NHS Digital

Submitting CDS Data to SUS

Using BULK or NET submission methods to send data to SUS

Information and technology
for better health and care

Contents

Introduction

This Document

SUS (Secondary Uses Service) is a comprehensive repository for hospital activity data which enables a range of reporting and analyses. The data supports the NHS in planning, commissioning, management, research, auditing and public health. This document details some key considerations when sending data to the SUS system. It should be read in conjunction with the NHS Data Dictionary which details the format and content of the data to be sent.

The NHS operating framework states that SUS should be used as the standard repository of activity data for performance monitoring, reconciliation and payments.

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

All sending organisations must register to submit data to SUS by completing a SUS SR1 Registration Form which is available on the SUS Guidance webpage.

This document provides guidance on submitting CDS data to SUS+. It describes:

- Considerations to protect the patient's confidentiality in the data submitted
- The steps taken by the SUS service to ensure that patient's confidentiality is protected
- The steps required to begin sending data to SUS+
- Choosing between BULK and NET submission protocols
- Things to consider when organisations split or merge

Audience

Providers

Providers of secondary care

Providers are encouraged to refer to this document to understand how to submit data to the national service and how their data will be processed.

PAS system and XML Middleware Suppliers

PAS (Patient Administration Systems) and other CDS (Commissioning Data Sets) suppliers and XML Middleware suppliers are advised to refer to this document to gain an understanding of the functions and changes required to support migration from BULK update to NET change.

Legal requirements for the submission of data to SUS

There are two areas where NHS Digital and the providers of data to SUS have specific legal duties of care regarding the protection of the patient's identity:

- NHS Digital has a duty of care to ensure that the patient's confidentiality is protected and is only known to those with a legal basis to access it
- Certain legislation requires that additional safeguards are implemented to protect the identity of patients who receive treatments regarded as Legally Restricted.

Protecting the Patient's Identity

Some organisations that receive data from SUS do not have a legal right to know who the patient is. In fulfilling its duty of care to protect the patient's identity, NHS Digital regards that certain fields present a risk of identifying the patient. These fields are known collectively as Person Confidential Data (PCD) and are listed in Appendix A.

When sharing submitted data with users or other systems who are not authorised to know the identity of individual patients, NHS Digital either pseudonymises or removes the contents of the PCD fields. This allows NHS Digital to share the data without divulging the identity of the patient.

If PCD data is included in fields other than the fields specified to contain it there is a risk that these are identifiers could be accidentally released by NHS Digital. This section describes the steps that NHS Digital takes to ensure that PCD is not included in other data fields and inadvertently shared. The presence of PCD in unexpected fields is referred to as PCD Leakage.

Failure to comply with the information in this section could result in the redaction of data fields found to contain unauthorised PCD.

Submitters of data to SUS+ are advised that they must not introduce personal confidential data (PCD) into any field other than the one identified to contain that data. The presence of PCD in a field that is not identified to contain that PCD is considered leaked PCD. NHS Digital may redact fields containing leaked PCD.

For example, NHS number should only appear in the NHS number field. If NHS number is introduced into another field, such as CDS Unique Id, then this would put NHS Digital at risk of inadvertently disseminating PCD in the clear and illegally identifying the patient.

Similarly, the PCD of one type (e.g. NHS Number) should not be used to form all or part of other PCD fields, for instance the Patient Pathway Identifier. This is because some data recipients are permitted to see some PCD fields but not others. In these cases, leaked PCD could be released illegally.

SUS+ has introduced a data interchange scanning capability that will screen CDS interchanges before data is accepted into SUS+. Should SUS+ detect PCD data items in fields not intended for that data then the data item will be redacted, and the data provider notified. The scanning will allow for small numbers of false positives. False positives will not be shown on the Interchange Feedback or Data Quality reports.

Commissioners and other recipients of SUS data will only have access to the redacted version of any fields identified as containing leaked PCD. Redaction will only occur on records where PCD is leaked.

This facility is initially implemented in 'warn only' mode but will be switched to 'redact' mode. Further communications will be made via the What's New page on the SUS website as progress is made with this development.

It is important that data providers raise a call with the National Service Desk if they feel that data is being identified as PCD leakage incorrectly. This will allow the team

to review and fine tune the algorithm appropriately before data is redacted.

Summary details of inappropriate use of PCD data are available in the Interchange Feedback report. This report details the processing status of interchanges submitted to SUS and can be requested via the SR1 form. Instructions for completing the SR1 form and requesting the Interchange Report are available in the Sender Registration Section of the SUS web page.

Details of the section of the report related to the inappropriate use of PCD data are included in Appendix B of this document.

Details of all records in an interchange that are identified as having leaked PCD are available in the Interchange Data Quality Report. Procedures for accessing this report, its contents, format and use are available here.

Data Related to Legally Restricted Records

'Legally restricted records' were previously referred to as 'Sensitive Records'. The change is in response to a review of terminology in relation to the data protection act.

To ensure that the SUS+ service is processing CDS data in accordance with the law it uses a list of legally restricted codes.

The list of codes regarded by SUS+ as being legally restricted is published separately on the SUS website. Any amendments to the current list will be updated in that document and communicated to the user community through a release note and What's New announcements as well as through the User Group and User Show and Tells.

CDS XML Submission

On submission of records containing legally restricted codes, or where a patient has submitted a withdrawal of consent request, providers must **anonymise** the record by removing the following PCD items before submitting data to SUS.

- NHS Number
- Patient name and address (if present)
- Local Patient Identifier
- Date of Birth
- Postcode

Other data items in the PCD list are used by SUS in its processing and are removed by the SUS system before being disseminated.

Any patient withdrawing consent must have their identity verified by the provider in line with the Data Protection Act 1998 and local information governance policy. It may be appropriate for this to be managed by the information governance department where applicable.

NHS Number Status Indicator

Organisations sending anonymised records must populate **NHS Number Status Indicator** with the value **07 (NHS number not present and trace not required)** for these records.

Withheld Identity Reason

Organisations sending anonymised records are also advised to populate **Withheld Identity Reason** with the appropriate value for these records in line with the NHS Data Dictionary.

SUS Processing

SUS anonymizes records that contain legally restricted diagnosis codes and procedure codes (OPCS, ICD-10, SNOMED or READ) or where a patient has registered a withdrawal of consent with NHS Digital. This processing removes the values from the PCD fields listed in Appendix A.

The processing performed by SUS does not reduce the responsibility of the provider to anonymise records before transmission.

SUS+ does not anonymise delivery date, even if it is the same as the baby's birth date.

For PbR spells that contain one or more episodes that are legally restricted, all episodes in the spell will be linked and processed/priced then all PCD data will be removed from all episodes in the spell. This processing is also carried out where a 'Withdrawal of consent' has been recorded by the patient with NHS Digital.

Confidentiality Category
Processed SUS records contain a derived '**Confidentiality Category**' data item, which is applied as follows.

[blank] Not marked as confidential

2/3 **Legally Restricted Record.** Record contains procedures or diagnoses that are restricted. PCD set to NULL.

4 **Withdrawal of Consent Record** Any data related to a patient has withdrawn their consent and registered that fact with NHS Digital

NHS Number Status

Legally restricted records are also assigned an **NHS Number Status** of **91** which indicates that SUS has anonymised the data.

