisation to which the certificate has been issued - certificate expiries are not monitored centrally and so you will not receive an alert when your certificate is about to expire.

Many system vendors will have their own processes in place for monitoring certificates and will be able to cover this as part of their service provision.

9. Ambulance Requests

Integrated Urgent Care services have the ability to directly request an ambulance for a patient where necessary.

A message specification for Ambulance Requests is defined as part of the Integrated Urent Care Domain Message Specification (previously NHS 111 Domain Message Specification).

Urgent & Emergency Care services, which are using NHS Pathways to support triage, are currently able to request an ambulance electronically through NHS Pathways.

These electronic ambulance requests are defined in the NHS 111 Domain Message Specification which can be downloaded from the NHS Digital TRUD Portal.

9.1. Ambulance requests from Clinical Assessment Services (CAS)

With the introduction of Clinical Hubs, clinicians may need to be able to electronically request an ambulance despatch without using the NHS Pathways product.

9.2. Identifying the correct ambulance service

To identify the appropriate ambulance service to send a request to, the postcode of the patient's current location is mapped to the ambulance service responsible for that area by mapping via the responsible Primary Care Organisation which is currently the Clinical Commissioning Group (CCG).

10. Repeat Caller Service

10.1. What is the Repeat Caller Service?

The Repeat Caller Service is a national service operated by HSCIC (NHS Digital) and is a core part of the Integrated Urgent Care national architecture.

The current functions provided by the Repeat Caller Service (RCS) are as follows:

- Respond to NHS 111 Repeat Caller Queries at the start of every NHS 111 encounter;
- Receive NHS 111 CDA submissions at the end of every NHS 111 encounter.

10.2. How does it work?

NHS 111 services are required to search the Repeat Caller Service (RCS) at the beginning of each urgent care encounter. The search contains a minimal set of patient demographics which are used to identify the caller.

If a caller's identity has been verified against the Personal Demographics Service (PDS), the person's NHS number will be used as the primary search term.

If a caller's identity has not been verified against the PDS, recorded demographic information will be used to try and match the person to existing records. The demographic items supported are:

- Verified NHS Number (only included if person is verified against the PDS)
- First Name and Last Name
- Date of Birth
- Gender
- Postcode

Using the available search criteria, the RCS will respond to the query to answer the question "Has this caller already called twice in the last 96 hours?" as shown in the following table:

If	Then	Status
There are not two previous calls for the caller	The RCS will respond 'No'	Not A Repeat Caller
There are two or more previous calls for the caller and the caller was identified by verified NHS number	The RCS will respond 'YES' and will include the previous call reports in the response	Confirmed Repeat Caller
There are two or more previous calls for the caller and the caller was identified using 4 or more of the 5 additional demographic details	The RCS will respond 'YES' and will include the previous call reports in the response	Confirmed Repeat Caller
There are two or more previous calls for the caller and the caller was identified using 3 of the 5 additional	The RCS will respond 'PARTIAL' without including call reports, and the NHS 111 is prompted to ask the	Potential Repeat Caller

demographic details	caller to confirm verbally	

10.3. Record Retention

Submitted documents are stored for a maximum of 96 hours before they are deleted.

10.4. Implementation Requirements

All IT systems used for receiving initial urgent care encounters must have connectivity to the Repeat Caller Service.

Systems should support both Repeat Caller Queries and CDA submissions of completed encounters.

10.5. Querying the RCS

Any system, that is used to manage people who are making first contact with Integrated Urgent Care, should query the Repeat Caller Service to identify whether that person has previously contacted the Integrated Urgent Care service.

If a caller's identity has been verified against the Personal Demographics Service (PDS), their NHS number should be included in the query and will be used as the primary search term.

If a person's identity has not been verified against the PDS, their NHS number should not be included within the query - the query should only include recorded demographic details.

If a person is identified as having called twice previously within the preceding 96 hours, the service then they should be transferred to a clinician as a minimum level of priority (anything of a higher priority should be followed).

10.6. Submitting to the RCS

All systems should submit a CDA document to the Repeat Caller Service upon completion of an encounter.

10.7. Error Handling

If a submission attempt is unsuccessful, the system must continue trying to submit the document for 96 hours.

Systems should continue to retry the submission unless the queued submission is explicitly removed from the submission queue by a user.

10.8. Configuration Requirements

Systems should provide the ability to disable Repeat Caller Service queries when necessary.

