SUS+ Essentials

Secondary Uses Service - User Guide

Information and technology
for better health and care

Contents

Introduction

This document provides a reference point for new and existing Secondary Uses Service (SUS) users. It introduces general concepts, provides an overview of the submission process and provides details on extracting data from SUS. It also highlights best practice and includes information on data quality, logging system issues and where to find out more about SUS guidance.

Users are encouraged to familiarise themselves with all SUS guidance materials for assistance in specific areas, including SUS Payment by Results guidance.

Background

Providers of NHS-funded healthcare in England are required to send Commissioning Data Set (CDS) patient activity data to SUS to support:

- Commissioning
- Healthcare development
- Improving NHS resource efficiency

SUS processes on average 5 million incoming records and 30 million outgoing records every day. It is therefore important for users to apply the recommendations in this guide to help ensure the provision of consistent and reliable data.

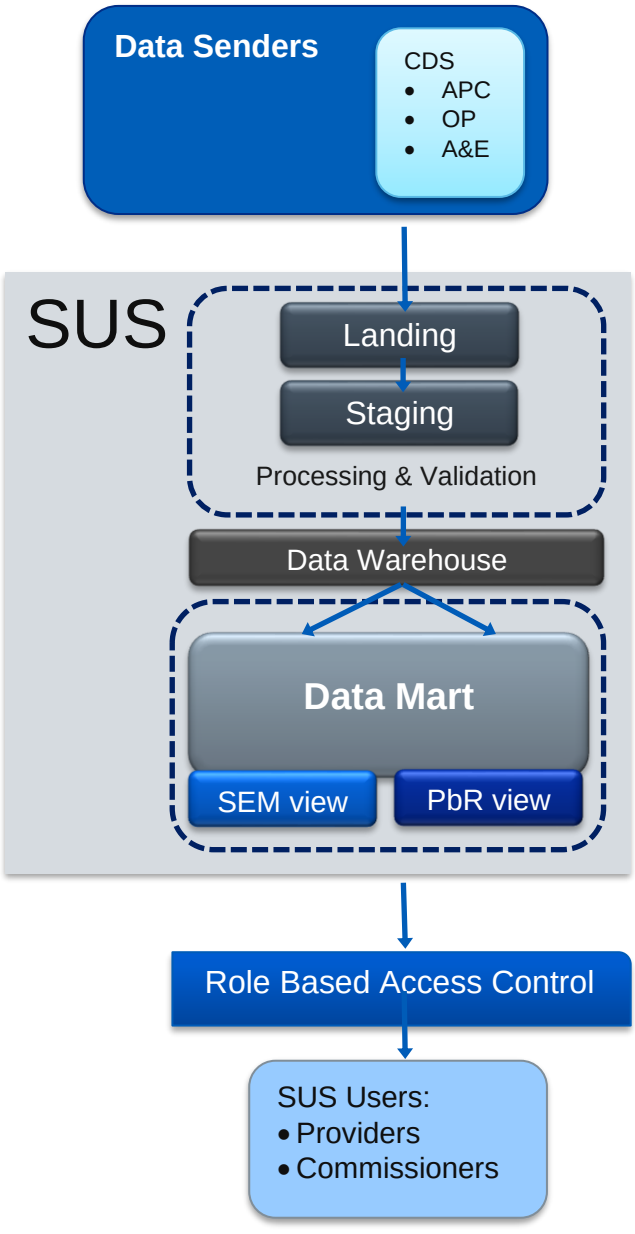
It is critical that high quality information for management and clinical decision making continues to be provided for the NHS to keep improving the quality and safety of its services. High quality data is not an 'option'. It is a fundamental basis for the business of each organisation. It should always be considered at the centre of any future developments for any organisations providing NHS-funded care and should be constantly under review.

The Department of Health mandates the collection and submission of all NHS-commissioned activity (Acute and Mental Health), including services provided for the NHS by the Independent Sector. This represents a wide range of organisations of varying sizes.

Management and Development

SUS is managed and developed by NHS England. It receives, processes and reports information for purposes other than direct clinical care, hence the title "secondary uses".

Activity data in SUS is submitted using patient-based Commissioning Data Sets (CDS).



Overview of the SUS Data Warehouse

SUS was originally introduced in order to provide a single consistent and authoritative system to process data flows and replace the historical NHS wide clearing service (NWCS). It was then identified as an enabler to support the Department of Health Payment by Results (PbR) national tariff policy initiative. SUS continues to be developed to support the ongoing functionality of national tariff policy by NHS England and NHS Improvement.

Since April 2012, the use of SUS has been mandated in the NHS Operating Framework for performance monitoring, contract reconciliation and payment.

The NHS Standard Contract requires that all NHS-funded care activity is reported to SUS using Commissioning Data Sets (CDS).

SUS has been designed to support government objectives and reduce the use of Person Confidential Data (PCD) for purposes other than direct patient care. SUS has significantly improved the security and confidentiality of data management through a combination of:

- Comprehensive access controls
- Anonymisation and pseudonymisation of data to replace information that could be used to identify individuals
- Enabling the linkage of data from different sources relating to the same care pathway

Local Data Collection review

Providers of NHS care should regularly review data collected on local systems and ensure that all CDS data is submitted to SUS.

Security and Confidentiality

SUS is a repository for Person Confidential Data (PCD) and access is strictly controlled. The protection of PCD information is a priority for the NHS and compliance is taken very seriously. To support this SUS utilises a robust Information Governance framework which ensures that data is always protected from unauthorised access.

Providers of NHS-funded care (including independent sector organisations) do not require Section 251 approval (special regulations to set aside the common law duty of confidentiality for defined medical purposes) to access SUS where they are accessing information relating to their own patients. They are able to view all records relating to their patients but are not able to view information relating to patients for whom they have not provided care.

Role Based Access Control

Access to SUS is managed via **Role Based Access Control (RBAC)**.

Under RBAC, new SUS users are issued with a:

- **Smartcard**
- **Passcode**

- **Unique User Identity (UUID)**

NHS Care Records Service Smartcard

These elements allow the management of user access to be monitored effectively, ensuring that data is kept secure and can only be accessed by the appropriate party. SUS can provide access to identifiable patient confidential data (referred to as 'clear' data) or pseudonymised data (referred to as 'pseudo' data) depending on a user's access rights.

Where access to pseudonymised data is appropriate, elements that could identify a patient are replaced with pseudonym values in order to protect privacy and conform to data protection rules.

To gain access to SUS, new users should approach their local Registration Authority (RA). The ***NHS England Registration Authority*** can also provide regional or national support.

N3 Connection

N3 is a secure national broadband network service for the NHS. A secure N3 connection is required to access SUS via Spine.

https://digital.nhs.uk/health-social-care-network

Access for Organisations

SUS data is only directly available to NHS organisations, their information suppliers, or independent sector providers of NHS-funded care.

Smartcard Limits

Smartcards to access SUS are limited to 3 per organisation. Smartcards should never be shared with any other users.

In exceptional circumstances, an organisation that can provide a valid business reason to increase their smartcard limit can raise a 'SUS User Limit Request' via NSD.

Deactivation

SUS automatically removes the user licence of any users who have not

accessed SUS for 3 months. Users must contact NSD to restore access.

Access for Individuals

To access SUS, individuals must have an NHS Care Records Service Smartcard with the correct Business Functions (access rights) assigned by the local RA.

SUS provides data outputs in both identifiable and pseudonymised form, depending on the access rights of the user. A combination of the user organisation and assigned Business Functions determines what type of data can be accessed.

*The **SUS RBAC Assignment Guide** lists the business functions that should be assigned to SUS users based on their role within the organisation. Local RA personnel should review this when granting RBAC rights. More information about Smartcards and RBAC can be found on the* Registration Authority webpage***.***

RBAC determines what a user's role requires them to do, based on the information assigned to their smartcard. SUS then allows access to the relevant functionality and data based on that information.

After completing the registration process, users must register one or more User Role Profiles (URP) and have Business Functions assigned by their local RA. This will grant access to the appropriate applications on the Spine.

Smartcards

Smartcards are issued directly to an individual user by an RA (Registration Authority) using confirmation of their identity. Sharing of smartcards is strictly prohibited.

RA Guidance

For more detailed RA information about configuring user smartcards using RBAC, please refer to the SUS RBAC Assignment Guide on the SUS Guidance webpage.

Pseudonymisation

Pseudonymisation is the de-identification of identifiable patient-centric data item values through the use of substitute values. Pseudonymised data can be linked and used for secondary purposes, such as trend analysis and peer comparison, without using identifiable data items.

Pseudonymisation of patient information enables:

- The legal and secure use of patient data for secondary purposes
- NHS business needs to be met without using identifiable data
- The continued effectiveness of NHS business processes in supporting the day-to-day operation of the NHS

Requirements for SUS Users

SUS is currently only directly available to NHS Organisations (or their information suppliers such as shared information services) and to a limited number of staff in each organisation. In order to access this information, users must have a Smartcard with the correct Business Functions assigned by their local RA (Registration Authority).

Registration

Smartcard

To obtain a Smartcard, users must contact their local Registration Authority (RA), who is responsible for issuing cards. The RA will enter the users' details on the NHS Care Record Service User Directory, known as the Spine User Directory (SUD) and the user will receive a Unique User Identifier (UUID). The record relating to the new user on the SUD will contain details of the organisation the user works for or is acting on behalf of, e.g. for a Shared Informatics Service.