Selecting the Submission Method

SUS supports **BULK Update** and **NET Change** submission methods.

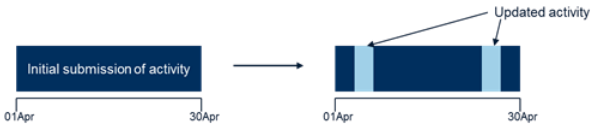
BULK Update Summary

When using 'BULK Update', all records within a specified period are submitted, replacing any activity currently held on the database for activity held between the dates specified.

Many organisations that deal with multiple source data sets are not able to submit using NET Change submission method due to technical difficulties in isolating records, and therefore submit using BULK update.

NET Change Summary

When using 'NET Change', only records that are new, or where details within the record have changed, are submitted. This can also include record-specific deletions.



NET change allows for more precision in managing records and generally reduces the load on the system due to the reduced number of records and processing required.

Although only 30 percent of submissions currently use NET Change submission method, many patient administration systems are capable of automatically producing CDS submission data files containing only the records that are new or have changed for a specified period. Where a single data source is used for CDS this would directly enable NET submission by those organisations.

Using BULK Update

Required Data Items

Details about the process and the CDS data items required for both **BULK** update and **NET** Change are defined on the Commissioning Data Set Submission Protocol page of the **NHS Data Dictionary**.

CDS INTERCHANGE SENDER IDENTITY
an15
The assigned EDI Address of the physical ORGANISATION or site responsible for sending commissioning data.
CDS SENDER IDENTITY
an3 or an5
The identity of the organisation acting as the Sender of a CDS submission.
CDS BULK REPLACEMENT GROUP CODE
an3
The CDS Group into which CDS Types must be grouped when using BULK update
CDS EXTRACT DATE
an10 ccyy-mm-dd
The date (along with an associated CDS EXTRACT TIME) of the update event. Used to identify the date when the update was made.
CDS EXTRACT TIME
HH:MM:SS
The time (with an associated CDS EXTRACT DATE) of the update event. Used to identify the time when the update was made.
CDS REPORT PERIOD START DATE
an10 ccyy-mm-dd
The start date (for the date range of the data being replaced) of the Bulk update time period.
CDS REPORT PERIOD END DATE
an10 ccyy-mm-dd
The end date (for the date range of the data being replaced) of the Bulk update time period.
CDS ACTIVITY DATE
an10 ccyy-mm-dd
"CDS Originating Date" specifically identified for each CDS TYPE

When a CDS interchange is submitted, SUS identifies the CDS SENDER IDENTITY**.** On doing so, it verifies all 5 characters, meaning that a code of **RNN** is different from **RNN00** and both are different from **RNN01** even though they are all clearly related to the same Organisation.

Using CDS REPORT PERIOD START DATE and CDS REPORT PERIOD END DATE the Sender ID and date combination is then verified against reference data which logs all previous submission periods for that sender.

Each **CDS TYPE** belongs to a **Bulk Replacement Group**. The CDS BULK REPLACEMENT GROUP CODE is used with the other listed data items to determine which records are replaced and processed.

Example:

All Finished Episode CDS Types

- ***General***
- ***Delivery***
- ***Birth***

Belong to the same Bulk Replacement Group.

A sender should include all records for these CDS Types in the same bulk interchange when they belong to the same period.

*Sending CDS Types **Finished General**, then **Finished Delivery** and then **Finished Birth** in separate interchanges for the same period will result in only the **Births** appearing in SUS data for that period.*

Initial Submission

If the sender has *not* previously sent data with the **same** CDS REPORT PERIOD START DATE and CDS REPORT PERIOD END DATE, the interchange will be accepted for processing.

Follow-up Submissions

If data has previously been sent for the **same** report period start and end dates, SUS verifies the CDS EXTRACT DATE and CDS EXTRACT TIME.

Rejected Interchanges (Not Applied)

If the interchange extract date and time is ***less than*** any interchange previously received from the same CDS SENDER IDENTITY, the interchange will not be processed. However, the system will record that the attempted transaction took place. Non-processed interchanges are identified in SUS Tracker as 'Not Applied'.

- Accepted Interchanges

If the interchange extract date and time combination is ***greater than or equal*** *to* the equivalent date and time in any interchange previously received from the same CDS SENDER IDENTITY, the interchange will be accepted for processing. All matching data is deleted between the report start and end dates. The records in the new BULK interchange are appended to the SUS database.

Matching records have:

- The same CDS BULK REPLACEMENT GROUP CODE
- The same CDS SENDER IDENTITY
- A CDS ACTIVITY DATE (episode end date for FCEs) between the CDS REPORT PERIOD START DATE and CDS REPORT PERIOD END DATE in the new BULK interchange

For example, where data is sent for 1st to 31st May and then re-sent with a later CDS EXTRACT DATE, also for the 1st to 31st May, the previously submitted records within these date parameters will be deleted and replaced with the new submission.

However, where data is submitted for 1 to 31 May and then resubmitted with the same, a later or an earlier CDS EXTRACT DATE but for 1 to 30 May, only the previously submitted records within these date parameters will be deleted. The records for 31t May will not be affected. If the new file contains data for 31st May records for this day will be duplicated on SUS. There is no check at SUS to ensure activity dates are within the stated report period dates. Care should therefore be taken when defining the report period dates as this is often a manual stage in the process. This error can be most easily rectified by resubmitting May data with the correct report period dates of 1st and 31st May and a later extract date than previous submissions.

Removal of CDS Prime Recipient Identity

Historically, the CDS PRIME RECIPIENT IDENTITY data item was a required field for BULK update submissions. Since April 2013 (SUS Release 13) this requirement

was removed in order to eliminate the risk of duplication of data due to changes in the patient's postcode. However, removing CDS PRIME RECIPIENT IDENTITY from the update method now means that changing the CDS SENDER IDENTITY of a record can have two possible effects:

- A new code that has not previously been received by SUS for the interchange report period will cause a duplication of those previously submitted records of the same included Bulk Replacement Groups containing the original CDS SENDER IDENTITY.

- Records containing a CDS SENDER IDENTITY code that has been received previously will replace those existing records for the same CDS Sender Identity, Interchange Report Period and included Bulk Replacement Groups. This does not necessarily equate to a direct replacement of like for like records. Senders with more than one data flow, from multiple sites should be aware of this, particularly when different sites at the same organisation are sending their own data.

Using NET Change

Required Data Items

Details about the process and the CDS data items required for both **BULK** update and **NET** Change are defined on the Commissioning Data Set Submission Protocol page of the **NHS Data Dictionary**.

CDS INTERCHANGE SENDER IDENTITY
an15
The assigned EDI Address of the physical ORGANISATION or site responsible for sending Commissioning data.
CDS SENDER IDENTITY
an3 or an5
The identity of the organisation acting as the Sender of a CDS submission.
CDS UNIQUE IDENTIFIER
an35
A CDS data element providing a unique identity for the life-time of an episode carried in a CDS message. This field must not contain any data that could be used to identify the patient. This includes but is not limited to NHS Number and Local Patient ID
CDS APPLICABLE DATE
an10 CCYY-MM-DD
The date (with an associated CDS EXTRACT TIME) of the update event (or the nearest equivalent) that resulted in the need to exchange this CDS
CDS APPLICABLE TIME
an8 HH:MM:SS
The time (with an associated CDS EXTRACT DATE) at which the CDS extract was undertaken.
CDS UPDATE TYPE
an1
1 indicates a CDS Deletion or Cancellation, 9 indicates a CDS Original or Replacement
CDS TYPE CODE
an3
The code to identify the specific type of Commissioning Data Set data

Initial Submission

When an interchange is submitted using NET change submission method

CDS SENDER IDENTITY

and

CDS APPLICABLE DATE **/** CDS APPLICABLE TIME

are verified against SUS reference data .