If Repeat Caller Service queries are disabled, the system should always prompt the user to confirm whether the caller has called before to establish whether they are a repeat caller.

The following settings should be configurable in the system without requiring new development / releases:

- Ability to Enable / Disable Repeat Caller Service interactions;
- Endpoint URL for the Repeat Caller Service (endpoints for Submissions and Queries should be separately configured).

10.9. Requirements for submitting documents to the Repeat Caller Service

10.9.1. Retry Logic

If a submission attempt is unsuccessful, the submission should be queued to retry the submission.

Systems should continue to retry the submission until a reasonable number of attempts have failed, or until submission is removed from the queue by a user.

Systems should implement retry logic which increases the amount of time between retries with each subsequent retry.

10.9.2. Monitoring

Systems should notify users to failed submissions, and provide them with appropriate tools to monitor and respond to issues.

11. Post Event Messaging (PEM)

The actions that need to be completed by NHS 111 System Vendors to resolve these issues are as follows:

11.1. PEM should be sent using ITK messaging standards where possible

All areas must have plans in place to implement ITK within the GP systems. ITK is proven to reduce the workload on GP's, as the current practice of using DTS increases workload on NHS 111, GP's, and increases the amount of faxing within NHS 111 service, in particular with Out of Area calls.

11.2. Primary Recipient messages MUST be addressed to ODS code and DoS Service ID

GP Primary Recipient messages must contain the DoS Service ID in the distribution envelope for routing purposes and the ODS code if it is available.

11.3. Copy Recipient messages SHOULD be addressed to both ODS code and DoS Service ID

GP Copy Recipient messages must contain the ODS code in the distribution envelope for routing purposes and the DoS Service ID if it is available.

11.4. Copy Recipient messages SHOULD not be sent when they are duplicates

GP Copy Recipient messages must not be sent when successfully referring to the same service using a primary interaction
(e.g. urn:nhs-itk:interaction:primaryOutofHourRecipientNHS111CDADocument-v2-0).

This should be determined by the DOS Service Type ID of GP Out of Hours. The current suppression of a copy message where it is the same GP as the primary message should continue to operate.

This must be developed as a configuration item within the application to ensure the suppression of PEM to any Service Type ID's can be turned back on should it be required.

11.5. Copy Recipient / Post Event Messages should be suppressed for certain dispositions

At the end of a patient journey within Integrated Urgent Care (IUC), a patient's GP practice should be notified, messages should only be sent when an encounter with the IUC service has concluded and no call backs or further care is going to be provided by the service.

This is to ensure the volume of messages a GP receives is kept to a minimum and the GP isn't receiving duplicate information.

For the purposes of Post Event Messaging (PEM) to a GP the following dispositions are categorized as “Never Send”. This means that upon completion of a NHS Pathways assessment, reaching any of these disposition messages do not need to be transferred to inform the patients GP.

The “Never Send” list can be found in Appendix 1.

11.6. CDA messages must contain the correct headings

Within all CDA documents at the /ClinicalDocument/component/structuredBody/component/section/component/section element **MUST** contain the following items only in the order presented, using the titles (/ClinicalDocument/component/structuredBody/component/section/component/section/title) shown here, and appropriate text (/ClinicalDocument/component/structuredBody/component/section/component/section/text):

1. Patient’s Reported Condition
2. Pathways Disposition (this should include selected service)
3. Consultation Summary
4. Pathways Assessment
5. Advice Given

Note: These headings will be updated in a subsequent message specification version – this document will be updated to reflect that

11.7. CDA messages should be rendered using specific XML transforms (XSLT)

For Primary Recipient messages **NHS111_CDA_Renderer_PrimaryRecipients.x**sl renderer **must** be used.

For Copy Recipient / PEM messages **NHS111_CDA_Renderer_CopyRecipients.xsl** renderer **must** be used.

These XML transform files can be found within the Integrated Urgent Care Domain Message Specification (downloaded via TRUD portal).

Appendix 1 – PEM Never Send List

This table lists the disposition codes for which a Post Event Message should not be sent to the patient's registered surgery.

DX Code	Description
DX 28	Contact Pharmacist
DX 52	Refer to Police
DX 60	Contact Optician next routine appointment within 72 hours
DX 22	To be seen by Dental Practice within 3 working days
DX 23	Contact Orthodontist next working day
DX 45	Provide Service Location Information
DX 46	Refer to Health Information
DX 63	Refer to Fluline

Last updated December 2016