User Role Profile (URP)

Users must contact their local RA and a registration form must be signed off for users to be assigned the required SUS Business Functions (BFs) by the RA. The RA will then update the Spine Directory Service (SDS) with the Business Functions to create the users URP.

The following Business Function codes are the most common used for access to SUS.

B0163	**Access PbR (Clear)**
B0164	**Access PbR (Pseudo)**
B1505	**Access SEM (Clear)**
B1510	**Access SEM (Pseudo)**

After following the above steps users should be able to enter the SUS Portal and access data relating to their organisation.

Sender Registration Form

All organisations required to send data must be registered with SUS using the SR1 Registration Form, available on the SUS Guidance webpage.

A new call should be logged with NSD weblog, with the completed SR1 form attached, and a request raised to process the sender registration.

The registration process ensures that the data sender, and all organisations for which they submit data, are registered with SUS.

The SR1 form includes primary and secondary email contacts that will receive notification of CDS interchange failures. It is recommended that the named contacts are staff members, directly involved in the local submission process, and who are able to take appropriate corrective action where necessary. It is important that data senders keep this information up to date and provision should be made for when named contacts are out of the office when data is submitted.

Users should complete an SR1 form if they:

- Have NOT sent data before
- Wish to send data using a new CDS Interchange Sender Identity (EDIFACT/EDI Address)

  Wish to change the registered organisation code.
- Wish to change contact details for email notification of interchange failure.

Data senders must notify NSD of any changes to nominated contacts.

CDS Interchange Sender Identity

In order to send a CDS Interchange, a CDS Interchange Sender Identity is required.

This comprises a 10 character EDIFACT address and a local 5 character tail specified by the data sender. The code is used to manage physical interchange

senders, particularly to ensure that interchanges are processed in sequence, flow blocking following an error is also managed at this level.

Most senders use the same 5-character suffix for all data, e.g. 00001.

Some senders use a different suffix for different dataset types (APC, OP etc) or for different PAS systems. However, there are risks associated with this practice. Users are advised to make sure they fully understand the update protocols before choosing to use specific suffix identifiers.

XML Supplier

Each provider is encouraged to enlist the help of an XML translation service to translate the provider's data into XML format. It is the responsibility of the XML translator to assist in obtaining and managing the EDIFACT address required by the provider.

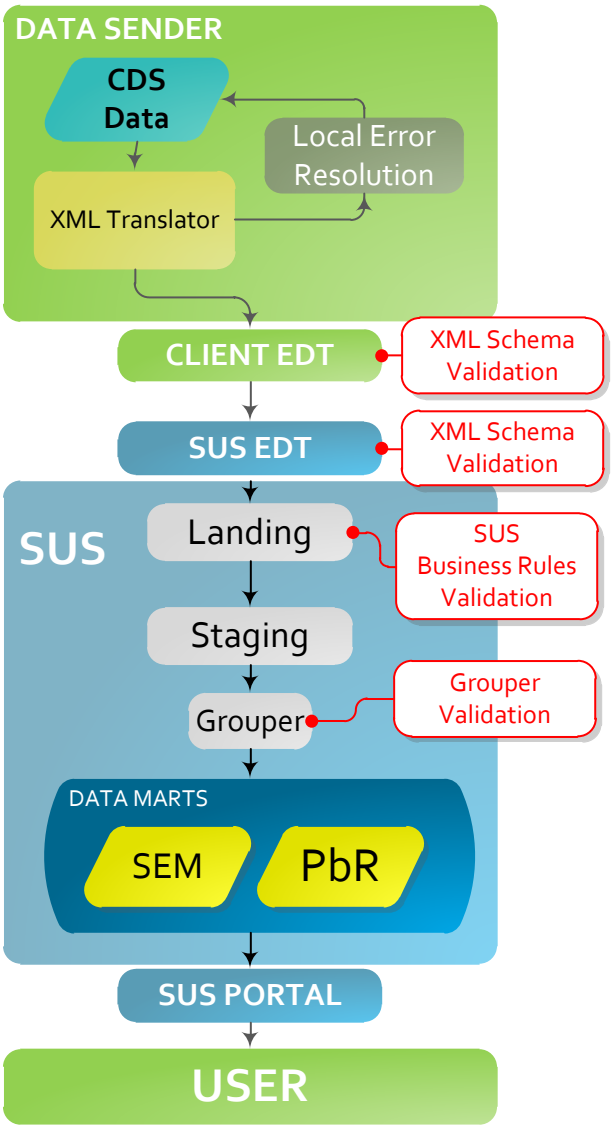
XML Validation

SUS can only accept data submitted as XML (Extensible Markup Language) which is a text-based language for encoding structured information. It allows consistent error checking based on NHS Data Dictionary definitions which are detailed in an XML schema.

Data senders requiring the use of an XML translation service must select a supplier from the list of accredited suppliers before they can submit data to SUS. The terms of this contract are negotiated between the sender organisation and the XML supplier.

Implementation guidance for XML can be found in the Data Sender Deployment chapter.

Interchanges are validated against the XML schema on submission. If an interchange passes validation it is transmitted to SUS where additional validations, referred to as 'SUS business rules', are performed to ensure that the data can be processed.



SUS Validation Flow Chart

Definitions of the CDS types and validation rules can be found on the NHS Data Dictionary and ISB websites as follows:

- The NHS Data Dictionary describes the structure and content of each CDS type. It includes codes that denote whether data is mandatory and the level of XML validation (such as whether format or values are validated) and the SUS business rules that are applied to each data item.
- XML schemas are also available on the NHS Data Dictionary website

- Changes to the definitions are documented via Information Standard Notifications (ISNs), formerly known as Data Set Change Notices (DSCNs), which can be found on the ISB website:
  www.isb.nhs.uk/library/isn
  www.isb.nhs.uk/library/dscn

Providers should implement the above standards and ensure that data within the originating systems, such as PAS (Patient Administration System), are consistent with the data requirements of CDS returns.

Message Exchange for Social Care and Health (MESH)

Message Exchange for Social Care and Health (MESH) is used to transfer batch data securely to SUS. The basic unit of transfer is an **interchange**. An **interchange** is a discrete file of data which may contain one or more individual data messages (APC, OP, etc.). Sender organisations and their XML suppliers are responsible for:

- Installing the MESH client
- Keeping MESH up to date with new versions
- Safeguarding the security of the local MESH host

The MESH mailbox id must be registered as a secure, 'authenticated endpoint' with SUS+ (white listing) via **National Service Desk**.

CDS Versions

The current CDS version is CDS v6.2. CDS versions identify the structure and validation rules within the CDS. Each new CDS version is an enhancement of the previous version and may contain structural changes, additional or removed data items, content revisions and amendments to allowable data item formats and values.

SUS can support up to **two** CDS versions at any one time. Failure to submit data using a supported CDS version will mean that an interchange will be rejected.

Senders should ensure that they have sufficiently tested the new CDS version prior to submitting for the first time. The new CDS version will not be accepted until a successful interchange has been submitted. There may be a short delay between successfully testing the new CDS version and SUS accepting the new version for live data.

Data senders are therefore advised to consider Submission Timetable inclusion dates when moving to a new version of CDS and allow adequate time for testing the submission process before the deadline.

Once approval has been given to submit a new CDS version it is not possible to revert to the previous version.

Submission Patterns

To a large extent, the submission pattern for a data sender will be determined by the operational environment of the organisation. However, there are submission patterns which optimise SUS processing efficiency. Data senders are encouraged to limit the number of interchanges to a maximum of **10 per day**.

Where larger data submissions are required, it is recommended that *larger* interchanges are sent, rather than *more* interchanges. This optimisation reduces the processing burden on the system and benefits the sending organisation and other sender organisations because interchanges can be processed more quickly.

To ensure that there is time to resubmit any rejected interchanges; users are encouraged to submit data in good time before the PbR inclusion date. The latest CDS submission timetable can be found on the SUS PbR Guidance webpage.

Submission Recommendations

- Submissions should be limited to a maximum of 10 per day
- Avoid submitting historic data in the week before an inclusion date. If possible, please only submit data which is pertinent to the current reconciliation and post reconciliation period in the week before each inclusion date
- When sending historic data, the most recent data should be sent first and, if possible, sent a month at a time. This will ensure the most relevant data is processed first and will be visible sooner

Net and Bulk Submission Methods

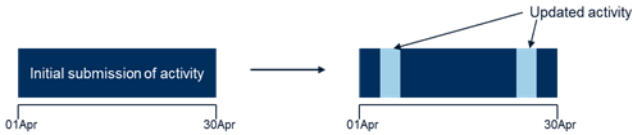
A CDS messages carries information that determines the update mechanism to be used to apply the new data to SUS. The two available submission methods are:

BULK Update

When using the '**BULK Update**' submission method, all records within a specified time period are replaced for that sender, for that period.

NET Change

When using '**NET Change'** submission method, only new records, or records where details have changed, are submitted. This includes deleting records that have been sent incorrectly using a NET Delete CDS.



NET change submission method is more efficient and more reliable. This is because it reduces both the load on the system and the likelihood of creating data quality issues such as accidental duplicates or deletions.

Current Submission Method Use

Currently, **30 percent** of submissions to SUS use **Net** submission method. Amongst the remaining **70 percent**, some systems are capable of producing extracts of new records together with only those records that have changed over a given period. Where a single data source is used for CDS this would directly enable NET submission by those organisations.

