|  |  |
| --- | --- |
|  | **SOP Title:** Data Transfer |
| **Study title:** *Give study title to which this SOP applies* |

1. **Scope and application**

|  |
| --- |
| The purpose of this Standard Operating Procedure (SOP) is to define the principles and practices of data transfer between internal/external parties and between any two systems or locations. Both electronic and paper are considered in this SOP. The transfer of data (including personal data) from any clinical research study must comply with the principles of Good Clinical Practice (GCP) and personal privacy laws as applicable.  |

1. **Responsibilities**

|  |  |
| --- | --- |
| **Function** | **Activities** |
| Data Manager | * Responsible for approving all in scope data transfers prior to the transfer.
* Approve the Data Transfer Plan
 |
| Sender of data | * Complete and sign the Data Transfer Plan
* Make sure that any additional data, needed to understand the data, is attached (i.e. data dictionary)
 |
| Recipient of data | * Sign the Data Transfer Plan
 |

1. **Definitions**

**CDASH**: Clinical Data Acquisition Standards Harmonization

**CDMS**: Clinical Data Management Software

**Data Conversion**: converted data from one format to another

**DTL**: Data Transfer Log

**DTP**: Data Transfer Plan

**GCP**: Good Clinical Practice

**SDTM**: Study Data Tabulation Model

**QC**: Quality Check

# Procedures

* 1. **Types of Data Transfer**

There are two aspects to a data transfer.

* Movement between two geographical locations or organisations
* Conversion between data formats or systems
	1. **Methods of Transfer**

The agreed method of transfer must be one of the following:

* Via the internet using web-based secure data transfer tools e.g. OneDrive, REDCap SendIt, WeTransfer, etc.
* Encrypted removable storage devices
* Encrypted email/WinZip encrypted attachment
	1. **Planning**

All data transfers between locations must be planned in advance using the Data Transfer Plan (DTP) (see Attachment 01). The DTP details the plan to carry out the transfer and will include the following:

* The person responsible for preparing and sending the data
* The person responsible for receiving the data
* The format(s) of the data
* The method of transfer
* The security measures that will be implemented
* The Quality Control procedure that will be used
* The frequency of the transfer – for instance, a one-off, on demand or a regular transfer at set intervals.

**Note:** The DTP is also used for the first transfer i.e. Transfer No. 1. Subsequent transfers i.e. Transfer No. 2 onwards for the same transfer should be captured on the Data Transfer Log (DTL) (see Attachment 02) ensuring to use the correct study and/or system name. Both the sender and recipient will sign-off on the plan, and the Data Management Lead will approve.

* 1. **Data Format**
* The data needs to be formatted in a way that will be understood by the recipient person or system. The data dictionary must be sent along to enable interpretation of coded values and variable names.
* If an industry standard data format is available for a particular data type then this format should be used by default e.g. CDASH, SDTM, etc.
* If the data is to be loaded into a system on arrival, then a test data transfer of a sample extract should be sent in advance to confirm the format will work with the destination system.
	1. **Security Measures**
* If the data transfer is indirect – i.e. the data will be handled by a third-party organization or system e.g., then the data must be password-protected using an agreed method.
* The sender should list all Security measures in the DTP.
	1. **Quality Control (QC)**
* The QC process gives a reasonable level of confidence that the data sent is complete and undamaged when received.
* For all data movements, use the Transfer Form to indicate the Transfer Number and the relevant details such as file names, file sizes, and descriptions. A description of any codes used in the data i.e. data dictionary, should also be included where appropriate.
* If the transfer also includes a conversion of file formats, then also carry out the steps required in section 4.8.
* The sender should list all Quality Control measures in the DTP.
	1. **Data Transfer Records**
* A log of all data transfers being sent out or received will be retained as a record. This may be in the form of files stored in a secured project workspace under a folder e.g. Transfer 1, Transfer 2, etc. or transfer log files from specific file transfer tools, using Attachment 02. A copy of all files sent in the data transfer will also be retained so that they can be checked to answer any questions from the recipient.
* At the time of transfer, place a copy of the entire transfer, exactly as sent or received – including any covering letter or email – in a Data Transfer Log folder in the project workspace.
* Data transfers will be retained for a minimum of 2 years from date of transfer.
	1. **Data Conversions**
* For data conversions, the 4-point QC check is required (in addition to any other required QC).
* The 4-Point check: For each data file
1. The number of records in the file,
2. A listing of the first record of data,
3. A listing of the last record of data,
4. For each data file, the sum of all the values in one column of numeric data or, if there are no suitable numeric fields, a frequency count of values in a categorical field e.g. no. of males/ females
* Run the check on the source data in the source system, carry out all steps of the conversion (print the output), then run the check again on the same data in the destination system (print the output). Confirm that all the results are the same in both systems. Sign and date the printed output and retain as a record.
* If the data transfer is indirect – i.e. the data will be handled by a third-party organisation or system e.g. email or courier, then the data must be password-protected using an agreed method.
	1. **Data with identifiers**
* The transfer of personal data is covered by the applicable regulations geographically; therefore, appropriate consent must be obtained or the data should meet the relevant exemption criteria and have appropriate permissions and agreements (as per SOP-WP3-15-Data Sharing) in place before any data transfer takes place.
* Confidentiality must be maintained at all times. Direct identifiers (e.g. study participant name, address, phone number…) should always be kept secure at site and separate from the main research data. Consideration should also be given to identifying what data should be pseudonymized or anonymized and how this is to be done, prior to any data being transferred.

# Attachments

|  |
| --- |
| **Attachments** |
| **Number** | **Title** |
| 01 | Data Transfer Plan (DTP) |
| 02 | Data Transfer Log (DTL) |
|  |  |

# Document History & References

|  |
| --- |
| **Revision**  |
| **Version number** | **Author** | **Date** | **Description/reason for modification** |
| 1.0 | Yusupha NjieFatoumatta Cole | 04/10/2019 | Initial versionReview by Hanne LanduytApproval by Bai Lamin Dondeh and Harry Van Loen |
| 2.0 | Fatoumatta Cole | 23/06/2022 | Review to ensure that the SOP is appropriate within ALERRT and with current clinical research best practices. |

# Approval

|  |  |  |
| --- | --- | --- |
| **Name and function** | **Date (dd/mm/yyyy)** | **Signature** |
| ***Author*** |
| *Indicate who wrote the SOP* |  |  |
| ***Review*** |
| *Indicate WP team members who reviewed (if applicable)* | *Date of review* |  |
| ***Approval*** |
| *Indicate WP Lead/Co-lead(s) who approved* | *Date of approval* |  |