CDS UNIQUE IDENTIFIER

is verified against existing SUS data.

CDS TYPE CODE is then used to determine the corresponding records to be updated.

Where CDS Update Type = 9 (CDS Original or Replacement) and a CDS UNIQUE IDENTIFIER is not already present in SUS for that CDS SENDER IDENTITY, the record is accepted for processing

Follow-up Submissions

When a subsequent interchange is submitted using NET change it is possible to update or delete records held in SUS.

Where CDS Update Type = 9 (CDS Original or Replacement) and a CDS UNIQUE IDENTIFIER is already present in SUS for that CDS SENDER IDENTITY, the record is accepted for processing.

Where CDS Update Type = 9 and one or more records for the same CDS SENDER IDENTITY with the same CDS UNIQUE IDENTIFIER are found to exist in SUS, and where the CDS APPLICABLE DATE and CDS APPLICABLE TIME is later than the CDS APPLICABLE DATE and CDS APPLICABLE TIME on the existing record, those existing records will be replaced with the records in the new interchange

Where CDS Update Type = 1 and one or more records for the same CDS SENDER IDENTITY with the same CDS UNIQUE IDENTIFIER are found to exist in SUS, and where the CDS APPLICABLE DATE and CDS APPLICABLE TIME is later than the CDS APPLICABLE DATE and CDS APPLICABLE TIME on the existing record, those existing records will be deleted

- **If a record with matching CDS SENDER IDENTITY and CDS UNIQUE IDENTIFIER**

has previously been sent as BULK the CDS APPLICABLE DATE and CDS APPLICABLE TIME will be compared to the CDS Extract Date and Time on the existing record. Where the CDS APPLICABLE DATE and CDS APPLICABLE TIME is later than the CDS EXTRACT DATE and CDS EXTRACT TIME on the existing record, those existing records will be replaced with the records in the new interchange or deleted.

'Self-delete' Records

NET Change submission enables data senders to delete records themselves by sending a NET delete record (CDS Update Type = 1, CDS Deletion or Cancellation). This is a 'self-delete' record where all matched records (i.e. records containing the same CDS SENDER IDENTITY and CDS UNIQUE IDENTIFIER**)** will be flagged as logically deleted. This means that SUS does not physically delete the record itself but rather marks the record as deleted.

Note: it is not possible to change a CDS UNIQUE IDENTIFIER ***that is already in SUS. It is only possible to update the data within the record or delete the record entirely.***

Changing APC CDS Types via NET Change

The **APC CDS Types** in the table below allow NET submission method to update or delete an existing record containing a different CDS Type.

Incoming CDS Type	Existing CDS Types that incoming CDS type will overwrite
120	120, 180
130	130,140,190,200
140	130,140,190,200
180	120, 180
190	130,140,190,200
200	130,140,190,200

These changes may include:

Unfinished	**to**	**Finished**
General	**to**	**Birth**
Birth	**to**	**General**

As can be seen from the table, it is also possible to make the following change:

Finished	**to**	**Unfinished**

Please note that SEM (Standard Extract Mart) and PbR views present this change differently where an interchange is made up entirely of unfinished activity.

For all other CDS types (listed below) NET change will only update/ delete an existing record containing the same CDS type:

Incoming CDS Type:
10, 20, 21, 30, 40, 50, 60, 70, 80, 90, 100, 110, 150, 160, 170, 210

Considerations when Mixing Submission Methods

Data senders can use NET Change and BULK Update according to which method is most suited for the interchange and CDS type they are sending to SUS.

Bulk updates will replace data sent as net change. All bulk processing procedures above will apply with regard to Report Period, Sender Code, Bulk Replacement Group and Extract Date and Time

Net changes will be applied to data sent as bulk update. All net processing procedures above will apply with regard to CDS Unique Identifier, Sender Code and Applicable Date and Time.

New records that meet acceptance criteria can be submitted under either method.

Risks

Mixing NET and BULK submission methods for the same CDS Types brings with it the following associated risks.

If the system finds one or more records for the same CDS SENDER IDENTITY with the same CDS UNIQUE IDENTIFIER, but where the Applicable date and time is earlier than the previous NET applicable date and time (or BULK Extract date and time) for all existing records the interchange will not be accepted. The previous applicable date and time includes test submissions and deletion submissions

NET change cannot identify BULK records without a CDS UNIQUE IDENTIFIER and, since this ID is mandatory for NET change submission method NET change cannot be used to replace BULK records without a CDS UNIQUE IDENTIFIER. Effectively, this practice means all records are duplicated when resubmitted in a NET interchange under these circumstances as they are all considered to be new records.

Missed Inclusion Dates and Retrospective Submissions

The SUS Submission Timetable (published annually on the SUS PbR Guidance webpage) provides an important supporting timescale framework for the NHS payment system. It enables the production of point in time snapshots of activity data to be provided to providers and commissioners from a known 'Inclusion Date' (submission deadline).

It is possible for data senders to miss an Inclusion Date or need to resubmit corrected or missing data retrospectively.

NHS Digital is not permitted to **change** the data submitted to SUS from provider organisations because SUS is used as a financial reimbursement solution. It is therefore necessary for the sender organisation to resolve the situation by resubmitting the appropriate data, using either BULK Update or NET Change. However, there are different factors and implications to consider for each situation, as described below.

Missing an Inclusion Date

Missing an Inclusion Date is commonly due to a provider or their XML translation supplier encountering technical issues or problems when submitting CDS records via XML.

The impact of missing an Inclusion Date is that the Reconciliation and Post-Reconciliation views will not contain up-to-date activity data.

Where a sender organisation has missed Inclusion Date, they should submit their activity and contact their commissioner to explain that the data has been submitted late and that it is available in the SUS **PbR Current** view and SEM view. Both organisations can then use the **PbR Current** view to determine a baseline to support contract reconciliation.

Resubmitting corrected or missing data

Activity data can change over time and may need to be corrected or completed. Providers can resubmit data as often as they wish, as long as this is in line with guidance for their chosen submission method (BULK or NET).

Where resubmissions are made *before* an **Inclusion Date** there is no impact. However, where resubmissions are made *after* an **Inclusion Date** the appropriate action should be taken, as described earlier in **Missing an Inclusion Date**.

Large Retrospective Submissions

SUS users wishing to perform large retrospective submissions are encouraged to submit them on a staged, month by month basis, ensuring that the resubmitted data is correct each month. SUS expects year to date resubmissions to occur as one offs every 3 to 6 months and at annual refresh. SUS users are reminded that Information Governance rules are "minimum amount of data sent for a specific purpose".

In most cases the priority for resubmission should be the most recent full month. Working back through the current financial year months, each month should be resubmitted and checked before moving on to the next. **Inclusion Dates** have already passed but this will allow corrected data in PbR Current or SEM to be accessed by commissioners.