It is understood that many of those not in a position to submit using NET update deal with multiple source data sets and have technical problems to resolve to isolate records for inclusion in submissions

More information about **Net** and **Bulk** submission methods can be found in the **Submitting CDS Data to SUS** guidance document on the SUS Guidance webpage.

When producing the CDS message, Bulk submitters must ensure the CDS REPORT PERIOD START DATE is entered correctly. Historically, data senders have inadvertently deleted data over a number of years by populating this data item incorrectly. Where possible, Bulk Update submitters are encouraged to automate the completion of CDS REPORT PERIOD START DATE and End dates as part of the construction of each submission.

CDS Type and Net Change

Net submitters need to be aware of the impact that **CDS type** has on **Net Change** submission method. Most **CDS types** can only be overwritten by the same **CDS type**. However, there are some exceptions to this general rule. The table below shows what CDS type can be overwritten by which other CDS type.

CDS Type	Overwritten by…
010	010
020	020
021	021
030	030
040	040
050	050
060	060
070	070
080	080
090	090
100	100
110	110
120	120,180
130	130,140,190,200
140	130,140,190,200
150	150
160	160
170	170
180	120,180
190	130,140,190,200
200	130,140,190,200

Table showing possible CDS Type overwrites

Please note that interchanges that contain **only unfinished** (CDS 170, 180, 190, 200)

episodes, this **change** will only be visible for **records** when using the **SEM** view. This is because such an interchange does not contain any records eligible for PbR processing.

Example:

A data sender has mistakenly assigned a **CDS Type** of **120** (Finished Birth Episode (APC)) as **CDS Type 130** (Finished General Episode (APC)) and submitted it to SUS. To change the **CDS Type** to **120**, the user cannot change the record and submit the record again (see table). Instead the same **CDS Type 130** record should be sent to SUS with a **Net Update Type** of '**1**'(delete). Once the record is removed from SUS, it can be changed to **CDS Type 120** and resubmitted to SUS as a Net Update Type '9' (new) **CDS Type 120** record.

Using NET submission method can help prevent data duplication of records in SUS.

Mixing Bulk and Net Interchanges

Mixing Bulk and Net interchanges can lead to unintended loss of data. If Net and Bulk submissions are mixed, Bulk will update all records in SUS, for the CDS SENDER IDENTITY, Report Start and End Date combinations, irrespective of Extract Dates, Applicable Dates or original submission method for that Bulk replacement group.

Example 1:

A user sends **10,000** records as **CDS Type 130** (Finished General Episode (APC)). The user then sends 500 records further records for the same period as **CDS Type 140** (Finished Delivery Episode (APC)) using **Bulk** submission method under the same CDS SENDER IDENTITY, **Report Start** and **End Dates.** Because CDS Types **130** and **140** are part of the same Bulk Replacement Group (**BRG 010**) the second submission overwrites all of the first submission; leaving **500** records as opposed to the **10,500** APC records.

It is possible to send a **Bulk** interchange with many records with the same CDS UNIQUE IDENTIFIER for the same sender.

A **Net** submission will replace all records containing a corresponding CDS UNIQUE IDENTIFIER for the sender, providing that the CDS APPLICABLE DATE is *later than* or *equal to* the **Extract Date**. If all records in a **Bulk** interchange have the same CDS UNIQUE IDENTIFIER and a subsequent **Net** change deletion record is submitted with the same CDS UNIQUE IDENTIFIER, all the **Bulk** records will be deleted.

Example 2:

A user sends **10,000** records using the **Bulk** protocol with CDS UNIQUE IDENTIFIER equal to '**99999999**' for all records (because it is not part of a **Bulk Update** submission and not used as a key field). The user then sends one single record under the same CDS SENDER IDENTITY where CDS UNIQUE IDENTIFIER is equal to '**99999999**' using **Net** submission. This single record in the second submission overwrites **all** the records from the first **Bulk** submission, leaving a **single** record, rather than **10,001**.

These examples highlight the two main risks of mixing **Bulk** and **Net**.

SUS validates **Applicable Date** against **Extract Date** when **Net** records update **Bulk** records, but does not check **Applicable Date** when applying a **Bulk** update to a **Net** change.

- A Bulk interchange will delete all Net records irrespective of Applicable Date
- If a Bulk interchange has not used a CDS UNIQUE IDENTIFIER then multiple records can be replaced by a single Net record.

Records sent as **Net** cannot be used to replace **Bulk** records that do not contain a CDS UNIQUE IDENTIFIER. Attempting a **Net** update of existing **Bulk** records in this way would effectively result in duplicate records being submitted.

Data Sender Deployment

This chapter describes the business processes necessary to deploy a new CDS-XML V6.2 data feeds

This process applies to every XML CDS data flow including those where MESH is installed locally or where a 'central bureau' service is employed.

Sending Data to SUS – MESH

A list of approved XML Service suppliers can be found at the end of this document.

Management and clinical systems collect CDS data and export it in a User Defined Format (UDF) such as in a comma separated values file. An XML middleware application translates the UDF data to XML.

The XML files are passed to SUS via MESH, but MESH does not validate the XML. **Another standalone XML check solution or the XML middleware supplier application, should be utilised on the XML before transmission via MESH to SUS**.

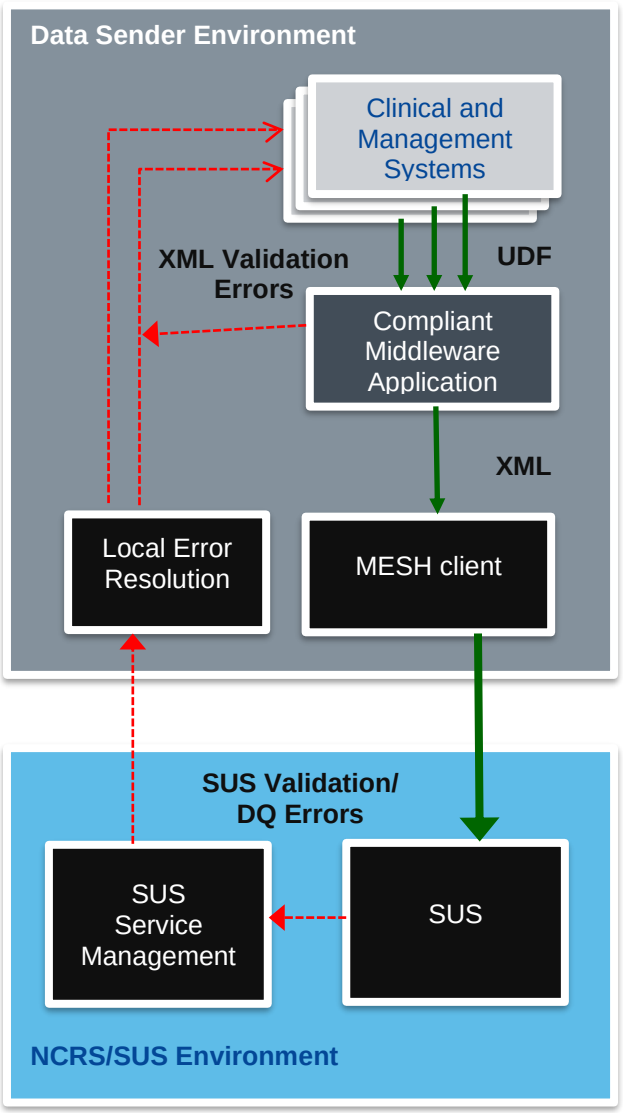
SUS applies additional 'business rules' before loading into the secure data warehouse.

Where submitted data fails XML schema checks on SUS or SUS business rule validation, SUS Service Management notifies the Data Sender and works with them until any problems are resolved. It is the responsibility of the data sender and their XML supplier to provide local error resolution address XML validation and business rule failures.

Workflow ID for SUS+ submission via MESH is SUS_CDS.

CDS interchange receiver id is 260000001200001.
SUS+ receiver MESH mailbox is X26HC023.

General XML submission model:



XML solution options

Locally Installed Service: A provider hosts the XML translation middleware and MESH locally. Management of the XML solution may be local or operated remotely by the software supplier.

Bureau Service: The XML supplier hosts the translation middleware and MESH at their data centre and the provider sends

UDF files to the bureau for validation, translation to XML and submission to SUS.

LSP Model: The management and clinical systems are hosted in the LSP's data centre where the CDS data is created. The data is sent to the trust for review (and possible addition of data from local systems) before being returned to the LSP data centre for MESH transmission to SUS.

Commissioning a CDS Data Source

Each CDS-XML data flow must be made via a supplier who is responsible for the conversion of data to CDS-XML.

Requirements

Before the process can begin the data, sender must have:

- Contracted a supplier to manage the CDS-XML translation and submission via MESH or confirmed they will undertake the role of supplier
- Registered their 15-character EDI address as a data sender. Providers only need to register if they are not currently registered, or their registration information has changed (e.g. contact details). Please use this opportunity to review the registration.
- Appropriate SUS Access Business Functions assigned to a smartcard

Commencing LIVE XML submissions

SUS Registration

CDS Data senders are registered by EDI address. To register a CDS-XML data flow, or to update registration details, please complete the SR1 “Secondary Uses Service, CDS Data Sender Registration Form” available on the SUS Guidance webpage.

A CDS Interchange Sender Identity (10 character EDI address) can be obtained from the NHS Address Registration Service

The SUS ‘CDS interchange sender identity’ EDI Address

Although CDS-XML is not an EDI flow, SUS continues to use the existing EDI addresses to manage interchange receipt. The CDS Interchange Sender Identity is used to identify the organisation that submits an interchange. It is a 10-character EDI id with a 5 character ‘local tail’ making a total of 15 characters. Typically, it might look like 190000099900001 where 1900000999 is the EDI identifier and 00001 is the ‘local tail’. A single MESH client may send interchanges from multiple EDI addresses and different MESH clients may send data from the same EDI address.

