Title	Database System Set-Up, Maintenance, and Security
SOP Code	SOP106_02
Effective Date	04-Jan-2016

Site Approvals

Name and Title (typed or printed)	Signature	Date dd/Mon/yyyy

1.0 PURPOSE

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

2.0 SCOPE

This SOP is applicable to all biorepository databases and to those personnel responsible for database set-up, maintenance, and security, such as Data Management and Information Technology (IT) personnel responsible.

3.0 RESPONSIBILITIES

The biorepository Director and IT Systems Support personnel (if applicable) are responsible for ensuring all system setup, maintenance, and security activities meet all of the applicable regulatory and local requirements. This includes consulting with IT personnel experienced in IT systems and support for electronic DMS ensuring adequate networking, systems, security and confidentiality of data associated with biospecimen collection and subject information, and electronic archiving for research studies are dealt with appropriately.

4.0 DEFINITIONS

See Glossary of Terms.

5.0 PROCEDURE

5.1 Database Set-up

Note: House the clinical dataset separately from the biorepository data, thereby preventing biorepository personnel from accessing the clinical data. Make the link between the biorepository data and the clinical dataset through the unique participant identifier.

5.1.1 Determine data variables to be captured according to the user requirements.

- Create the data dictionary which identifies software version, variable names, type (e.g. character, date, time, derived, numeric) and associated attributes.
- Review and approval of the data dictionary
- Define the applicable code-lists and the group of fields that will reflect the data storage
- Annotation of the biorepository sample (where applicable)
- Review and approval of the annotation of sample
- Create database user's manual

5.1.2 Ensure that requirements are defined for data transfers and integration with other systems, such as, but not limited to, laboratory databases or medical dictionary linkages (MedDRA, WHOdrug).

5.1.3 Design the data entry screens and ensure they are user-friendly and flexible for data entry. Take into consideration the data collection method being used when setting-up the database.

5.1.4 Define items/fields to be coded and the standard dictionaries to be used (e.g. MedDRA), as applicable.

5.1.5 Create specifications for database access authorization (user roles, e.g. data entry, and accounts).

5.1.6 Identify and program the edit checks and validation rules. Perform User Acceptance Testing (UAT) of the database and edit checks against user requirements or specifications, with expected and unexpected data in a testing environment.

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

5.1.8 Ensure that database finalization and agreement of approval by Data Management and biorepository Director are complete. Document appropriately that test and production environments match with UAT.

5.2 System 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.

5.2.7 [Audit, monitor and document access to information by logging] Ensure system logs events when information is accessed or released. Audit logs to ensure that the procedures are limiting access to authorized personnel and users only.

5.2.8 Ensure a back-up process is in place to ensure the database can be fully recovered. Biorepositories should ensure data is backed up on a daily basis.

5.3 Security

5.3.1 Information that is disclosed in the context of a professional or research relationship must be held confidential to the extent permissible within the law.

Confidential information may be written, verbal, electronic, photographic or stored in any other medium (i.e. tissue, diagnostic images).

5.3.2 Protection of confidentiality in the context of biospecimen collection and management includes prevention of disclosure, to other than authorized individuals, of any information which could identify a subject.

5.3.3 Every person with direct access to clinical data must comply with the regulatory requirements and privacy legislation for the maintenance of confidentiality and subject identity.

5.3.4 Authentication of the person who has access to the data constitutes the most important aspect of security. It determines the overall level of protection and is linked to key elements of data security.

5.3.5 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.

5.3.6 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.

5.3.7 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.

5.3.8 Retain a tracking document with the signatures and initials of all persons authorized to register data, or to make corrections to the data, with the essential biorepository documentation.

5.3.9 Physical security concerns the premises where biospecimens are stored, files containing essential documents and clinical data, as well as computer equipment used for data management, such as telecommunication servers, database servers and computers are located. 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.. [A backup process should be in place to ensure the database can be fully recovered. Biorepositories should strive to ensure data can be fully recovered on a daily basis,]

5.3.10 Establish a mechanism for control of access to secure premises. Document the procedure. It is recommended that the control mechanism includes use of magnetic cards or a biometric recognition system that allows tracking of movement in and out of the premises, if applicable.

5.3.11 Logical security concerns management of access to data, which includes identification, authentication, and authorization. In order to ensure logical security, the following measurements should be applied:

- Limit authorized access to members of the research team, and those identified by the protocol, the consent form, and the delegation of authority form;
- Grant privileges for physical or electronic access to data , to personnel according to the roles and responsibilities defined by the biorepository;

5.3.12 Designate a person in charge of system management (system administrator).

5.3.13 System Administrator's responsibilities include:

- Develop and enforce standardized procedures for logical security;
- Assign a different identification code to each user of the data management system;
- Ensure that users change their confidential password regularly, according to the period defined by the system administrator;
- Ensure the confidentiality of the authentication of system users, and document access tracking;
- Establish a Disaster Recovery Plan, for saving and recovering data, in the event of loss or disaster;
- Suspend the authorized access of a user after a given number of errors. Inform other users of this suspension. Update the delegation of tasks form, accordingly. Retrain user, if required. Document training; and
- Cancel access for research team members who leave the repository program (resignation, illness, maternity leave, etc.). Update the delegation of tasks form, accordingly.

5.4 Data Confidentiality

5.4.1 A participant who authorizes access to his/her data, must be reasonably assured that the biorepository, its authorized representatives, will take precautions to ensure that verified and collected data remain confidential.

5.4.2 Ensure that the informed consent form (ICF) and process addresses the

provisions and limits of confidentiality, within the context of the repository program, as per ICF process and form SOP,

5.5 Specimen De-identification:

5.5.1 Specimens received at the biorepository are de-identified and assigned a unique identifier. This unique identifier can only be linked back to the clinical dataset by select biorepository personnel.

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.

2011 NCI Best Practices for Specimen Resources. Office of Biorepositories and Biospecimen Research, National Cancer Institute, Bethesda, MD. http://biospecimens.cancer.gov/bestpractices/2011-NCIBestPractices.pdf

ISBER Best Practices for repositories: Collection, storage, retrieval and distribution of biological materials for research. 3rd Edition, http://www.isber.org

CTRNET Standard Operating Procedures, Canadian Tissue Repository Network

7.0 REVISION HISTORY

SOP Code	Effective Date	Summary of Changes
SOP106_01	01-Aug-2012	Original version
SOP106_02	04-Jan-2016	5.2.7: Added logging of user use. 5.2.8: Added database back-up. Updated references. Remove OTRN logo.