Data Management Requirements for Central Data Management Facilities

The following clinical trial data management requirements must be met in order to ensure the authenticity and integrity of data. The Division of Acquired Immunodeficiency Syndrome (DAIDS) may choose to conduct or to have a data management assessment visit to the facility conducted by an independent contractor.

1. Data Management Operations

1.1 Facility Staff

1.1.1 Create and keep on file a current organizational chart for central data management personnel at the facility.

1.1.2 Appoint a Head of data management with the appropriate credentials and training in relation to the responsibilities assumed in the position.

1.1.3 Create and keep on file current job descriptions of key data management personnel.

1.1.4 Ensure that the assigned data management roles and responsibilities of the staff are reasonable compared with the experience/training of each individual.

1.2 Training Needs

1.2.1 Develop an overall training plan that is relevant to the chosen data management system. Include what training is provided, to whom it is provided, how often it is provided, who provides the training, and how training effectiveness is monitored (e.g., written test after training, hands-on demonstration of new skills).

1.2.2 Develop a training documentation system to track training given and received and to maintain training records.

1.3 Standard Operating Procedures (SOPs)

Establish data management/information technology (IT) SOPs adequate to control the security, privacy, and accuracy of the data, including, but not limited to:

- System Development and Validation
- Installation and Validation of Software
- Facility, System, and Data Security
- System User Account Maintenance
- System Maintenance
- Change Control and Configuration Management
- Backup, Restore, and Disaster Recovery
- Data Collection Forms (review and approval process)
- Data Storage
- Database Design and Validation

- Coding Mechanism and Process
- Data Acquisition, Entry, and Processing
- Data Queries and Data Error Correction
- Adverse Event Reporting (AEs, SAEs, EAEs, Safety Reports)
- Database closure/archiving (not required prior to enrollment)
- Data audits (not required prior to enrollment)
- Data Management Training

1.4 Quality Assurance (QA)/Quality Control (QC)

Develop and document (e.g., QA/QC SOPs, Data Quality Management Plan) the data management QA/QC process. Include how the accuracy, integrity, consistency, reliability, and completeness of data received from the data collection site(s) will be ensured; the frequency of quality review; the percentage of records reviewed; the error rate; and the measures taken to correct and resolve data errors.

2. Overall Data Management System

2.1 Hardware

2.1.1 Choose a computer system platform, including workstations, servers (e.g., UNIX, Windows), and versions used for central storage, security, processing, and other data management, that is of sufficient size and speed to be able to efficiently support the chosen data management software and database needs.

2.1.2 Perform and document computer system validation. Include requirements/ specifications (e.g., validation protocol), test results, review of results, remediation taken to fix any problems, and test results after remediation.

2.1.3 Maintain system documentation and reference manuals used during the clinical trial.

2.2 Software

2.2.1 Choose software to be used as the database system, including versions, capability, and associated tools, that has sufficient capacity to handle the anticipated data volume for the facility and has the capability of generating the data in the manner needed, keeping an audit trail, and performing process inspections and edit checks.

2.2.2 For each software package used in the data management process, perform and document software installation validation.

A. For custom software validation, include requirements/specifications (e.g., validation protocol, test scripts), test results, review of results, remediation taken to fix any problems, and test results after remediation.

B. For off-the-shelf software validation, follow the test scripts provided by the company and document the steps taken.

2.2.3 Maintain software documentation and reference manuals used during the clinical trial.

2.3 Internet Capabilities

2.3.1 Choose an Internet service that will provide the speed, reliability, security, and times of access necessary to facilitate the conduct of the clinical trial.

2.3.2 If possible, establish an Internet connection independent of the institution or organization (e.g., main university, main hospital), if applicable.

2.4 Physical Security

Develop a security plan for the computer room and the main server room (if in a location separate from the computer room). Include who has access to the computer room/server room and how access is requested and approved; how access is monitored and documented; and how the computer room/server room is protected from fire, electrical power problems (e.g., power interruption, electrical surges), flooding, and theft.

2.5 Data Security

Develop a security plan for data, both electronic and hard copy data.

2.5.1 For electronic data, include password protection, virus protection, firewalls, encryption, and authority checks (used to ensure only authorized individuals access the system).

2.5.2 For hard copy data, include who has access to the storage area and how access is requested and approved; how access is monitored and documented; and how the storage area is protected from fire, flooding, and theft.

2.6 Rights Access, Roles, and Privileges

Develop a process for how access levels for user accounts, roles, and groups are determined. Include who approves user accounts, roles, and groups; how user accounts, roles, and groups are created, modified, and privileges removed; how user accounts and groups are documented; and how visitor access is handled and documented.