Addressing

The first 10 characters are mapped to a registered ODS code. On receipt of an interchange the 10 characters are used to look up the ODS code, If no registered ODS code is found the interchange is rejected. Where the interchange is accepted, if the interchange fails validation, notification messages are sent to the individuals registered against the mapped ODS code. This SUS ODS table is maintained at three characters for Trusts – R*nn*, Care Trusts – T*nn* and 5 characters for non-NHS senders – N*Annn*). With XML, although mapping is made at the 10-character level, all 15-character EDI addresses must be registered. If the 15-character codes are not registered, the interchange will be rejected.

Sequencing

CDS Interchange Sender Identity (EDI Address) is used to sequence data at the 15-character level. SUS processes interchanges in the order received from the MESH client.

Blocking

Following validation errors, SUS blocks processing of interchanges for the affected 15-character CDS Interchange Sender Identity (EDI Address). Processing will not resume until the helpdesk is informed by the registered contact that they understand the failure and will take appropriate action. The blocked queue is irrespective of CDS Type.

Shared EDI addresses

Request conflicts in EDI address migration have highlighted issues around organisations using a single EDI address to send data from multiple sites. For example:

- **a clinic is hosted at a partner hospital site**
- **a hospital system sends data on behalf of a number of local providers**

The configuration and use of interchange flows via MESH and EDI addresses is a local matter. However, it is recommended that logically distinct flows employ separate EDI addresses.

The potential impacts of sharing a 15-character CDS Interchange Sender Identity across multiple CDS flows include:

- **Delayed processing:** Only one interchange within a sequence from the same ID can be processed at a time.

- **Blocked processing:** This follows a validation failure for the Sender ID. (A major hospital flow could be

interrupted by errors in another provider's submission via the same Sender ID).

- **Difficulty managing multiple contacts:** Multiple contacts may exist for a single sender and it may become complex to ensure that all users are aware of failures and submission issues.

Please ensure the migration of shared EDI address is coordinated between all senders.

Data Standards

SUS adheres to the rules set out by NHS Data Standards and documented in the NHS Data Dictionary.
www.datadictionary.nhs.uk

The Data Standards helpdesk email address is datastandards@nhs.net

Alternatively, contact Data Standards via: enquiries@nhsdigital.nhs.uk

Data Validation

There are two levels of validation applied to interchanges they are:

- XML schema validation is applied at SUS+ landing. Before sending an interchange, users are advised to validate the interchange against the appropriate XML schema locally.

- SUS business validation applied at the SUS server. Following receipt of the interchange, a number of 'business' validations are applied. If the interchange fails any of the validations it is rejected, and a notification is sent to the registered user(s). A single error will cause failure of the entire interchange.

Details of the validation applied at CDS attribute level and the Mandatory/Optional status of each attribute can be found in the NHS Data Dictionary in the Commissioning Data Sets section.

www.datadictionary.nhs.uk

Interchange Updates

SUS uses two update submission methods; 'bulk update' and 'net change'. Both of these support updates based on a composite key which uniquely identifies a record.

Bulk update does not require records to be assigned a unique key, updates are made in date delimited blocks.

Net change does require each record to be maintained with a unique identifier, the updates are based on the unique id. The updates keys are detailed below.

Bulk Update Key (Composition)

Sender Code (Organisation)
<OrganisationCode_CDSSenderIdentity>

Bulk Replacement CDS Group<CDSBulkReplacementGroup>

Report Period Start Date
<CDSReportPeriodStartDate>

Report Period End Date
<CDSReportPeriodEndDate>

Net Change Key (Composition)

Sender Code (Organisation)
<OrganisationCode_CDSSenderIdentity>

Record Identifier
<CDSUniqueIdentifier>

Please note that any changes to keys when attempting to update a record will cause a new record to be created, and duplication within the SUS database.

Submitting Test interchanges

CDS data senders can send Test interchanges to SUS+ by submitting a “1” in the CDS INTERCHANGE TEST INDICATOR. Test interchanges are processed by SUS+ and can be seen in the SUS+ Portal Interchange Tracker. Test interchanges will always have a zero-record count on Tracker due to no records being committed to the SUS+ live database.

Organisational Considerations

Organisations Intending to Submit Data from Multiple Sites

CDS authentication prevents data senders from overwriting other organisations data. Only organisations authorised to send another provider's data can submit that data to SUS.

To comply with CDS authentication, each CDS SENDER IDENTITY (*5-character* ODS code) must be associated with only one CDS INTERCHANGE SENDER IDENTITY. The CDS INTERCHANGE SENDER IDENTITY is a *10-character* EDIFACT ID (EDI address) with a *5-character* 'local tail' making a total of 15 characters. A new organisation can obtain a unique *10-character* EDIFACT ID from the NHS Address Registration Service.

Where different sites within an organisation wish to submit data to SUS, the CDS SENDER IDENTITY must be the full *5-character* site code to ensure each site has a different code. A separate EDI address must be set up against each CDS SENDER IDENTITY for each site by completing a CDS Sender Registration Form SR1 Form and sending this to NSD.

Alternatively, where an organisation with multiple sites chooses to send data from one site, each CDS SENDER IDENTITY may be registered with the same EDI address.

A provider cannot submit data from different EDI addresses using the same CDS SENDER IDENTITY and must not send separate submissions for each site using only its *3-character* organisation code. To send data from different sites in separate submissions senders must use *5-character* site codes as CDS Sender Identities and have been issued different EDI addresses for each site by the National Service Desk.

Example *3-character* organisation code:

- RRX

Example *5-character* organisation code:

- RRX01

Provider Sub-commissioning Activity

Where an NHS Trust commissions activity from an independent provider, it is the responsibility of the NHS Trust to ensure that the associated CDS data is sent.

Where an NHS Trust commissions activity from an overseas provider it is the responsibility of the NHS Trust to ensure that the associated CDS data is sent, *except* where a lead commissioner is involved, in which case the lead commissioner is the responsible party.

Organisational Merger, Separation and System Change

Organisations about to undergo a merger, separation from an organisation (de-merger) or system change should review the 'Merging Organisations' chapter of Submitting CDS Data to SUS (available on the SUS Guidance webpage) and inform NSD using the SUS Sender Registration Form (SR1). The guidance contains information on how PAS records for patients in hospital at the time of a merger should be handled and the use of EDI address with CDS SENDER IDENTITY.

Organisations Submitting on behalf of another Provider

Some providers sub-contract healthcare and delegate the associated CDS submission(s) to another care provider. Arrangements to exchange this data must be made locally. There is no provision for

exchange of data or reallocation of activity between providers in SUS.

Senders wishing to submit data on behalf of a different provider must complete an SR1 (Sender Registration) form and return it to the National Service Desk.

Only <u>one</u> provider should send data relating to this activity to SUS, as agreed between these organisations.

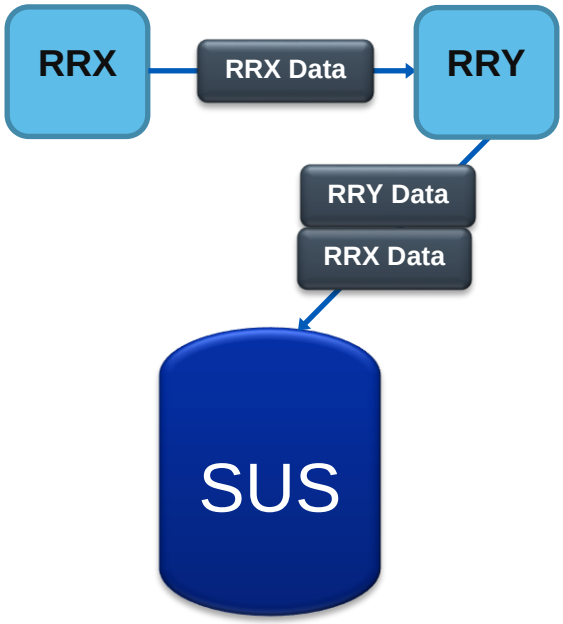


Diagram showing provider organisation (RRY) submitting on behalf of another provider (RRX)

If a second provider wishes to add more records to those already submitted for the first, they can submit them with their own data and identify these records by using the provider site code of the first provider.

If a completely separate submission is preferred for this data, they must use a different value of the CDS SENDER IDENTITY in the header to that used by either themselves or the first provider. This may involve changing the last 2 digits of the 5- character code (site element). This second value of CDS SENDER IDENTITY must be registered and must be different to any already in use or submissions will not be accepted.

Provider Code and Site Code

ORGANISATION CODE (CODE OF PROVIDER) (Provider Code) and SITE CODE (OF TREATMENT) (Site Code) are not used as key fields for either the BULK or NET submission methods. However, keeping the provider code consistent within data from all sites will allow spells from episodes across the sites to be correctly constructed. Data from different parts of a spell at the same provider should have the same provider code but may have different site codes if the patient is cared for at different locations within that spell.

