Erie Shores
HealthCare
Care Happens Here

SOP 002_08

Title	System Backup and Recovery Planning
SOP Code	SOP 002_08
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	Munira Sultana	23/06/2023

1.0 PURPOSE

This SOP describes the system backup, redundancy, and recovery planning for large and small scale Data Management Systems (DMS), ensuring accurate, reliable, complete, and secure data recovery in the event of a system error or natural disaster.

2.0 SCOPE

This SOP is applicable to all clinical studies undertaken at the site (Erie Shores Health Care), and to those research and Information Technology (IT) Systems service provider personnel responsible for backing up, redundancy, and recovery planning of research study databases.

3.0 RESPONSIBILITIES

The Sponsor, Sponsor-Investigator, and/or Qualified Investigator (QI) are responsible for ensuring all system backup and recovery planning 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, 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 Documentation

5.2.1. Clearly develop and maintain a documentation manual for all computer system hardware, (i.e. server, hard disk drive, external drive, DVD, RAID) and backup/recovery software used in the Data Management System.

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, test and maintain a Data Loss Prevention (DLP) plan. The DLP plan must clearly indicate backup hardware and software to be used, the backup process, backup type, i.e. daily, weekly, monthly, partial backup or 100% backup, and the backup medium such as RAID, SAN, NAS, onsite, or off site.

5.2.4. Create and maintain a log for all updates and modifications to the backup and recovery process.

5.2.5. Create and maintain a log of user accounts and corresponding user privileges as part of the backup and recovery plan process, 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.

5.2.6. Clearly document if there is any encryption or compression done to the database and how it can be recovered to the original readable state.

5.3 Backup

5.3.1. Backup and archiving processes must be tested regularly, i.e. bi-weekly or monthly.

5.3.2. Backup security measures must be identified, for example, identifying and documenting who has access to backup data.

5.3.3. Virtual security: ensure that the backup medium such as SAN, NAS, server, workstation and/or network shared drives to be used in the backup process are protected against unauthorized access.

5.3.4. Physical security: ensure that the backup medium such as SAN, NAS, server, workstation and/or external drives, DVDs are behind locked doors against unauthorized access.

5.4 Recovery

5.4.1. Recovery process must be tested periodically, i.e. monthly, quarterly or annually with some common failure scenarios.

5.4.2. Maintaining a step-by-step recovery instruction manual is essential, recovery manual must be accessible to key personnel and key personnel must be clearly identified.

5.4.3. Clearly identify and record the recovery plan for worst case scenarios.

5.4.4. Identify the maximum timeout or downtime allowed for the DMS before implementing the recovery plan.

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.

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).