Impact on HES

HES (Hospital Episode Statistics) data is updated monthly and each month the current financial year activity data submitted to SUS is used to update HES. Therefore, corrected or late-submitted data received after **Inclusion Date** will be reflected in HES in the following month.

If data is resubmitted after **HES Annual Refresh**, HES will not be updated with corrected data for that financial year. If this happens, data senders are advised to

contact enquiries@digital.nhs.uk and request that a HES Data Quality (DQ) note is placed against the relevant HES activity data for the data sender organisation.

Sender Organisation Identifiers

Sender organisation data items:

CDS INTERCHANGE SENDER IDENTITY

CDS SENDER IDENTITY

ORGANISATION CODE (CODE OF PROVIDER)

Are used to:

- **Register flows**
- **Authenticate submissions**
- **Sequence interchanges**
- **Enable monitoring**

CDS Interchange Sender Identity

Identifying a sending instance

CDS INTERCHANGE SENDER IDENTITY is used to identify an organisation sending an interchange. It is presented as a 10 character EDIFACT id with a 5 character local 'tail', making a 15 character code. Typically it might look like this:

190000099900001

Where **1900000999** is the **EDIFACT ID** and **00001** is the **local 'tail'**.

A new organisation can obtain a unique 10 character EDIFACT ID from the Address Registration Service**.**

It is recommended that the remaining 5 characters are used to uniquely identify the individual XML translation applications where more than one is in use by an organisation. Individual organisations are responsible for determining and managing the local 5 character 'tail'.

Most senders use the same 5 character suffix for all data (e.g. 00001.) However, some senders choose to use a different suffix for different dataset types (APC, OP etc.) or to identify different PAS systems locally. There are risks associated with this practice and data senders are advised to make sure they fully conversant with submission methods before adopting this method.

CDS INTERCHANGE SENDER IDENTITY is found in the **CDS INTERCHANGE HEADER.** The full code is used in the registration process.

Interchanges are sent to SUS by the Electronic Data Transfer (EDT) client, which is managed by SUS. It is worth noting that the same sending application can be used to send interchanges for more than one CDS INTERCHANGE SENDER IDENTITY but there can be only one CDS INTERCHANGE SENDER IDENTITY per interchange.

Sequencing Interchanges

The CDS INTERCHANGE SENDER IDENTITY is used to sequence interchanges at the 15 character level. SUS assumes that the order received from the EDT client is the order in which interchanges should be processed.

Potential Problems in sharing a Sender ID

Sharing a 15 character CDS INTERCHANGE SENDER IDENTITY across **multiple** organisations/senders/types can potentially cause the following:

- **Delays to SUS processing**
  SUS Processing can be delayed because all submissions from that address will be processed in order of receipt and only one interchange within a sequence can be processed at a time.
- **Submission progress tracking issues**
  It is possible to have multiple contacts for a single sender. It can therefore be difficult to ensure that all affected users are aware of submission issues or failures.

Organisations sending from a single 10 character EDIFACT code are therefore advised to consider using different 15 character variants (such as providers with multiple sites and/or PAS systems) of CDS INTERCHANGE SENDER IDENTITY to avoid these potential problems.

Tracking submissions

When an interchange is processed, the first 10 characters of the CDS INTERCHANGE SENDER IDENTITY are referenced against the registered ODS code for that sender (as submitted on the SR1 Sender Registration form). SUS **Tracker** uses the three-character ODS code for NHS providers and

5-character ODS code for non-NHS data sender organisations.

Tracker looks up the registered ODS code at the time the interchange was submitted and determines the valid organisation name. If a CDS INTERCHANGE SENDER IDENTITY is re-used without re-registration the interchanges will not appear on the new organisation's Tracker report.

Interchanges for newly registered codes will only show on Tracker against the new organisation *after* the registration has been processed.

The SR1 form must also be used to register *changes* to CDS INTERCHANGE SENDER IDENTITY and/or the associated ODS code and contact details.

The **SUS SR1 Registration Form** is available on the SUS Guidance webpage.

CDS Sender Identity

There is potential for confusion between the CDS SENDER IDENTITY and CDS INTERCHANGE SENDER IDENTITY data items. Users should therefore ensure that they clearly distinguish between the two.

CDS SENDER IDENTITY is a 3 or 5 character organisation code assigned to each organisation by ODS. 3 character codes identify an organisation and the 5 character codes are used to identify site. As previously stated

- **Rnn**
- **Rnn00**
- **Rnn01**

are all treated as different entities by SUS.

The CDS SENDER IDENTITY forms part of the unique record level update key for both BULK update and NET change. Changing the CDS SENDER IDENTITY for data that has already been sent will cause duplication because SUS will not recognise the new records as replacing the old ones.

CDS SENDER IDENTITY is found in the **CDS TRANSACTION HEADER GROUP.**

It is reported on the Data Quality Report (DQR) and is shown when a user drills down into an organisations DQR.

Organisation Code (Code of Provider)

ORGANISATION CODE (CODE OF PROVIDER) is not a sender code and is not used as a key. It is included here for completeness because it is used in reporting.

It is an ODS code and is always used to report at the organisation level (at three characters for NHS providers and 5 characters for non-NHS data senders.

PbR or SEM extracts use the Organisation Code data item to match against "Reason for Access" and/or the selected provider. Data is only available for providers where the organisation code on the user's smartcard matches this code.

Organisation and Sender IDs – further considerations

It is important to note that CDS SENDER IDENTITY, CDS INTERCHANGE SENDER IDENTITY and ORGANISATION CODE (CODE OF PROVIDER) may represent different organisations. For example:

NHS **Trust A** (**Rnn**) may send an interchange for CDS INTERCHANGE SENDER IDENTITY 999999999999999 which is registered for **Rnn**.

Included in their interchange may be data for CDS SENDER IDENTITY **Rnn01** which is **Trust B** that has its mental health patient records on the PAS system of **Trust A**.

It may be that **Trust B** mental healthcare is provided under a sub-contract with **Trust C** who has the Provider Code **Tnn**.

This means that:

- The data will appear on tracker for **Trust A** and failures will be reported to the registered contact for this trust.
- Data will be updated with **Trust B** code in the sender code, but **Trust B** will not receive a Managed Service Extract in their SUS Inbox.
- Records will appear in Trust C's extracts in PbR and SEM for Trust C as provider.

CDS Authentication

CDS Authentication is a validation mechanism which ensures that organisations only send data for which they are authorised. It prevents a CDS submission inadvertently deleting another organisations data and reduces the risk of data duplication for bulk update senders. Any CDS submission that does not meet authentication requirements is rejected by SUS.

Authentication Method

CDS Authentication works by checking that two identifying data items match data held from SR1 registration forms

- The CDS INTERCHANGE SENDER IDENTITY is the assigned EDI address of the physical organisation or site responsible for sending CDS data. It is a 10 character EDI address and a local 5 character tail selected by the sender.
- CDS SENDER IDENTITY is a mandatory 5-character organisation code of the organisation acting as the physical sender of the CDS.

There can be more than one CDS SENDER IDENTITY in an interchange (XML file of data) and it is usually the ODS code for the organisation. Data senders should include the site element if another organisation sends data on behalf of the site.