Data Integrity

Submitting Data in line with the NHS Data Dictionary

Responsibility for Data Integrity
Data senders are directly responsible for the integrity of the CDS data they submit. This means that data senders must not flow legally restricted or identifiable information using data items that are not designed for this purpose. Data senders must adhere to the specific guidance for each CDS data item in the NHS Data Dictionary. Failure to follow the guidance for each data item may constitute a breach of the Data Protection Act. Further security and confidentiality information is available on the following webpages of the Submission Protocol and Security Issues and Patient Confidentiality webpages of the NHS Data Dictionary.

APC CDS Type
Information on populating APC CDS Type can be found via the link below. Other CDS Types can be found in the left-hand menu.

CDS V6-2 Type 130 - Admitted Patient Care - Finished General Episode Commissioning Data Set

Populating Prime Recipient
The Prime Recipient CDS data item should be populated in accordance with the Addressing Grid. The code of a NHS England Region (formerly Local Area Team) should not be used in this data item, even where the NHS England Region is responsible for commissioning the activity. This is because it is not possible to derive postcode which is required for Prime Recipient.

NHS England Region codes should be submitted in the Copy Recipient or Organisation Code (Code of Commissioner) CDS data items.

Users are advised to contact NHS England for further guidance on policy.

The Importance of Valid DOB
A date prior to 01/01/1880 or later than the CDS activity date constitutes an invalid Date of Birth.

If an invalid Date of Birth is submitted the associated record will delay PbR processing for the submitting organisation.

Provider organisations are advised to carefully review and validate the population of the DoB data item prior to submission.

SUS and the NHS Operating Framework
Submitting data to SUS is a mandatory requirement outlined in the NHS Standard Contract 2015/16.

28.13 *The Provider must submit commissioning data sets to SUS in accordance with SUS Guidance, where applicable. Where SUS is applicable, if:*

28.13.1 *there is a failure of SUS; or*

28.13.2 *there is an interruption in the availability of SUS to the Provider or to any Commissioner,*

the Provider must comply with Guidance issued by NHS England in relation to the submission of the national datasets collected in accordance with this SC28 pending resumption of service and must submit those national datasets to SUS as soon as reasonably practicable after resumption of service.

Interpretation and application
In order to translate this requirement into local practice, the following principles and best practice should be applied:

1. Providers and commissioners should use SUS as the definitive source of data for patient activity and where a national tariff is applicable, for the price calculation as well.

It is recognised that there are some areas where further information is needed in addition to SUS data to implement tariff policy. The areas are:

- some Best Practice Tariffs
- marginal rate for emergency admissions
- Non-payment for emergency readmission

2. In order to confirm that all activity has been captured and locally agreed tariffs

have been applied, providers and commissioners will need to reconcile local data and billing systems to SUS, to a jointly acceptable level of tolerance.

Providers and commissioners should document in their service agreements the method by which they will reconcile local billing systems with SUS data. Commissioning data sets (CDS) for patient activity not covered by PbR should still be submitted to SUS.

Providers should flag activity that is subject to locally agreed tariffs in order to support reconciliation. This can be achieved by using the service agreement data items in the relevant CDS. Further guidance is available in the Locally Priced Activity chapter of the SUS PbR Reference Manual.

3. As a means to improve the quality of data submitted to SUS, commissioners should apply measures and conditions to the timeliness and accuracy of provider submissions as reflected in the service agreement.

4. In order to effectively reconcile local systems with SUS, providers and commissioners should apply NHS England guidance in conjunction with local NHS communities.

a. Use consistent snapshots of data from local systems and SUS. For SUS snapshots, it is strongly recommended that extracts should be taken using the PbR Reconciliation and Post- Reconciliation views.

b. Use SUS PbR as the basis for reconciliation. The Standard Extract Mart (SEM) view is much more difficult to use for this purpose. SUS PbR processing is applied in a consistent manner according to published DH policy and also effectively handles all activity that is subject to policy exclusion.

c. Ensure all episodes in a spell are updated (coded) and then extracted.

d. Ensure that local payment systems apply rules that are consistent with those applied by SUS.

Further guidance is available in the Reconciling SUS PbR with Local Systems chapter of the SUS PbR Reference Manual.

Patient Objections

Where a patient requests their identifiable PCD data items not to flow, (known as ‘patient objections’ or ‘removal of consent’) providers are required to remove all Person Confidential Data from the CDS file for the data items identified in the Legally Restricted Records section of Submitting CDS Data to SUS, thus making these patient records anonymous. No substitute or pseudonym values should be submitted in their place.

The objecting patient’s identity should be appropriately verified in line with an organisation’s Information Governance guidance and the Data Protection Act 1998. It may be appropriate for this aspect to be managed through an organisation’s Information Governance department.

Data Quality Issues

Incorrect construction of CDS Unique Identifier

The CDS UNIQUE IDENTIFIER data item must not include any patient identifiable data, even where included as part of a concatenated set of codes or 'compound' code. This represents a potential information governance risk, as this is not anonymised for sensitive records.

Recommended practice: The standard for construction of this data item should be followed. In particular it should be noted that the purpose of this data item is to identify a RECORD for use by the Net Update protocol when updating SUS with a new version of that record. Please refer to the NHS Data Dictionary for more information.

Unpopulated, inaccurate or invalid NHS Number

NHS NUMBER is essential in making it possible to share patient information safely, effectively and accurately across NHS organisations. Where NHS Number is not populated correctly there is a major impact on tracing patients, linking data and deriving additional data items from PDS.

Recommended practice: NHS Number must be submitted except for sensitive records, patient objections or those covered under Section 10 of the Data Protection Act. Please refer to the Data Quality Dashboards for information on counts of errors.

If data is withheld, data senders must populate data item WITHHELD IDENTITY REASON.

Unpopulated or invalid Provider Codes

The Provider Code (**ORGANISATION CODE (CODE OF PROVIDER)**) is a mandatory data item. Interchanges are rejected where it contains an invalid code.

Retired or unregistered codes, or codes submitted using non-UPPERCASE (e.g. AbC), or non-alphabetic characters (e.g. A/C) are identified as invalid. Failure to correctly populate Provider Code will mean that the activity is not accepted for PbR processing, which may lead to payment not being received. Such records will not appear in the Provider's extracts from SUS.

Recommended practice: Provider Code should always be populated with a valid, current organisation code, in the correct format.

Unpopulated or invalid Commissioner Codes

Commissioner Code (ORGANISATION CODE (CODE OF COMMISSIONER) is a mandatory data item and an interchange will be rejected if it is omitted.

The majority of invalid Commissioner Codes are out of date or invalid organisation codes. An unpopulated Commissioner Code could result in the Provider receiving no payment. Such records will not appear in the Commissioner's extracts from SUS.

Recommended practice: Commissioner Code should always be populated with a valid, current organisation code. Please refer to the SUS Data Quality Dashboards for information on counts of errors.

Invalid CDS Activity Date

CDS ACTIVITY DATE should be populated with the 'originating date' for the activity within the CDS, as described in the NHS Data Dictionary (e.g. Episode End Date in APC, Appointment Date in OP etc.). Where this is not the case, it is possible that an incorrect **Age at Activity Date** may have been assigned. This means that derivations from PDS may not be using the correct time period.

Recommended practice: CDS ACTIVITY DATE should always be populated with the originating date as described in the NHS Data Dictionary.

Unpopulated or potentially inaccurate A&E times

Where time data items in the A&E CDS are not submitted or the submitted data is not correct to the minute, the usability of the data becomes limited for measuring waiting times in A&E and also potentially

compromises use when monitoring breaches of the four-hour wait target.

Recommended practice: Times should always be submitted, as accurately as possible. Please refer to the SUS Data Quality Dashboards for information on counts of errors.

Unpopulated, Invalid or Inaccurate Site Code of Treatment codes

Where SITE CODE (OF TREATMENT) codes are unpopulated, invalid or inaccurate it is not possible to determine the hospital site where treatment took place. This could potentially impact on monitoring of patient safety and limits the use of the information for patient choice.

Recommended practice: SITE CODE (OF TREATMENT) should always be populated with a valid organisation site code. The code should not end in '00' as this gives no information on site, and all records for a Provider should not be submitted under the same site code. Please refer to the SUS Data Quality Dashboards for information on counts of errors.

Should additional site codes be required, these should first be registered with the Organisation Data Service (ODS).

Population of Morphology codes

Morphology codes are 8 characters long and exceed the 3-6-character length validation for **Diagnosis** data items in the CDS schema. Therefore, **Morphology codes** fail validation.

In some cases, users have tried to shorten (truncate) the code so that it will be accepted. However, doing so can invalidate the code and result in an undefined HRG (UZ01Z) being derived.

Recommended practice: Morphology codes are for local use only and should not be submitted to SUS.

Invalid clinical codes in A&E CDS

A&E clinical codes (Diagnosis, Investigation and Treatment) are six-character codes concatenating a number of codes, constructed in specified positions of the code. Inconsistency in the submission of each part of the codes can lead to them being misinterpreted.

Recommended practice: Standards should be followed for the submission of these codes. See NHS Data Dictionary.

Unpopulated or invalid Diagnosis Codes

Unpopulated, invalid Diagnosis Codes, use of the 'R69X' (not specified) or retired codes, will mean that records are not able to be ‘grouped’ in SUS PbR. Secondary use of the data is also compromised.

Recommended practice: Valid diagnosis codes should be submitted for all records.

Inconsistency between Procedure Codes and Operation Status

In cases where OPERATION STATUS CODE indicates that a procedure took place, but no Procedure Code has been submitted, it is impossible to determine what happened to the patient. This limits the use of the data and could have financial implications in PbR.