2.7 Environment and Maintenance

2.7.1 Develop environmental controls to support effective operation for computers, servers, and peripherals (i.e., temperature, humidity, power, etc.). Include how the environmental controls are monitored and how the environmental values are logged.

2.7.2 Develop a maintenance plan for the computer systems. Include who is responsible for maintenance, a description of the maintenance schedule, and how and where maintenance logs are maintained.

2.8 Change Control Procedures

Develop change control procedures to document changes made to the computer system, including software changes. Include how changes are requested, how the impact of the change is assessed, who is responsible for authorizing the change, how the change is tested and released, and how changes are documented.

2.9 Backup and Restoration

2.9.1 Develop a database backup plan. Include who is responsible for the backup, the frequency of the backup, the log created during the backup, backup media rotation strategy, where the backup media are stored, and how backup activities are documented.

2.9.2 Develop a database restoration plan. Include how restorations are tested, how restoration requests are logged, and how database files are restored after loss.

2.10 Disaster Contingency Plan

Develop a disaster contingency plan (e.g., in the case of a fire, theft). Include how the computer system will be restored/replaced and revalidated; how the software will be restored/replaced and revalidated; how the data will be restored/replaced and quality reviewed; and a description of the system or process that will be used while restoration/ replacement takes place (e.g., hand capturing data).

3. Protocol-specific Database(s)

3.1 Data Collection Tools

3.1.1 Data Collection Tool Development

Establish a development process for data collection tools (e.g., case report forms, questionnaires). Include design, development, coding, generation, review, revision, approval, testing, version control, and distribution.

3.1.2 Data Coding

Develop a plan for data coding and text coding, including any standard dictionaries to be used.

3.1.3 Completion Instructions

Develop completion instructions for data collection tools to accurately describe the way data should be collected, including a timeline for completion and submission.

3.1.4 Receipt Control and Tracking Procedures

Develop a plan for receipt control and tracking of data collection tools (e.g., barcoding, numbering system).

3.1.5 Storage

Establish storage space for both paper and electronic data collection tools that is adequate to store study documentation, complies with participant confidentiality, has adequate security in place, and has controlled access.

3.1.6 Source Documentation

Develop source documentation requirements in relation to the data collection tools, including collection, verification, storage, and participant confidentiality.

3.1.7 Change Control Procedures

Develop change control procedures to ensure quality control in changes made to the data collection tools. Include how changes are requested, how the impact of changes is assessed, who is responsible for authorizing the changes, how the changes are tested and released, and how the changes are documented.

3.2 Database Development

3.2.1 Programming Standards

A. Develop data programming plans to include programming standards for database development. Include application architecture, design, programs, database structure, and physical implementation details.

B. Document adherence to the programming standards during database development.

3.2.2 Coding Criteria Establishment

Develop the requirements for coding (coding plan) for the trial. Include actual coding, review, QA/QC, coding standards, and dictionary versioning.

3.2.3 Edit Check Development Process

Establish an edit check development process that includes edit check requirements/specifications, design documentation, test results, review of results, remediation taken to fix any problems, and test results after remediation.

3.2.4 Protocol-Specific Database Validation

A. Perform and document protocol-specific database validation. Include database requirements/specifications (e.g., validation protocol), design documentation, test results, review of results, remediation taken to fix any problems, and test results after remediation.

B. Develop documentation for the approval of the database for production implementation.

3.2.5 Technical Database System Documentation

Develop and maintain system documentation that describes the database structure, variable names, data attributes, coding schemes, missing values, collected variables, calculated variables, transformed variables.

3.2.6 Change Control Procedures

Develop change control procedures to document changes made to the database design. Include how changes are requested, how the impact of the change is assessed, who is responsible for authorizing the change, how the change is tested and released, and how the change is documented.

3.3 Enrollment/Randomization Procedures

3.3.1 Develop and document enrollment procedures and, if applicable, randomization, and stratification procedures. Include how eligibility for enrollment will be checked; the methods used to minimize/avoid bias, management of randomization codes, and security and integrity of randomization; and how enrollment/randomization will be suspended or closed.

3.3.2 Perform and document validation of the randomization schema, if applicable. Include randomization requirements/specifications (e.g., validation protocol), design documentation, test results, review of results, remediation taken to fix any problems, and test results after remediation.