Where an organisation submits data on behalf of another organisation, care must be taken to ensure the correct use of these identity fields. This will avoid inadvertent duplication or deletion of records held on SUS.

To comply with CDS Authentication Each CDS SENDER IDENTITY **must be associated with only one** CDS INTERCHANGE SENDER IDENTITY**.**

Which submission method should I use?

It is currently up to each individual provider to decide which submission method to use. The use of NET Change can help to the reduce the risk of accidental deletions and record duplication, and provide greater levels of precision and control of interchanges afforded to data senders. However, BULK Update allows large amounts of data to be replaced with less preparation. A summary of advantages and disadvantages is provided below.

BULK Update

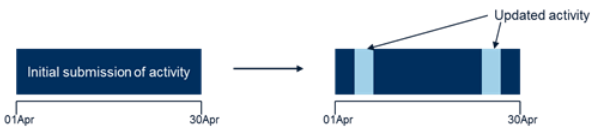
Replaces all records within a specified date range.

Advantages:

- Simplest method to submit data.
- Can quickly replace large amounts of data.
- Simpler to identify activity data set for submission.
- No need to move to new processes that support NET submission.
- Easy to delete large amounts of data.
- More suited to catering for organisations with multiple sources.

Disadvantages:

- Potential for accidental deletion of large amounts of data.
- Potential for creation of duplicate records through inadvertent misuse of update method
- Less precision. It is not possible to isolate individual historic records when updating.
- Can involve processing and submission of large numbers of records that do not need to be updated. For large organisations this can mean submitting thousands of records in BULK to update a small number of records.



NET Change

Only new records or those that need to be changed/deleted are submitted as updates.

Advantages:

- Precise control over data held at the centre for updates and record-level deletions (using 'self-delete' records).
- No risk of potential mass deletions.
- No risk of creating duplicates.
- Facilitates smaller, more frequent submissions often leading to more up to date central data.
- Can alleviate system 'bottle-necks' due to reduced processing requirements.
- Clear audit trail of interchange history.

Disadvantages:

- Initial overhead in converting business process to NET change.
- More preparation time required to determine what data needs to be submitted.
- More difficult to determine which data has changed and should be resubmitted when CDS is fed from multiple sources.
- CDS data items which NET submission relies on must be populated in line with Data Dictionary and Data Protection guidance.

Bulk Replacement Groups and CDS Type table

Supported Bulk Replacement Groups (BRG)

BRG	CDS Type(s)	Description	Activity Date Column Name
010	**120, 130, 140**	Finished Birth/General/Delivery Consultant Episodes	EP_END_DATE
020	**180, 190, 200**	Unfinished Birth/General/Delivery Consultant Episodes	EP_START_DATE
030	**160**	Other Delivery	DELIVERY_DATE
040	**150**	Other Birth	DELIVERY_DATE
050	**170**	Detained and/or Long Term Psychiatric Census	CENSUS_DATE
060	**020**	Outpatients	APPOINTMENT_DATE
070	**030**	Standard Variation of Elective Admission List End of Period Census	DECIDED_TO_ADMIT_DATE
080	**040, 050**	New and Old Variations of Elective Admission List End of Period Census	AGREEMENT_CHANGE_DATE
090	**060**	Add Variation of Elective Admission List Event During Period	DECIDED_TO_ADMIT_DATE
100	**070**	Remove Variation of Elective Admission List Event During Period	EAL_REMOVAL_DATE
110	**080**	Offer Variation of Elective Admission List Event During Period	ADMISSION_OFFERED_DATE
120	**090**	Available/Unavailable Variation of Elective Admission List Event During Period	SUSPENSION_START_DATE
130	**100, 110**	New and Old Variations of Elective Admission List Event During Period	AGREEMENT_CHANGE_DATE
140	**010**	Accident and Emergency Attendance	AE_ARRIVAL_DATE_TIME
150	**021**	Future Outpatients	APPOINTMENT_DATE

Merging Organisations

The steps outlined should be taken to ensure continuity of data flows that can be correctly attributed to the pre and post-merge organisations and to enable continuing access to data extracts.

Organisational mergers of NHS care providers do not always result in an immediate merger of IT facilities and systems to enable a single flow of CDS to SUS. During a merger transition, CDS data can flow for multiple sites from multiple senders and providers must take extra care to avoid inadvertent deletion or duplication of records in SUS.

A number of approaches can be taken but the solution will be dependent upon the range of local systems and services in use at the merging organisations, including for example:

- Patient administration systems
- A&E systems
- Maternity systems
- Critical Care systems
- CDS preparation methods
- Data warehouse set-up
- XML translation solutions
- CDS submission methods

We will focus on the issues common to all organisations, such as the use of the **organisation code** data items within the submission methods used. This will help determine an appropriate approach for the local situation.

CDS Sender Organisation Configuration

Merging organisations will each have a different

- **CDS Interchange Sender Identity,**
- **CDS Sender Identity**, and
- **Organisation Code (Code of Provider)**

Merged organisations should attempt to move to using their new Provider Codes as soon as possible after the merger date.

The new Organisation Code should be used from the point at which the merger is effective. The CDS Activity Date should determine which period the activity belongs to. For example, as the Admitted Patient Care (APC) CDS is submitted at episode level, the Provider Code in effect at episode end should be used for submission. If the change happens at year-end, data relating to that year should continue to flow from the predecessor sender using the existing Organisation Codes. Data for the next year should use the new Organisation Code.

CDS Interchange Sender Identity

CDS Interchange Sender Identity is used to identify the organisation that submits a CDS interchange. It comprises a **10 character** EDIFACT id with a **5 character** 'local tail' making a total of **15 characters**. Typically it might look like **190000099900001** where **1900000999** is the EDIFACT id and **00001** is the 'local tail'.

A new organisation can obtain a unique 10 character EDIFACT id from Addressing Registration. The remaining 5 characters are decided locally and configured within the XML translation software. It is recommended that these 5 characters are used to uniquely identify the various sending applications in use at the organisation. Each organisation is responsible for managing this themselves.

The **CDS Interchange Sender Identity** is carried in the **CDS Interchange Header** and only one can be sent per interchange.

SUS uses the **CDS Interchange Sender Identity** to sequence interchanges at the 15 character level. SUS assumes that the order received from the EDT client is the order in which interchanges should be processed. It is therefore suggested that merged organisations using a single 10 character EDIFACT code consider having different 15 character variants of **CDS Interchange Sender Identity** for each translation application to prevent any problems due to incorrect sequencing.

CDS Authentication

The **CDS Authentication** process is enabled by a table of 'allowed pairs' of **CDS Sender Identity Codes** and **CDS Interchange Sender Identity Codes**. To comply with **CDS Authentication** each **CDS Sender Identity** must be associated with only one **CDS Interchange Sender Identity**. This means that if a single XML translation application is used by a merged Provider and the pre-merge Providers submit separate interchanges, each of the Providers must use a different **CDS Sender Identity**. Interchanges that do not comply with **CDS Authentication** will be rejected.

CDS Authentication only uses the first 10 characters of the **CDS Interchange Sender Identity**. For example, 190000099900001 and 190000099900002 will be regarded as the same code.

A CDS SR1 Sender Registration Form must be submitted to the National Service Desk (NSD) to enable the relationship of these codes to be set up for the merged organisation. If data is to continue to flow from more than one **CDS Sender Identity**, this will need to be done as many times as there are flows under the new **Organisation Code** (see 'Summary of Steps').