Recommended practice: Both Operation Status and Procedure Code data items should be populated with a valid, consistent code. If no operation took place, Operation Status should be populated with code ‘8’ – No Operation Took Place. Please refer to the SUS Data Quality Dashboards for information on counts of errors.

Sending ICD-10 codes in place of A&E diagnosis codes

In some cases ICD-10 codes are incorrectly sent in place of A&E diagnosis codes in the A&E CDS with DIAGNOSIS SCHEME IN USE populated with ‘01’ (Accident & Emergency Diagnosis).

This is not the correct way to flow the data and can impact on A&E diagnosis analysis across areas that include organisations submitting the data incorrectly.

Recommended practice: Organisations should only submit Diagnosis Scheme in Use ‘01’ (Accident & Emergency Diagnosis) with A&E diagnosis codes. A&E diagnosis codes are required for grouping purposes.

ICD-10 and READ codes are optional for additional use in A&E CDS.

Duplicate records due to change in Sender Code

Resubmitted records containing a new CDS INTERCHANGE SENDER IDENTITY code do not overwrite the corresponding, previously submitted records because the key data items do not match.

Recommended practice: Users are encouraged to use the 'Data Quality Dashboard' and 'Monthly Database Counts' to monitor duplicates.

Loss of data submitted in a previous interchange

It is possible for data submitted in a previous interchange to be lost. This can be due to the following possible reasons:

1) Data senders using BULK update submitting General CDS types (120,130,140) separately. These should all be sent under a single Bulk Replacement Group. Failing to do so will result in records of the latest CDS type overwriting all records in the previous CDS types for the same reporting period.

2) Data senders mixing BULK and NET interchanges. Without an advanced understanding of the two update protocols, mixing BULK and NET can lead to these submissions overwriting each other. It is therefore not recommended to mix BULK and NET.

3) Data senders using incorrect BULK Start and End dates in submissions.

More information about Net and Bulk submission methods can be found in the Submitting CDS Data to SUS guidance document on the SUS Guidance webpage.

Data senders are also advised to check the Monthly Reconciliation report on the Operational Support webpage to monitor counts.

Maternity data submitted as General Episodes

Maternity Data (CDS types 120 or 140) is often submitted as General Episodes (CDS type 130). Where this occurs, these records will be 'cleaned' in HES to become Maternity records, by looking at the Procedure code or DOB/Episode Start Date/ Admission Method/ Episode Order, which will relate to maternity. However, this will leave blank maternity data items that are mandatory in SUS because they are not available in General Episodes (CDS type 130).

Recommended practice: Delivery and Birth episodes should be submitted as the correct CDS type. Please refer to the Maternity Data Quality Dashboard for numbers of General records that HES will 'clean' to Maternity. The Commissioning Data Set Mandated Data Flows webpage of the NHS Data Dictionary lists the mandatory CDS flows.

Maternity 'tails'

Maternity 'tails' are blocks of repeating delivery (birth) information caused by flat-files output by local systems generating extra local groups.

Up to 9 delivery events can be generated this way; forming a Maternity 'tail' that contains extraneous activity information. When these records are created, values for the first and only baby can be populated through the extraneous 'tails' in the CDS submission. This can create data that appears to represent multiple identical babies for a single delivery.

Recommended practice: Data senders are advised to put the necessary processes in place to ensure that these extra XML data items are not being populated. This would include ensuring that the number of submitted XML groups is equal to the number of babies in the delivery episode.

Future Outpatient (CDS 021) appointments in Outpatient CDS 020

The Outpatient CDS (020) is a retrospective data set and contains information on activity that has happened. The Future Outpatient CDS (021) is a prospective data set

containing planned activity. Where Future Outpatient appointments are submitted as part of the Outpatient (where ATTENDED OR DID NOT ATTEND = 0 - Not applicable - APPOINTMENT occurs in the future) it results in poor data quality in a number of data items relevant to future appointments.

Recommended practice: Future appointments should always be submitted as CDS 021 Future Outpatient and not CDS 020.

Undefined HRG codes being derived (UZ01Z)

When a valid HRG has not been successfully derived in SUS, no tariff can be applied. This failure may be due to key data items, such as Diagnosis or Procedure, either not being populated where required or being populated with an invalid code.

Recommended practice: Refer to the SUS Data Quality Dashboard to determine if the number of 'UZ01Z' (Undefined HRG) codes is higher than expected and the Error Extracts, available via the SUS Portal for detailed reasons for these errors.

Accessing Data

Data is accessed by extracting it from the secure portal, using an NHS Smartcard.

Access is controlled using Spine and Role Based Access Control (RBAC). Users can access data appropriate to the role and organisation on their Smartcard. The portal enables users to download data extracts to local systems to support local summary analysis and reporting.

The legacy SUS system used a dual-DataMart system, with SEM (Standard Extract Mart) and a PbR Mart containing:

- SEM – Completed **Episodes** without PbR derivations.
- PbR – Completed **Spells** with PbR derivations

Historically, SEM was available before the PbR mart following inclusion date because of the time taken to process PbR derivations and pricing to support National Tariff policy.

In SUS+, PbR processing is performed at the point at which extracts are requested using a single mart. An equivalent SEM or PbR 'view' can be specified from the single SUS+ data mart in the extract configuration.

Access Levels

Providers and commissioners have different levels of access to data contained within SUS.

Providers may have access to 'clear' (patient confidential data) data.

Commissioner access is restricted to pseudonymised records.

However, certain organisations can be granted access to 'weakly' pseudonymised data which allows greater levels of data linkage for commissioning organisations with accredited safe haven status. Further information can be found on the Data flows transition webpage.

Reasons for Access

Data senders must specify where other organisations, such as commissioners, have a right to access the CDS data.

Data Senders should use the NHS Data Dictionary CDS Addressing Grid to determine who can access the data once it has been submitted to SUS.

Users can select all or a combination of 'Reasons for Access' when requesting extracts from SEM or PbR. The values are either submitted as data items within the CDS or derived in SUS using PDS data

Reasons for Access codes:

Prime Recipient Code:

Provider submitted value

Copy Recipient Code:

Provider submitted value

Provider Code:

Submitted value of Organisation Code (Code of Provider)

Organisation of Responsibility Code (Derived):

Derived from Person Demographics Service (PDS) data using submitted NHS Number. PDS-held GP Practice is used to derive Organisation of Responsibility. Where derivation from PDS is not possible, SUS uses the submitted GP Practice.

Organisation of Residence Code (Derived)

Derived from PDS data using submitted NHS Number. PDS-held Postcode is used to derive Organisation of Residence. Where derivation from PDS is not possible, SUS derives a value using submitted postcode.

Organisation of Residence Code (Submitted)

User submitted Organisation Code of Residence.

Commissioner Code (Submitted)

User submitted Organisation Code (Code of Commissioner). Used in the configuration of SUS PbR Managed Service extracts.

Standard Extract Mart (SEM) View

Data is accessed using a smartcard via the Spine network. This allows the user to extract data where their organisation is identified in Reasons for Access. Details of the data items available in SEM can be found in the Standard Extract Mart (SEM) specification workbook on the SUS Guidance webpage:

Payment by Results (PbR) View

The PbR views contain all CDS data items along with additional derived data items that support national tariff payment.

The SUS Portal User Guide provides guidance on extracting data and SUS Extract Specification workbooks provide details of available data items.

File Formats

Care must be taken with '.csv' or other delimited output because where the delimiter character is present within the data there is no way of distinguishing between it and the corresponding character contained in the data. This can cause errors in software application interpretation of the output columns being misinterpreted.

Commissioner Organisation Derivation

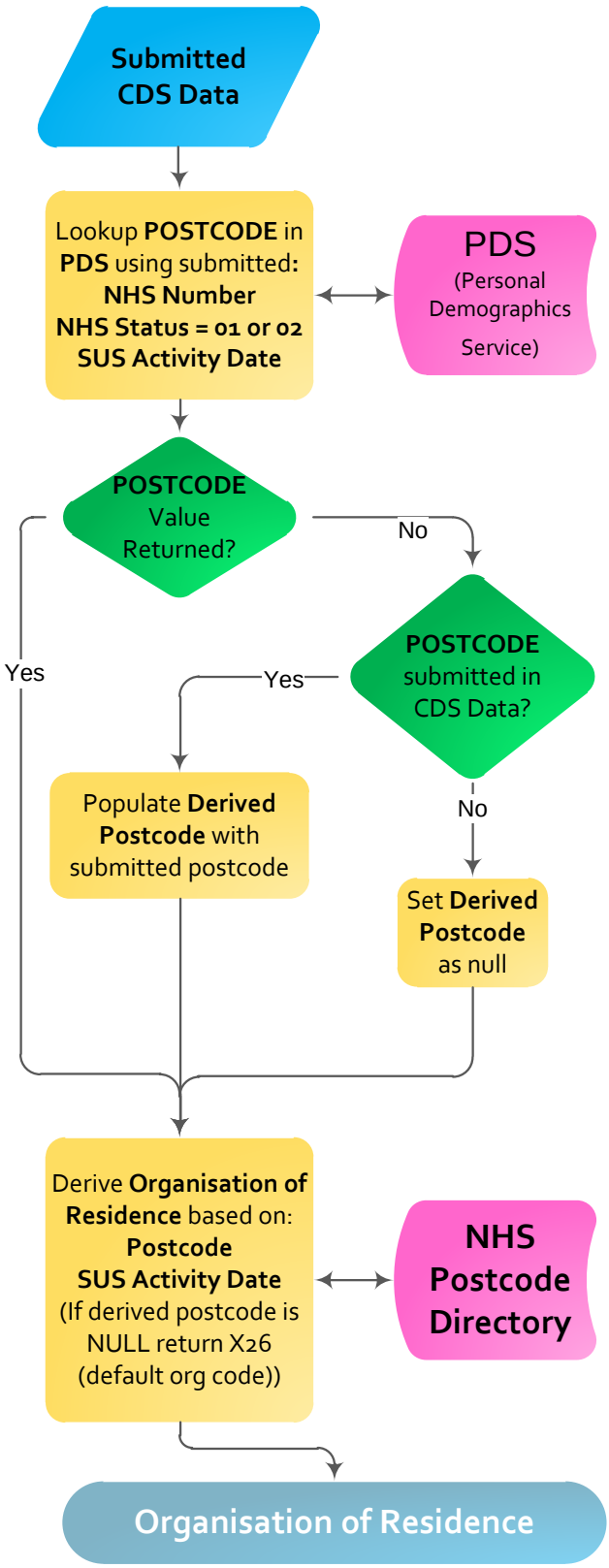
Data Senders are responsible for determining the correct commissioner organisation for all activity and include that organisation within the CDS submission.

