



PaCCSC
Palliative Care Clinical Studies Collaborative

Standard Operating Procedures

5.5.2 Electronic Data Transfer ©2007

History			
Version	Date	Author	Reason
1.1	18 th July 2007	B Fazekas	New procedure
1.2	18 th August 2007	B Fazekas	Changes ratified by MAB
1.3	16 th October 2007	B Fazekas	Update after David Currow review

Approval				
Version	Author	Signature	Approval Name	Approval Signature
1.3	B Fazekas	<i>B. Fazekas</i>	D Currow (CI)	<i>D. Currow</i>

Scheduled review

Date August 2009

Responsible person PaCCSC Project Officer

5.5.2 Electronic Data Transfer

Purpose

Data for clinical studies may need to be stored, checked and managed in a separate location from where the data will be monitored or analysed. Studies need to ensure that the data are transferred from one person and location to another in a safe and secure way that will maintain data integrity and participant anonymity and in a timely manner.

This SOP describes the procedure for data transfer for data generated within PaCCSC. In most cases this data transfer occurs when the study statistician needs to check allocation codes against study data (for data safety monitoring) or for study analysis (interim or final). Others may need access to the study data at various times throughout the study, this will always be approved by the lead investigator in the first instance.

Other related SOPs

Essential Documents
Electronic Data Handling

Attachments

File Notes

Other files that apply

References

Note for Guidance on Good Clinical Practice (CPMP/ICH/135/95). Annotated with TGA comments 2000 (accessed 250207)
<http://www.tga.gov.au/docs/pdf/euguide/ich/ich13595.pdf>

Procedure

Data download

This procedure is undertaken by the Project Officer at the Coordinating agency, and downloaded onto this person's computer and their personal password protected network drive, which is backed up to tape each evening.

Data are downloaded each month (see Electronic Data Handling) for back-up. On each occurrence the following procedure is followed;

1. The data are tagged for export from the website
2. The following download options are ticked
 - a. Detailed response information (dates and times of data entry – this is a data tracking process for initial entry and any subsequent change)
 - b. Detailed user information (Names and IP address of person entering data)
 - c. Export open ended results (text items are exported)
 - d. Export with aliases (The coded question and responses are exported, ie, 1 = yes)
3. Data download is saved to password protected PC as a CSV text file with file name indicating CRF name and date.
4. CSV file is viewed for completeness and gross validation. This is not data checking (see Electronic data Handling SOP) but a check to see that all data fields have been downloaded in a complete and consistent manner.

Data safety

This procedure is undertaken when there has been a specific request for data who is external to where the data are held.

1. The CSV file is “zipped” into a password-protected Winzip file that includes 128-bit secure encryption. The data file is sent via email to the responsible party (this may be the coordinating site, lead investigator or lead statistician depending on the data and the request).
2. The password to open the zipped data file is forwarded to the responsible party separately via telephone.
3. The responsible party opens the encrypted data file using the password and imports the data into an appropriate statistics programme using the import function
4. Field and data codes are entered as per the study data dictionary in order to facilitate analysis.
5. The main study data are merged with the table of allocation codes by the responsible party. This will only take place in the following situations:
 - a. For unmasked data analysis as requested by the Data Safety Monitoring Board (DSMB);
 - b. At the completion of study accrual to facilitate all study analyses.

File Notes

File notes are to be used when errors or alterations are made to data not already documented via the Data Report Forms. This may be when ID numbers have been altered on email instruction from sites, where errors are made in recording randomisation codes, or where errors are recorded during monitoring and audit procedures.

Sample Only



File Note

Purpose

File notes are to ensure that any changes to participant files or actions taken are documented and are able to be authenticated by any member of the study team and monitors.

Any changes to data and study related documentation that does not have an associated file note is subject to suspicion and doubt, leading to possible exclusion of the participants data from the analysis.

Complete one of these forms for each and every change made to the recording of data that does not have a data query form.

Instructions

All of the following sections are to be completed by the person who made the change or another who can authenticate the change. The original is to be stored at the site of origin, a copy is to be forwarded to the Coordinating Agency for filing.

Note:

The reason for the error or the change. An explanation as to why the information was altered or incorrect.

Date of change:

The Date the information was changed or corrected

Changed from:

Original entry

Changed to:

The new entry

Changed by:

Name of person who made the change or corrected the error, or reported the inconsistency

Date of File note:

[Date this page is completed and signed]

Signature of person completing file note.