Submission Methods

SUS will accept CDS messages in XML files provided by either NET Change or BULK update submission methods. There are a number of fields in the CDS that are used as update keys for the SUS database and these are dependent upon the method used.

How each of the merging organisations currently sends CDS is important as it will impact on the submission method chosen by the new organisation. The following submission scenario should be considered throughout this section:

Trust A (ODS code **RZA**) merges with **Trust B** (ODS code **RZB**) to become **Trust C** (new ODS code **RZC**) on 1 April

Trust A's new ODS Site code = **RZCAB**

Trust B's new ODS Site code = **RZCYZ**

Please note that the ODS codes given above are for illustration only and senders should substitute their own codes as allocated by ODS where appropriate. Note also that organisation codes are used in a number of different CDS items such as **Organisation Code (Code of Provider)** and **Site Code (of Treatment)** and the use of pre and post-merger codes in examples applies equally in whichever item an ODS code change is required.

In order to ensure that SUS will update historical data as well as new data, CDS records should always be sent using their original **CDS Sender ID** (an ODS code). If the **CDS Interchange Sender ID** (a 15-digit EDI Number) has changed the new EDI address must be registered to use the old ODS code or the interchange will fail CDS Authentication.

The provider code is not required for either submission method, but making this the same value for data from all sites will ensure correct spell construction for spells from episodes across sites.

Merging Sender Organisations Currently All Using BULK Update

Within an interchange, SUS identifies the **CDS Sender Identity**, taking all 5 characters into account.

Code Rnn is different from Rnn00 and both are different from Rnn01.

SUS then checks the **report start** and **end** date combination against the existing database.

1. If the sender has not previously sent data for the CDS REPORT PERIOD START DATE and CDS REPORT PERIOD END DATE the records will be applied to the database – even if data for the same period has been sent. E.g. if data is sent for 01 May to 31 May and then resent with an earlier extract date but for the 01 May to 30 May the interchange will be applied,

deleting later records except for the ones on 31 May.

2. If data has previously been sent for exactly the same report period **start** and **end** dates, SUS will check the CDS EXTRACT DATE and CDS EXTRACT TIME. If this date is greater than or equal to the equivalent date and time in any interchange previously applied to SUS, the interchange will be applied to the database. However, if the extract date and time is less than any interchange previously processed by SUS, the interchange will not be applied (although it will be recorded that the transaction took place). These interchanges are identified in SUS Tracker as 'Not Applied'.

When an interchange is applied to SUS, all the *matching* data is deleted between the report start and end date (where the CDS Extract Date and Time is equal to or later than the existing records in the same CDS report period). The records in the BULK interchange are then applied. *Matching* records have:

- The same **Bulk Replacement Group** (BRG)
- The same **CDS Sender Identity**
- A **CDS Activity Date** (episode end date for FCEs) between the **CDS Report Period Start** and **End** dates in the new interchange

Changing the **CDS Sender Identity** of a record can have two effects:

1. A new code that has not previously been received by SUS for the interchange report period will cause ***duplication*** of those previously submitted records of the same included Bulk Replacement Groups holding the original sender code.

2. Records with a code that has been received previously will replace those existing records in SUS for the same sender code, interchange report period and included Bulk Replacement Groups – which will not be a direct replacement of like for like records.

   Data senders with more than one data flow should take note of this consequence when merging those flows.

BULK update: Update fields used by SUS

Data Item	Format	Description
CDS INTERCHANGE SENDER IDENTITY	an15	The assigned EDI Address of the ORGANISATION or site responsible for sending the commissioning data.
CDS SENDER IDENTITY	an5	Identity of organisation acting as the sender of a CDS submission.
CDS BULK REPLACEMENT GROUP	an3	CDS Group into which CDS Types must be grouped when using BULK update.
CDS EXTRACT DATE	an10 ccyy-mm-dd	Date (with associated CDS EXTRACT TIME) of the update event (or the nearest equivalent) that resulted in the need to exchange this CDS
CDS EXTRACT TIME	HH:MM:SS	Time (with an associated CDS EXTRACT DATE) at which the CDS extract was undertaken.
CDS REPORT PERIOD START DATE	an10 ccyy-mm-dd	Start date (for the date range of the data being exchanged) for the bulk update time period.
CDS REPORT PERIOD END DATE	an10 ccyy-mm-dd	End date (for the date range of the data being exchanged) for the bulk update time period.
CDS ACTIVITY DATE	an10 ccyy-mm-dd	"CDS Originating Date" specifically identified for each CDS TYPE

It is possible to update records sent before the merger as long as the same pre-merge **CDS Sender Identity** is used. Any records migrated to a different Patient

Administration System (PAS) as the result of a merger may also be updated in SUS by using the original **CDS Sender Identity**.

To maintain Separate Multiple Data Flows

If the merging organisations intend to continue to have separate CDS submissions they should use the new organisation codes RZC where appropriate but will need to make sure they use different **CDS Sender Identities**:

Trust A, formerly **RZA**, may register as Sender Code **RZCAB**

Trust B, formerly **RZB**, may register as Sender Code **RZCYZ**

If **Trust A** and **Trust B** both use **RZC** without site suffix identifiers, this will contravene CDS Authentication.

Merging Sender Organisations Currently All Using NET Change

For NET interchange records the **CDS Sender Identity**, **CDS Unique Identifier** and **CDS Applicable Date** and **CDS Applicable Time** are checked against SUS and then applied according to CDS Type.

- For CDS Update Type = 9, if a CDS Unique Identifier is not on the database for that CDS Sender Identity, the record is added
- For CDS Update Type = 9, if one or more records are found for the same CDS Sender Identity with the same CDS Unique Identifier, it will replace them with those in the interchange where the CDS Applicable Date and Time is later than the CDS Applicable Date and Time on the existing record
- If a record with matching CDS Sender Identity and CDS Unique Identifier has previously been sent as BULK, the CDS Applicable Date and Time will be compared to the CDS Extract Date and Time on the existing record

It is possible to send a NET delete record, CDS Update Type = 1. This can be thought of as a 'self-delete' record where all records it finds a match with (i.e. the same CDS Sender Identity and Unique CDS Identifier) will be deleted (marked on the database as logically deleted) and the NET delete record will then delete itself.