The Organisation of Responsibility and the Organisation of Residence are also derived to assist in instances where clarity may be lacking regarding the correct commissioner.

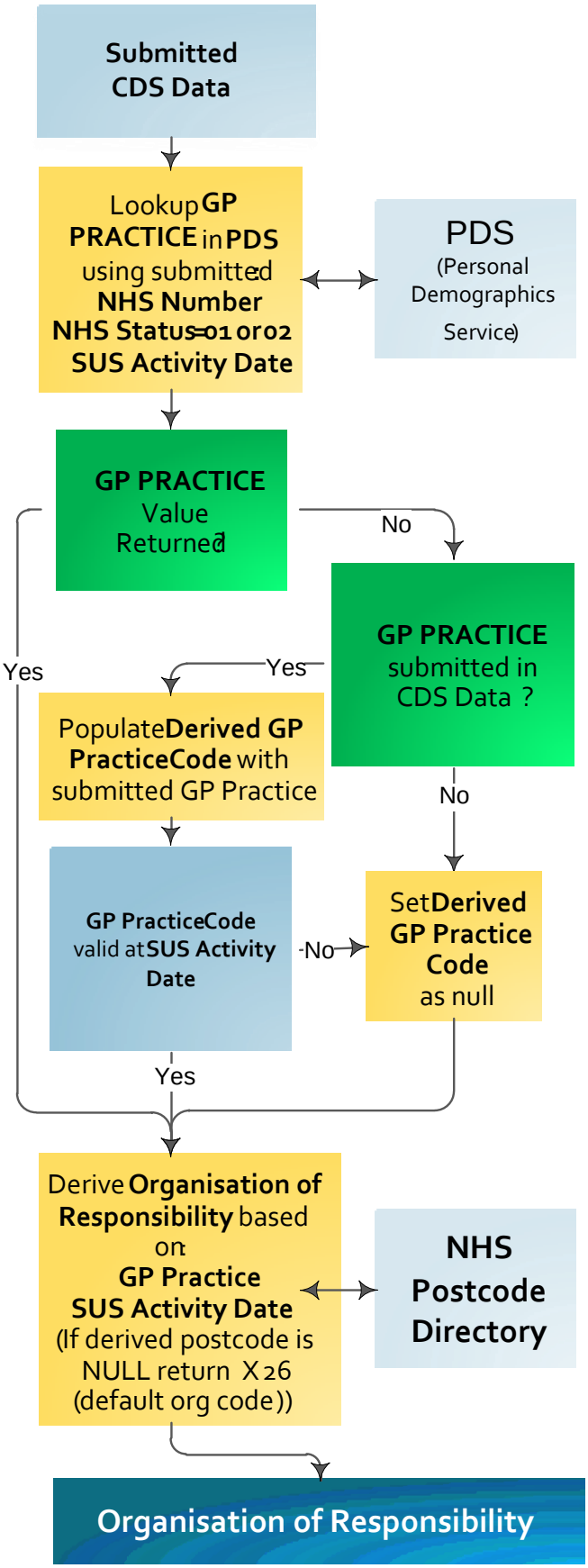
Discrepancies

If a discrepancy exists between submitted and derived values the correct value should be determined through local negotiation. There is no implication that the SUS derived value is any more correct than the provider submitted value.

Organisation of Residence



Organisation of Responsibility



Efficient System Usage

Avoiding Busy Periods

Most extracts are requested at the beginning of the week. Monday mornings are the busiest time and this tails off into Tuesday (the second busiest day). Where possible, SUS users are encouraged to run ad-hoc extracts outside of these times – a lower demand on this service should allow results to be returned more quickly.

There is also a higher demand for extracts in the week immediately prior to a month-end reconciliation deadline. If possible, users should only run essential extracts at this time. Again, this should help all users to receive results more quickly. Reconciliation dates can be found in the latest **SUS PbR Submission Timetable**, available on the SUS PbR Guidance webpage.

The contracted hours of service for SUS are **8am** to **6pm** on normal workdays. Although SUS is available outside of these service hours this is the time when the system can be taken out of service for maintenance activities.

Initiating a large extract late in the day can cause it to fail as it will run into SUS overnight processing. SUS will make two further attempts to restart a job that has been stopped by system processing. After a third stop the job will be marked as a failure. Users must limit the data to be extracted by selecting different dates or specifying organisations in the extract configuration, or no data will be obtained. Under these circumstances simply restarting the same extract will lead to further failure and more lost time for all users.

Avoiding Large Date Ranges

It is strongly advised that organisations do not extract data across extended date ranges on a regular basis. These extracts take a long time to run and will impact extract performance for other users.

NHS England reserves the right to re-prioritise or cancel extracts which are deemed to be using excessive amounts of system resource and which are adversely impacting 'normal' extract processing.

Using 'Reason for Access' Options

The '**Reason for Access'** facility is used to simultaneously extract data across a number of providers and create a single file for all data relating to the organisation code matched against that reason. However, selecting multiple reasons for access significantly increases the processing required to generate the data. The resulting file returns **one line** of data, regardless of the number of reasons matched. It is understood that it may be appropriate to use multiple reasons, but extracts will be delivered more swiftly where an extract uses only one '**Reason for Access'**.

Sharing Extracts in an Organisation

SUS also provides a facility which can automatically share extracts between users in the same organisation. If another user in the same organisation with the same role has requested an extract, the extract will be made available in both users SUS inboxes. This approach will help to reduce system burden of the practice of multiple users submitting the same extract requests.

Cancelling Unrequired Data Extracts

Many extracts are run that are never downloaded. This results in unnecessary load on the system that slows down the processing and delivery extracts for other users. It is therefore recommended that users cancel queued extracts that are no longer required.

Deleting Downloaded Extract Files

Users are encouraged to delete extract files that are no longer required and also delete the links to extracts from their own inbox that have been created by another user. Where a link is deleted, the extract will still be visible to other users with whom the link has been shared.

Extracts for Multiple Organisations

Sometimes it is necessary to extract data for a large number of organisations in a single extract. Users are encouraged only to schedule extracts for the organisations they require data for and to request separate extracts for each organisation.

If only one reason for access is selected, then multiple organisations may run more quickly than running the same extract for each organisation and combining them locally. Extract production times can be variable depending on the load on the system at that time. Extracts will take longer to get to the top of the queue (change from 'Active' or 'Waiting' to 'Processing') at busy times, such as immediately after a reconciliation point.

Extract Management

Users should download extracts to local systems rather than hold them in SUS. Users are therefore encouraged keep the number of extracts in SUS to a minimum and delete extracts once the data has been used.

It is an IG requirement that extracts are deleted from 3 months after the extract date.

Operational Support

Monthly Trust Statements

Monthly Trust Statements are generated to track the status of all data submissions up to the date displayed on the report header. The reports are used to check the status of all submissions for a particular organisation.

Senders are encouraged to use the reports to check that data has been received by SUS, particularly after any organisational or system (PAS or XML) changes.

Monthly Trust Statements are available on the Operational Support webpage.

Monthly Database Counts

The Monthly Database Counts workbooks track the number of records in SUS by Activity Month for the current year and previous two preceding years. Activity is displayed for each CDS type on a separate worksheet and can be used to highlight any peaks and troughs in submissions, or when an organisation has duplicated or deleted data, or started or stopped submitting data.

Monthly Database Counts are available on the Operational Support webpage.

Monthly Performance Review

The Monthly Performance Reviews show service activity levels, delivery performance against targets and system statistics.

Browser Compatibility Issues

On most standard builds, users will not experience any problems and the Portal should function as expected. However, in a small number of cases, browser compatibility or instability issues have been encountered. In nearly all cases, these browser compatibility issues have been successfully resolved by the provider or commissioner's local IT department or service solution.

Users experiencing issues should raise a service call with the National Service Desk (NSD).

Service Availability & Incident Management

This section provides details on:

- Service availability and general support
- Raising an incident
- Incident management process

Service availability and support

Hours of operation

Business hours of operation are **8am** to **6pm Monday** to **Friday** excluding bank holidays. Although the system is usually available outside of these hours, it is occasionally taken down to perform planned maintenance.

"8am to 6pm Monday to Friday"

Notification of Outages

We aim to ensure that where possible outages occur outside of business hours. Any unplanned outage occurring during business hours of will be handled as a high severity incident and regular updates will be posted on the Service announcements and outages webpage.

