




SOP 002_07

Title	System Setup, Maintenance, and Security
SOP Code	SOP 002_07
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 002_07

1.0 PURPOSE

This SOP describes the system setup, maintenance, and security for large and small scale Data Management Systems (DMS), containing study database(s) to ensure accurate, reliable, complete, and secure data.

2.0 SCOPE

This SOP is applicable to all studies undertaken at the site (Erie Shores Health Care) and to research and Information Technology (IT) systems service provider personnel responsible for setting up and maintaining DMS which contain research study databases.

3.0 RESPONSIBILITIES

The Sponsor, Sponsor-Investigator, and/or Qualified Investigator (QI), and IT Systems Support personnel (if applicable) are responsible for ensuring all system setup, maintenance, and security activities at the site meet all of the applicable regulatory, International Conference on Harmonisation (ICH) Good Clinical Practices (GCP), and local requirements. This includes consulting with IT personnel experienced in IT systems and support for electronic DMS ensuring networking, systems, and security meet regulations.

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.

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

5.0 PROCEDURE

5.1 Implementation

5.1.1. This SOP must be followed in conjunction with local site IT and regulatory policies, in addition to federal and international, to ensure issues such as electronic archiving for research studies are dealt with appropriately. For example, policies and rules concerning the length of time to archive, the format for electronic archiving, and the personnel responsible for the archiving are study specific and related to data ownership and contractual agreements.

5.2 Setup and Maintenance Documentation

5.2.1. Clearly document and maintain a manual for all hardware information and configuration details for the DMS such as network information, network shares, and computer system specifications.

5.2.2. Clearly identify and document all software related information and details that are part of the DMS such as the operating system, encryption software, backup software, vendor name and website, relevant contact information, release/version numbers, and details on any special patches, etc.

5.2.3. Create, maintain and document a plan for system backup and recovery to include processes for all components of the DMS. Backup and recovery process must be tested periodically for most common failure scenarios.

5.2.4. Create and maintain a log for all updates and modifications to the DMS settings for the hardware and software configurations.

5.2.5. Develop and maintain a DMS plan for routine maintenance (patch, software updates) and services. Refer to Sponsor-Investigator, IT Systems Support personnel instructions, and/or local standard operating procedures for system maintenance.

5.2.6. Create and maintain a log of user accounts and corresponding user privileges and record any changes and/or modifications made to the accounts and privileges, i.e. granting different access types or account termination for unauthorized users such as ex-staff.

5.3 Security

5.3.1. Virtual security: ensure that the DMS components (i.e. computer system) to be used for housing study codes, applications and databases are protected against unauthorized access by taking such measures as security patches, anti-virus/anti-spy-ware software, and firewalls.

5.3.2. Create, test and maintain system security measures to be implemented such as demilitarized zone (a multi-level firewall protection), an internal firewall, an external firewall, network access, account privileges, and database access privileges.

5.3.3. Physical security: ensure that the DMS components, such as the server, workstation or external drives are behind locked doors, protected against unauthorized access and are also protected from other forms of potential damage caused by water leaks, fire, and electromagnetic fields.

5.3.4. If applicable, create a plan for security measures to be implemented for web-based applications such as FTP site users, user privileges, database access privileges, source codes updates, application version control, database access and database extraction.

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).

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.



SOP 002_07

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).