NET change – update fields used by SUS

Data Item	Format	Description
CDS INTERCHANGE SENDER IDENTITY	an15	The assigned EDI Address of the ORGANISATION or site responsible for sending Commissioning data.
CDS SENDER IDENTITY	an5	The identity of the organisation acting as the Sender of a CDS submission and is represented by that organisation's code
CDS UNIQUE IDENTIFIER	an35	A CDS data element providing a unique identity for the life-time of an episode carried in a CDS message.
CDS APPLICABLE DATE	CCYY-MM-DD	The date (with an associated CDS APPLICABLE TIME of the update event (or the nearest equivalent) that resulted in the need to exchange this CDS.
CDS APPLICABLE TIME	HH:MM:SS	The time (with an associated CDS APPLICABLE DATE of the update event (or the nearest equivalent) that resulted in the need to exchange this CDS.
CDS UPDATE TYPE	an1	9 for insert or update, 1 for a delete
CDS TYPE	n3	The code to identify the specific type of Commissioning Data Set data

Certain CDS types allow NET change to update/delete an existing record containing a different CDS type. These are listed in the table below:

Incoming CDS Type	Existing CDS Types that incoming CDS type will overwrite
120	120, 180
130	130,140,190,200
140	130,140,190,200
180	120, 180
190	130,140,190,200
200	130,140,190,200

For all other CDS types (listed below) NET change will only update/delete an existing record containing the same CDS type:

Incoming CDS Type:010

020, 021, 030, 040, 050, 060, 070, 080, 090, 100, 110, 150, 160, 170, 210

To maintain Separate Multiple Data Flows

- Records to be updated must be sent with their original **CDS Sender Identity**
- CDS Unique Identities must remain the same through every version of the individual CDS record

If the merging organisations intend to continue with separate CDS submissions they will need to ensure the **CDS Unique Identifier** is unique across the new organisation. System suppliers should be able to provide details on the method of generating this data item and further details can be found on the NHS Data Dictionary.

CDS Unique Identifier is applied at the event record level. This means each episode in an APC CDS should have a different value, as should each Outpatient or A&E attendance.

If there is replication of **CDS Unique Identifiers** then this should be resolved before the merger date. This is illustrated in the following example:

If two merging organisations use the same PAS supplier they should follow NHS Data Dictionary guidance in the construction of the **CDS Unique Identifier**. This stipulates that a trust specific element is used.

Two different patients with the same PAS identifier number (e.g. patient master index entry number), 0123456 and same chronological event on each PAS (e.g. first APC episode in first non-elective spell on system) may be identified in a CDS extracted separately from each PAS as ***BRZAAB0123456_1_1*** and ***BRZBYZ0123456_1_1***.

If both appear in their respective CDS extracts as ***0123456_1_1*** local processing should add the trust prefixes before sending to SUS. It is possible to send data using a single CDS flow before a PAS merger takes place, so this action will enable an easier transition to a future single CDS flow.

It is recommended that the merging organisations do not move to using the new organisation code ***RZC*** in the prefix until any PAS merger takes place, even if a single CDS flow is adopted. The merging organisations should however use the new organisation codes **RZC** where appropriate for provider or site code but will need to make sure that they use different **CDS Sender Identities**:

Trust A, formerly **RZA**, may register as Sender Code **RZCAB**

Trust B, formerly **RZB**, may register as Sender Code **RZCYZ**

If **Trust A** and **Trust B** both use **RZC** without site suffix identifiers, this will contravene CDS Authentication.

To initiate and use Single Combined Data Flow:

Once the decision has been taken to move to a single combined CDS flow it is important that the Sender code in all CDS is populated with the new organisation

code of **RZC** and site code fields with the appropriate ODS registered new site code.

To prepare SUS to receive data as a single NET CDS, the following actions should be taken:

- **DELETE** existing records with the old ODS codes by submitting a NET delete using **CDS Unique Identifier** with their original **ODS Sender Code**.
- **RESUBMIT** historic records with activity from the date of the merger with their new **CDS Unique Identifier** and with the new **RZC** sender code. These could be sent from an existing EDI address or from a new EDI Address specific to the merged organisation as long as either is authenticated to send **RZC** records.

These actions will:

- replace data that relates to activity subsequent to the merger but which carries codes for the pre-merge organisations
- provide data that holds the correct organisation codes at a given point in time
- allow all data for the new organisation to be updated or replaced as part of local business as usual processes for the single combined data flow

Trusts using or planning to use NET change should be careful to manage changeover to a single PAS as they will need to ensure that previously generated **CDS Unique Identifiers** are not reused for different records.

Merging Sender Organisations using a combination of NET and BULK

This situation would typically occur where merging trusts separately employ different methods for their SUS submissions.

To extend the previous example, Trust A (RZA) is a NET sender; Trust B (RZB) uses BULK.

Risks Associated with Mixing Update methods for the Same Organisation

It is possible for senders to use NET change and BULK update according to which method is most suited for the interchange and CDS type they are sending to SUS. However, mixing NET and BULK for the same CDS Types is not recommended and carries associated risks.

- NET will replace all the records with the same **CDS Unique Identifier** for the sender providing the Applicable Date is equal to or later than the previous record(s) Extract Date. It is possible to send a BULK interchange with many records with the same **CDS Unique Identifier** for the same sender, thus if all the records in a BULK interchange have the same **CDS Unique Identifier** and a subsequent NET change delete record is sent with that **CDS Unique Identifier**, it follows that all the BULK records will be deleted.
- NET change cannot identify records without a **CDS Unique Identifier**; therefore it cannot be used to replace BULK records that have been submitted without a **CDS Unique Identifier**. This could result in BULK records effectively being duplicated, with one version with a **CDS Unique Identifier** and one without.
- BULK will update all NET records for the **CDS Sender Identity**, **CDS Report Period Start** and **End Date** combinations irrespective of Extract Dates and Applicable Dates. This will also happen regardless of the contents of the **CDS Unique Identifier** field.

  For example, if a provider were to submit APC General Episodes (CDS type 130) on a regular basis using NET and then submit APC Delivery Episodes (CDS type 140) data using BULK, the BULK maternity submission will overwrite all existing NET APC records within the BULK report period submitted for all sender/recipient pairs found.

The above highlights the two main risks of mixing NET and BULK:

- **A BULK submission will delete all NET submissions, irrespective of applicable date.**

- **If BULK has not used a CDS Unique Identifier, multiple records can be replaced by a single NET record.**

To maintain Separate Multiple Data Flows:

Where separate data flows are maintained organisations need to ensure that the CDS

Unique Identifier is unique across the new organisation by checking with system suppliers that no records on any local system have the same value in this field. Both NET and NULK submissions from the merged organisations should carry this data item. This will support any eventual merger onto a single system.

The merging organisations should use the new organisation codes **RZC** where appropriate but will need to make sure that they use different CDS Sender Identities:

Trust A, formerly **RZA**, may register as Sender Code **RZCAB**

Trust B, formerly **RZB**, may register as Sender Code **RZCYZ**

If **Trust A** and **Trust B** both use **RZC** without site suffix identifiers, this will contravene CDS Authentication.

To initiate and use Single Combined Data Flow

Once the decision has been taken to move to a single combined CDS flow it is important that the sender code in all CDS is populated with the new organisation code of **RZC** and site code fields with the appropriate new ODS registered site code.

Patients in Hospital at the Time of the Merger

Guidance on when **Hospital Provider Spells** should be closed and reopened, including the associated administrative codes to record for the discharge and admission events generated, can be found on the NHS Data Dictionary.

The merge process involves the closing and opening of organisations so patients in hospital must be discharged from the closing organisation on the merge date and immediately admitted by the successor organisation.

The organisation codes where each spell closes should be used to submit the related APC CDS. This will register where the activity took place at the correct point in time.

The impact of this will be to inflate the number of admissions and discharges across all NHS organisations, but will not affect counts for the individual constituents.

In this situation, SUS PbR and the HRG grouper will regard activity at each provider organisation as separate spells. Spell construction will therefore be affected by the merger and agreements should be made to avoid double-payment for the affected spells. This may include a one-off regrouping exercise using the actual admission and discharge dates and one set of provider codes to determine the appropriate tariff.