Interchange failures

Users can expect to be notified of any interchange validation failures within **3 business hours**. However, at busy times, this may take longer so please allow **8 business hours** before reporting any delays.

Please note that where interchanges are submitted via a third party, notifications of invalid interchanges will be sent to the third party.

Data availability

PbR Inclusion and Delivery Dates are published on the SUS PbR Guidance webpage.
PbR processing is applied when extracts are requested. The length of time taken for extracts to run depends on the size of the extract and complexity of the database search as determined by its parameters.

Raising an incident

If the service levels outlined above are not met, or if the system does not behave as you would expect, users are advised to raise a call with the National Service Desk.

For any service issues, please contact the **National Service Desk** (NSD) via:

NSD weblog tool (log in and N3 connection required)

Or call on **0300 30 35 035**

The **Help section** of the SSD National Service Desk login webpage provides guidance on how to register with NSD and how users that do not have an N3 connection can raise an incident. Any users experiencing any problems with Weblog or registration process are advised to telephone the helpdesk.

Incidents are generally resolved more quickly if details of the issue are provided using the **weblog tool**. Users can expect a response as per the following table:

Severity	Resolution time
Sev1	4 hours
Sev2	8 Hours
Sev3	20 Hours
Sev4	80 Hours
Sev5	200 Hours

Patient Confidential Data

Patient Confidential Data (PCD) should never be included in either a telephone conversation or weblog call with NSD. Inclusion of such information constitutes a reportable breach of information governance rules. If it is necessary to refer to individual records to illustrate the issue, the SUS Generated Record ID should be used as it is not PCD.

Incident Management Process

The National Service Desk (NSD) is open from **08:30** to **17:30 Monday** to **Friday** excluding Bank Holidays.

Updates regarding higher severity incidents will be published on the Service Management Service Status webpage.

When reporting an issue via telephone, by the end of the conversation users should have been told:

- The reference number allocated to the issue
- The name of the operator who logged the call
- The short description recorded for the issue
- Confirmation of user reference number if provided
- The priority (Severity Level) allocated to the issue

If it is possible to resolve the issue immediately, a summary of the resolution will be provided. If it was not possible to resolve the issue immediately users will be advised when a progress update can be expected.

Whether an incident is raised with NSD via telephone, weblog, or both; a confirmation should be received.

When a resolution has been determined, users will be contacted with the details. NSD will keep the incident open for **3 working days** to allow users time to respond if they do not think the issue has been resolved.

- No further action is required if the issue is considered to be resolved.
- If a related issue persists users should reply within three working days and the resolution will be reviewed.

If NSD has not had a response after **3 working days** the call will be closed. If the call is closed users must raise a new incident.

Independent Providers

It is important that Independent providers of NHS care adhere to the following guidance in order to ensure that their data is correctly configured and can be accessed in SUS:

- Reference Data Configuration
- Accurate Data Submission
- Setting Extract Parameters

Reference Data Configuration

Questions 1-3 of the Independent Provider registration form determine the data available in SUS:

Question 1: Populate the Parent/HQ code (either a 5- or 3-character code) and include the name of the organisation. E.g: XYZA1 or XYZ, Provider Name)

Question 2: Populate the 3-character Organisation Code e.g: XYZ

Question 3: List all sites participating in the ISHP arrangement by name and ODS code. **5 character provider code** with the first 3 characters corresponding to the code given for Question 2.

Example for Question 3:

XYZA1	Name of Provider, Anytown 1
XYZA2	Name of Provider, Anytown 2
XYZA3	Name of Provider, Anytown 3

Accurate Data Submission

Organisation Code (Code of Provider)
The Organisation Code (Code of Provider) can be the 3-character HQ code or the 5-character site code of treatment. Incorrectly assigned Organisation Codes can impact on the quality of Patient Reported Outcome Measures (PROMS) data and Choose and Book (CAB) data flowing from HES from certain independent organisations. Site code of Treatment must still be completed with the 5- character code for the actual site of treatment.

CDS Update Type
NET submitters (Data Senders using the NET submission method) must ensure that when updating and adding new records to SUS they use a CDS Update Type of 9. The incorrect use of CDS update Type 1 will cause the record to 'self-delete'. Where no matching record exists on the database, no record will be added.

CDS Unique Identifier (CDS Unique ID)
NET submitters must ensure that their CDS Unique ID algorithm derives a unique field for every record submitted to SUS. An algorithm that is unique for every patient is not unique for every record. CDS Unique ID is an essential data item required for NET submission and, if it is not unique, records will be inadvertently overwritten by subsequent submissions.

Setting Extract Parameters

Organisation:
All participating organisation sites, entered for **Question 3**, are available for selection. Users can select many Organisations at a time by using the "ctrl" or "shift" key. If only the 3-character Parent/HQ code is selected data for all the sites will *not* be selected. Instead users must select the 5-character organisation codes that were submitted as the Code of Provider. If an organisation is not available, or no data is extracted the reference data may not be correctly configured. Users should raise a call with National Service Desk.

Reason for Access:
Select "Provider Code"

Date From and **Date To:**
Records where the **Activity Date** is between these two dates will be included within the extract.

Commissioner:
Leave as "**All**" unless a specific Commissioner is required.

Provider:

Leave as "**All**".

CDS v6.2 Human Behavioural, Organisational and Technical Guidance

The Human Behavioural, Organisational and Technical Guidance document outlines the way in which changes to the Commissioning Data Sets (CDS) version 6.2 should be interpreted and used by clinical, administrative and informatics staff involved in secondary care which is NHS funded and/or provided by NHS Organisations.

The recommended audience is:

- **Providers of NHS Funded Care** (including Trusts and Independent Sector Providers)
- **Suppliers of secondary care systems**, including Patient Administration Systems (PAS), Clinical Care Records systems and other operational systems such as Accident and Emergency, Maternity and Critical Care
- **CDS XML/middleware suppliers**
- **Other organisations** that use the CDS Information Standard

This document provides information about the usage and implementation of CDS6.2 and contains a useful **Summary of Changes** in **Section 4**.

The document can be accessed via the ISB website.

www.isb.nhs.uk/documents/isb-0092/amd-16-2010/0092162010guid.pdf

XML Service Suppliers

IQVIA Technology Services (IMS/Ardentia)
Ardentia House
Staffordshire Technology Park
Stafford
ST18 0LQ.
www.imshealth.com

EMIS (Indigo4)
Aizlewoods Mill
Nursery Street
Sheffield
S3 8GG.
www.indigo4.com

Iuvo
6 Windsor Court
Clive Road
Redditch
Worcestershire
B97 4BT
www.iuvo.co.uk

Further Information

There are several web resources containing information for SUS users. These include:

- SUS Guidance material
- SUS Updates via SUS 'What's New'
- NHS Data Dictionary
- Information Standards Notices
- Data Set Change Notices

SUS users are encouraged to review these information sources regularly.

SUS General Guidance

SUS PbR Guidance

SUS What's New

NHS Data Dictionary
Information Standards and Collections (Including Extractions) - National Governance

http://digital.nhs.uk/isce

www.isb.nhs.uk/library/dscn

www.isb.nhs.uk/library/isn

It is recommended that SUS users set up internal processes to review Information Standards updates so that they are kept aware of all changes that affect them. Users can subscribe to the ISB distribution list to receive notifications of updates to these standards:

www.isb.nhs.uk/yoursay

Glossary of Terms

Term	Definition
A&E	Accident and Emergency
ACC	Adult Critical Care
APC	Admitted Patient Care
AQP	Any Qualified Provider
BP	Best Practice
CAG	Confidentiality Advisory Group
CC	Critical Care
CCG	Clinical Commissioning Group
CCP	Critical Care Period
CCUF	Critical Care Unit Function
CDS	Commissioning Data Set
CR	Commissioning Region (of NHS England)
CSU	Commissioning Support Unit
DH	Department of Health
DoB	Date of Birth
DPA	Data Protection Act
DQ	Data Quality
DRP	Data Retention Policy
DSCRO	Data Services for Commissioners Regional Office
EM	Emergency Medicine
FCE	Finished Consultant Episode
HES	Hospital Episode Statistics
HRG	Healthcare Resource Group
HSCIC	Health and Social Care Information Centre
ICD	International Classification of Diseases
IG	Information Governance
ISN	Information Standard Notice
LoS	Length of Stay
MESH	Message Exchange for Social Care and Health
MHMDS	Mental Health Minimum Data Set
MSC	Main Specialty Code
N3	National Broadband Network for the NHS
NCC	Neonatal Critical Care
NHS	National Health Service
NHSE	NHS England
NIGB	National Information Governance Board
NSD	National Service Desk
NWCS	NHS-Wide Clearing Service
ODS	Organisation Data Service
OP	Outpatient
OPCS	Office of Population Censuses and Surveys
PbR	Payment by Results
PCC	Paediatric Critical Care
PDS	Patient Demographics Service
PCD	Person Confidential Data
PPI	Patient Pathway Identifier
RA	Registration Authority
RAP	Readmissions Pathway
RBAC	Role Based Access Control
RTT	Referral to Treatment
SEM	Standard Extract Mart
SSC	Specialised Service Code
SUG	SUS User Group
SUS	Secondary Uses Service
TATD	Tactical Authority To Deploy
TFC	Treatment Function Code
TMS	Transaction Messaging Service
UUID	Unique User Identity
XML	Extensible Mark-up Language (encoding) for information