




SOP 003_05

Title	Database Maintenance and Management
SOP Code	SOP 003_05
Effective Date	30-June-2023

Site Approval/Authorization to Adopt

Name and Title of Local Personnel (Type or print)	Signature	Date dd/Mon/yyyy
Neelu Sehgal Director, Interprofessional Practice & Research Chief Nursing Executive, Erie Shores Health Care		
Dr. Munira Sultana Office of Research, Erie Shores Health Care		23/06/2023



SOP 003_05

1.0 PURPOSE

This Standard Operating Procedure (SOP) describes the management and maintenance of the study database from database launch until database lock to ensure accurate, reliable, complete, and secure electronic data.

2.0 SCOPE

This SOP is applicable to all studies databases managed at the site (Erie Shores Health Care) and to those personnel responsible for management and maintenance of studies databases, unless otherwise stated in the study contract or Data Management Plan.

3.0 RESPONSIBILITIES

The Sponsor-Investigator or Qualified Investigator (QI)/Investigator, Data Management personnel and IT Systems Support personnel (when applicable) are responsible for ensuring that the processes involved in all database maintenance and management meet all the applicable regulatory, International Conference on Harmonization (ICH) Good Clinical Practice (GCP), Sponsor and local requirements.

Any or all parts of this procedure may be delegated to appropriately trained study team members, but remain the ultimate responsibility of the Sponsor, Sponsor-Investigator and/or Qualified Investigator (QI)/Investigator.

4.0 DEFINITIONS

Computer system: The term computer system applies to the set of computer hardware or other similar device by or in which data are recorded or stored and any procedures related to the recording or storage of the study database. For example, a computer system may be a mainframe, server, virtual server, workstation, personal computer, portable device or a system of computers arranged as a network.

Database: The term database applies to all computer software which is used to format, manipulate or control storage of the electronic data for the study. This may be one computer file or a system of files which are maintained as the study database.

Study Database Manual: The repository of information concerning the study data base. User Acceptance Testing (UAT): A formal means by which one verifies that the system meets the required business functions by emulating normal use conditions.

See also, "CDISC Clinical Research Glossary, Version 8.0" and "N2 Glossary of Terms".

5.0 PROCEDURE

5.1 Documentation

5.1.1. All documentation and record keeping described in the following sections must be maintained as part of the study database manual.

5.2. Change Control

5.2.1. Clearly document all software information (software name, vendor name, release/version, patches) and the database configuration. Keep track of all changes and upgrades.

5.2.2. Clearly document all hardware information (server, network share, etc) and the hardware configuration on which the database resides. Keep track of all changes and upgrades.

5.2.3. Create and maintain a list of users who have access to the database. If there is restricted access to the database, keep track of the access privileges of all users.

5.2.4. Maintain training logs for data management personnel and for end-users of the database.

5.2.5. When changes are made to the database structure, follow the relevant steps in the site's database set-up procedures. These steps include, but are not limited to:

- Update the requirements for data transfers and integration with other systems.
- Update the data entry screens.
- Update edit check programs and validation rules.
- Perform UAT of the changes.
- Notify and train end users as necessary.
- Update the study database manual.

5.3. Data Auditing

5.3.1. Where possible, establish an electronic audit trail of all modifications and of additions to and deletions of entered data. Where an electronic audit trail is not possible, a paper trail documenting all modifications, deletions and additions must be maintained, including the date and time, the reason for change and initials of the person making the change.

5.3.2. When data is directly entered into an eCRF, and there is no paper record, the audit trails must be computer-generated and time-stamped and must contain:

- The date and time of the change, addition or deletion.
- The user making the change, addition or deletion.
- The reason for the change, addition or deletion.

- The old value.
- The new value.

5.3.3. Data modifications, deletions and additions requested after database lock and which are outside of the audit trail capability must be clearly documented.

5.3.4. Where possible, an archive of the database before modification should be maintained so that it is possible to track the changes electronically.

5.4. Database Security

5.4.1. If the database is located on a networked share drive, ensure limited access to the database using network accounts or database access accounts.

5.4.2. Ensure the computer system housing the database is protected with the latest antivirus and anti-spyware software and that it is in a secure location preferably with limited physical access and protected from fire and water damage.

5.4.3. Create, maintain and document a data loss protection (DLP) process for the database. Database backup and recovery must be periodically tested.

5.5. Interim Release of Data

5.5.1. Ensure privacy legislation provisions (local, provincial, national, and international as applicable to the study) are met within the database for identifiable data (including coded data).

5.5.2. Refer to your local requirements for the release of data. Maintain appropriate documentation and authorizations for access to the requested data.

5.5.3. Best practice before releasing interim data is to follow the local procedure for database lock. This may mean temporarily removing the write access. These steps may include but are not limited to:

- Notification of sponsor/investigator,
- Entry and reconciliation of all data received,
- Reconciliation of SAE's,
- Performance of quality control checks,
- Identification of protocol violations,
- Completion of all medical coding, and
- Resolution and quality control of outstanding data queries.

5.5.4. Ensure the recipient is aware of the regulations regarding the use of linked data.

5.5.5. Where necessary, maintain the blinding of the treatment coding in the released datasets. This may mean replacing the treatment codes with mock codes or sending the dataset without the treatment assignments.

5.5.6. Maintain a record of the released datasets to include:

- The data fields in the dataset,
- The date and time the dataset was created,
- The person to whom the dataset was released, and
- Whether or not the recoding of the treatment assignment was implemented.

5.5.7. If feasible, make a duplicate of the released data set for archiving. Ensure the file specifications include the date and time the original released file was created.

5.5.8. For the transmission of datasets, follow your site's requirements regarding the transfer of study data.

6.0 REFERENCES

Health Canada, Food and Drug Regulations, Part C, Division 5, Drugs for Clinical Trials Involving Human Subjects, (Schedule 1024), June 20, 2001.

Health Canada, Guidance for Industry, Good Clinical Practice: Consolidated Guideline, ICH Topic E6, 1997.

Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada, Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, December 2014.

Department of Justice (Canada), Personal Information Protection and Electronic Documents Act (PIPEDA), updated 2006.

Pharmaceutical Inspection Convention, Pharmaceutical Inspection Co-operation Scheme, Annexe 11, Computerised Systems.

CDISC Clinical Research Glossary, Version 8.0, Glossary. December 2009. Canadian Institutes for Health Research, Privacy Advisory Committee, CIHR Best Practices for Protecting Privacy in Health Research, September 2005.

US Food and Drug Administration, Code of Federal Regulations, Title 21, Volume 1:

- Part 11, Electronic Records; Electronic Signatures, (21CFR11).
- Part 50, Protection of Human Subjects, (21CFR50).
- Part 56, Institutional Review Boards, (21CFR56).



SOP 003_05

US Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information.

US Department of Health and Human Services. Food and Drug Administration. Office of the Commissioner. Guidance for Industry, Computerized Systems Used in Clinical Investigations. Guideline. May 2007.

Official Journal of the European Communities, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

Official Journal of the European Communities, Directive 2001/20/EC of the European Parliament and of the Council of 4 April 2001. Medical Dictionary for Regulatory Activities (MedDRA), Maintenance and Support Services Organization (MSSO).

The Society for Clinical Data Management, GCDMP Committee, Good Clinical Data Management Practices. December 2009 Ed. WHO Drug Dictionary, Uppsala Monitoring Centre (UMC).