Reopened spells will have an admission method of '81' (non-emergency transfer) and an admission source of '51,'52' or '53' (hospital ward) and will not count as a readmission.

Demergers

When organisations separate they may or may not revert to their pre-merge organisation codes depending on the new configuration of services. Advice on which codes to use should be sought from the Organisation Data Service (ODS).

Much of the guidance applicable to mergers is equally valid for demergers in that each organisation resulting from the split should be regarded as a new sender in relation to SUS. The same steps will need to be completed and particular attention should be given to ensuring that activity is attributed to the correct provider at the correct point in time.

Commissioning Organisations Separating Provider and Commissioner Functions

Until such time as the provider function becomes a separate statutory body either in its own right or as the result of a merger with another provider organisation, both parts of such an organisation will use the same organisation code. It may be appropriate to introduce local procedures to limit the access to data held on SUS of

individual staff working in the different functions of such organisations.

Access to SUS Extracts

In order to maintain access to extracts for pre and post-merger organisations, it is necessary for the new organisation code to be added to existing Smartcards. Existing RBAC functionality should remain against pre-merge organisation codes and be copied against the new code.

The ODS team can transfer existing users across to the new organisation using the Organisation Migration Service (OMS). The reconfiguration lead in your organisation should have this scheduled as part of the wider reconfiguration plan.

Summary of Steps

At the discretion of the organisations concerned, some of the planning for these steps can be undertaken before the merge takes place.

After registration of the new organisation with ODS, in order to successfully submit data to SUS and maintain access to SUS extracts, the following steps need to be completed:

Step 1: Review and decide submission configuration

Merging organisations should review their current sending configuration in terms of internal data flows, number of XML translation applications and CDS Interchange Sender and Sender Identity codes in use.

The decision to consolidate flows does not need to be made straight away, and it may not be appropriate for this to occur, but to comply with CDS Authentication, individual sites and systems within the new organisation must use unique **CDS Interchange Sender Identity** and **CDS Sender Identity** combinations. The new organisation must therefore make use of the relevant ODS site codes as the CDS Sender Identities to differentiate multiple CDS data flows for the same provider by using the last 2 digits of the Organisation Code.

Step 2: Register for CDS Authentication

Complete a CDS SR1 Sender Registration form and submit to NSD.

Step 3: Enable CDS Authentication and access to extracts

NHS Digital to update:

- Organisation code and parent-child mapping tables to ensure staff can access new and historic data for the organisation.
- CDS Authentication table with new unique legitimate relationships between CDS Interchange Sender and the CDS Sender

NSD will notify the end user when this process is complete.

Step 4: Local update of smartcards

The local Registration Agent (RA) must ensure all smartcards have access profiles granted against the new organisation. The ODS Organisation Migration Service (OMS) can help if necessary.

Step 5: Review and decide submission strategy

The merged organisation should review the manner in which it sends data to SUS in terms of the submission method used and whether it is appropriate to consolidate flows. This decision may influence **Step 1** but may be deferred until such time as any merger of supporting systems such as PAS has taken place. The submission strategy should support data flows so that data from different sources does not conflict to cause either duplication or inadvertent deletion of SUS data.

Step 6: Update SUS to create correct point in time position

It is essential that data held on SUS represents the correct position of all organisations pre and post-merger. This step should include resubmitting data with the new organisation code for activity relating to the post-merge period.

Merger Checklist

The following Merger Checklist summarises the tasks that merging organisations should complete in order to maintain CDS flows and access to SUS data extracts.

- Obtain new organisation code from Organisation Data Service (ODS)
- Update smartcards
    - New organisation codes must be added to cards
    - May need to contact Organisation Migration Service (OMS)
- Review current submission configuration
    - Single or Multiple XML translation applications
- Implement new submission configuration
    - May need to obtain new EDI address(es) from Addressing Registration
    - May need contact with current XML translation supplier(s)
    - Register new sender codes using SR1 form to comply with CDS Authentication
- Update SUS data to represent correct point in time position for pre and post-merge organisations
- Notify NHS Digital that data from merged organisations will be flowing under new codes
- Review current submission strategy across new organisation
    - All BULK/All NET/Combination of BULK and NET
    - May need to check uniqueness of CDS Unique Identifier across existing PAS applications or data warehouses within new organisation
- Implement new submission strategy if different
    - May need to prepare SUS to update historical records using NET by resubmitting data with appropriate CDS Unique Identifier

The main stages in this checklist are equally applicable to organisations separating as part of a demerger.

-

Appendix A – Fields that Contain Patient Confidential Data (PCD)

- NHS Number
- Local Patient ID
- ALL VGP (very general purpose) fields
- Name
- Patient Usual Address
- Postcode of Usual Address
- Date of Birth
- Hospital Spell Number
- Local CCMDS ID
- Mothers details (on birth CDS):
    - Local Patient ID (Mother)
    - NHS Number (Mother)
    - Birth Date (Mother)
    - Patient Usual Address (Mother)
    - Postcode of Usual Address (Mother)
- Babies details (for all babies on delivery CDS):
    - Local Patient ID (Baby)
    - NHS Number (Baby) Birth Date (Baby)
- Patient Pathway Identifier
- UBRN Converted

Appendix B – Interchange Feedback Report

The Interchange Feedback report is requested via the SR1 form completed when providers register to send data to SUS. The SR1 form can be amended at any time to add or delete email addresses to which the report should be sent.

As well as details related to the success or failure to process an interchange the report also includes summary details of any potentially inappropriate use of PCD identified in the interchange.

The report contains summary details only as the distribution of the report is not sufficiently controlled to support the inclusion of PCD data.

The report shows:

- The total number of records in the interchange that contain one or more instances of misuse of PCD
- The total number of records that contain one or more instances of misuse of PCD for each provider with data in the interchange
- For each combination of Provider, PCD Field and Inappropriate field the:
    - Provider
    - PCD Field
    - Inappropriate Field
    - Total count of records
    - Up to three record identifiers

The record identifiers provided will be either the CDS Unique Id or the Generated Record Id.

- The CDS Unique Id is the preferred identifier and where the CDS Unique Id does not contain PCD that is the identifier provided.
- Where the CDS Unique Id cannot be provided the SUS Generated Record id is provided. If the Generated Record Id is provided it will be preceded with “**” to denote that it is the Generated Record Id.

An example of the output is:

```
Failure reasons:
  - 15: Total number of CDS records containing the instances of PCD value found in non-
PCD/candidate field(s)
  - [(Provider Code, Invalid Record Count)]: [('QQQ', 8), ('FFF', 7)]
  - [(Provider Code, PCD Field, CDS Attribute containing PCD Field value, Invalid Record
Count, CDS Unique Identifier/Generated Record ID**)]: [('QQQ', 'nhs_number',
'patient_pathway_id', 8, [710000000000000000000000000254681894, **1445354770999999999]),
('FFF', 'local_patient_identifier', 'ambulance_incident_number', 5,
[710000000000000000000000000254681895, 771000000000000000000000000254681945]),('FFF',
'spell_number', 'patient_pathway_id', 2, [**1445354770999999996, **1445354770999999997])
```

*Note: This example includes identifiers for two records, the actual report will show upto three

For further information:

www.digital.nhs.uk

0845 300 6016

enquiries@nhsdigital.nhs.uk