

SOP 840 Clinical Data Management System DATA MANAGEMENT AND SECURITY

| | |
|---|--|
| For Use in: | Research |
| By: | All staff |
| For: | All staff involved in the conduct of research |
| Division responsible for document: | Research & Development |
| Key words: | CDMS, Data Management Security |
| Name of document author: | Martin Pond |
| Job title of document author: | Head of Data Management, Norwich Clinical Trials Unit, UEA |
| Name of document author's Line Manager: | Matt Hammond |
| Job title of author's Line Manager: | Deputy Director of the Norwich Clinical Trials Unit |
| Supported by: | Julie Dawson NNUH Sarah Ruthven UEA NNUH Digital Health |
| Assessed and approved by: | Julie Dawson: Research Services Manager NNUH Sarah Ruthven: Research Manager UEA |
| Date of approval: | 21/09/2023 |
| To be reviewed before: This document remains current after this date but will be under review | 21/09/2026 (3 years, unless legislation or process changes) |
| Reference and / or Trust Docs ID No: | 14284 |
| Version No: | 4 |

Version and Document Control:

| Version No: | Date of update | QPulse Change Request reference (CR no.) | Change Description | Author |
|-------------|----------------|--|--------------------|-------------|
| 3 | September 2023 | - | New template | Martin Pond |

This Standard Operating Procedure (SOP) is available on the Research & Development pages on the NNUH website

Copies downloaded from the website are only valid on the day of downloading.

SOP 840 Clinical Data Management System: DATA MANAGEMENT AND SECURITY

1. Contents

| Section | Page |
|---|------|
| 1. Contents | 2 |
| 2. Definitions of Terms Used / Glossary | 2 |
| 3. Objectives | 2 |
| 4. Scope | 2 |
| 5. Purpose | 3 |
| 6. Rules | 3 |
| 7. Procedure | 3 |
| 7.1 Access via the user interface | 3 |
| 7.2 Direct access to the database | 4 |
| 7.3 Access to the servers | 4 |
| 7.4 Managing exported data | 4 |
| 7.5 Backup and restore | 4 |
| 8. Encryption | 5 |
| 9. Audit Trail | 5 |
| 10. References and Related Documents | 5 |
| 11. Approval | 6 |
| 12. Training Implication | 6 |

2. Definitions of Terms Used / Glossary

| | |
|------|--|
| CDMS | Clinical Data Management System |
| CTU | Clinical Trials Unit |
| GCP | Good Clinical Practice |
| ICH | ICH International Conference for Harmonisation |
| ITCS | Information Technology Corporate Systems |
| NNUH | Norfolk and Norwich University Hospital |
| R&D | Research and Development |
| SOP | Standard Operating Procedure |
| SU | Service User |
| UEA | University of East Anglia |

3. Objectives

The aim of appropriate management and security of data is to ensure that data is available only to those entitled to use it, protected from unauthorised or accidental access or modification and that there are appropriate copies of the data.

4. Scope

Clinical data management systems reside either on the UEA or NNUH network and are subject to the following institution-wide policies:

SOP 840 Clinical Data Management System: DATA MANAGEMENT AND SECURITY

- UEA High Level Information Security Policy
- UEA General Information Security Policy
- UEA Desktop Computer Procurement and Deployment Policy
- NNUH IT Security Policies

5. Purpose

This SOP describes the steps that are taken to ensure that trial data is:

- Available to those that are entitled to use it
- Protected from unauthorised or accidental access and modification; and that
- Previous copies of the data are available and restorable

6. Rules

ACCESS TO DATA

Most data management systems designed for clinical trials are in two parts:

- The user interface
- The database

The user interface provides Service Users (SU) with access to the database. Under normal circumstances SUs will not have direct access to the database.

Studies without Norwich CTU Support

The use of Microsoft Access at the NNUH is not supported by the Digital Health team, where possible the NNUH Digital Health team suggest the use of Microsoft SQL database technologies.

7. Procedures

7.1 Access via the user interface



- The user interface is programmed such that users must always log in with a **username** and **password** to gain access to trial data.



- In some trials, there is a requirement to restrict each user's access to data to a subset of the whole dataset (multi-centre trials)
- Access restrictions such as these must be listed in the **Functional Specification** and they will be included in any system tests.

SOP 840 Clinical Data Management System: DATA MANAGEMENT AND SECURITY



- Users must always be granted the **lowest** level of access to data that enables them to perform their job.

7.2 Direct access to the database



- For studies built in REDCap no one outside the data management team has direct access to the database



- Where users of underlying databases require access to the raw data to write their own queries etc. (e.g. from MS Access or SAS), read-only access can be provided.
- This allows read-only access to the data and does not give direct access to update the underlying database.



- Read-only access to the live database must only be made available to users on the UEA network or with access via a secure remote link such as VPN.



- Any direct access to the database shall be restricted to the data that the requester needs to see.
- Particular attention must be paid to prevent the unblinding of a user who should remain blinded

7.3 Access to the servers

Login access to the server where the underlying database resides is restricted to:

- Database Management Team
- IT Services staff at UEA

7.4 Managing exported data

Data can also be provided to users by exporting data sets from the database. Any datasets containing randomisation data or patient identifying data, and any datasets that are being dispatched outside the UEA network **must** be encrypted before transmission to the requester.

7.5 Backup and restore



- Databases are automatically backed up daily by the IT departments at the UEA and NNUH.
- Restoration is by request to the appropriate IT team.

SOP 840 Clinical Data Management System: DATA MANAGEMENT AND SECURITY



- MySQL and SQL databases are backed up daily (Full Backup). In addition to being taken 'off-line' the MySQL backups are left 'on-line' for 7 days and the SQL backups are left 'on-line' for 3 days both in a designated folder on the server.
- SQL server databases are each backed up daily (Full Backup).



- Copies of the *backup* folder are taken offline daily using a procedure provided by UEA's ITCS department.
- The files are stored offsite at a location approved by UEA external auditors.



- On a regular basis, the Data Manager **must** request a random backup from the last 3 months, restore it to a new location and check that the contents are readable.

8. Encryption

Websites on the Norwich CTU server are set up so that web traffic between users and the database is encrypted using SSL.

9. Audit Trail

CDMS are built with a special facility that keeps an audit trail of:

- All data changes made
- When the change was made
- Who made the change

10. References and Related Documents

References

UEA High Level Information Security Policy

UEA General Information Security Policy

UEA Desktop Computer Procurement and Deployment Policy

NNUH IT Security Policies – Available from Trust Docs

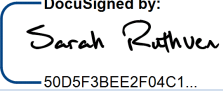
SOP No.

SOP Title

SOP 825

Clinical Data Management System - VALIDATION

SOP 840 Clinical Data Management System: DATA MANAGEMENT AND SECURITY**11. Approval**

| | |
|---------------------------------------|--|
| Author | Martin Pond |
| Role | Head of Data Management, Norwich Clinical Trials Unit, UEA |
| Approved & Authorised NNUH | Julie Dawson |
| Role | Research Services Manager |
| Signature |  <small>4CBAB366CF354A2...</small> |
| Date | 21 September 2023 12:26 BST |
| Approved & Authorised UEA | Sarah Ruthven |
| Role | Research Manager |
| Signature |  <small>50D5F3BEE2F04C1...</small> |
| Date | 21 September 2023 3:52 BST |

12. Training Implication

| | |
|-----------------------------|--|
| Training Implication | |
| Actions required | <ul style="list-style-type: none"> • Review SOP |