3.4 Blinding Procedures

Develop and document blinding procedures, if applicable. Include how study agent is blinded, how the blinding codes are maintained, how the integrity of blinded data is maintained, and who is responsible for holding the blinding codes.

3.5 Data Processing

3.5.1 Data Entry

A. Develop a process for maintaining a log of data received from the data collection site(s).

B. Determine a method of data entry (e.g., double data entry, split screen verification, electronic data capture) that will ensure the completeness, reliability, and accuracy of the data.

C. Develop data entry instructions, including timelines for data entry.

3.5.2 Electronic Data from Other Sources (i.e., Laboratory Data)

A. Develop plan for receipt and processing of electronic data from other sources. Include how data will be transferred, received, quality controlled, loaded into the database, and synchronized with the clinical database.

B. Document the process to be used to perform quality control checks on laboratory and other data received from other sources.

C. Perform and document validation of systems/processes to be used to transfer, receive, load, and synchronize the data. Include requirements/specifications (e.g., validation protocol), design documentation, test results, review of results, remediation taken to fix any problems, and test results after remediation.

3.5.3 Data Error Correction

A. Develop a process for how data errors are detected. Include query and edit check specifications (e.g., logic checks, out of range checks), how quality control reviews are performed, and how often the reviews are performed.

B. Develop a process for how data errors are corrected. Include distribution and tracking of data queries (data clarifications) to the data collection site(s) and how data errors are documented, tracked, resolved, and corrected.

3.5.4 Quality Review of Data

Develop a plan for retrospective quality review of data. Include the frequency of review, the percentage of records reviewed, the error rates, and the measures for error correction and resolution.

3.6 Unblinding for Safety

Develop a plan for how to break the blinding code when the safety of a participant is at risk, if applicable, including who is responsible for making the decision to unblind and how to contact the responsible person outside of business hours.

3.7 Adverse Event Reporting

3.7.1 Adverse Event Coding

A. Choose an adverse event coding system (e.g., MedDRA).

B. Perform and document installation validation of coding–related software. Include coding system requirements/specifications (e.g., validation protocol), design documentation, test results, review of results, remediation taken to fix any problems, and test results after remediation.

3.7.2 Adverse Event Reporting Procedures

Develop a process for disseminating adverse events data, which includes adverse events (AEs), serious adverse events (SAEs), and expedited adverse events (EAEs). Include how adverse event data are received from the data collection site(s) (i.e., logged, tracked, entered, and processed), reported according to the specifications in the clinical protocol, documented, and quality controlled.

3.7.3 Data Reconciliation

Develop a plan for reconciliation of data between the safety database (EAEs/SAEs) and the clinical database (AEs), if applicable. Include documentation of reconciliation efforts, test results, review of results, remediation taken to fix any problems, and test results after remediation.

3.7.4 Safety Reports

Develop a process for writing and submitting safety reports. Include report specifications for reports to be sent to safety monitoring committees (e.g., Data and Safety Monitoring Board (DSMB), Institutional Review Board (IRB)/Ethics Committee (EC)) and regulatory agencies, how routine safety reports are generated and to whom they are provided, how report testing/validation is documented, the process for conducting quality control review of the data, and timeframes for submission.

3.8 Study Reports

Establish a process for report development, including specifications, programming, testing/validation, and documentation.

4. Database Closure and Archiving

4.1 Final Database Audit

Develop a plan for final database audit. Include the timing for the final database audit, the audit process, acceptable error rates, and how data errors are detected, documented, tracked, resolved, and corrected.

4.2 Database Closure

Develop procedures for how the database is closed. Include who is responsible for making the decision to close the database, the steps that are followed, and how the activities are documented.

4.3 Database Review

Describe the process for reviewing the database once the database is closed, if it is necessary to do so. Include who is responsible for making the decision; the steps for re-opening, reviewing, and re-closing the database; and how the activities are documented.

4.4 Unblinding for Data Analysis

Describe how the blinding code is broken for data analysis, if applicable. Include who is responsible for making the decision to break the code, the steps that are followed, and how the activities are documented.

4.5 Final Datasets

Develop a plan for final datasets. Include location and security of final datasets, documentation for final datasets, and final disposition/archival of datasets.

4.6 Final Safety Data

Develop a plan to provide final safety data to the DAIDS Regulatory Compliance Center (RCC) at the end of the clinical trial.

4.7 Record Retention

Develop a plan for record retention, both electronic and hard copy. Include when record retention begins, the length of time the records are retained, where the records are retained, the security of the storage space, who has access to the storage space, who is responsible for approving access, how access is documented, how record retention is documented, and how records will be accessible for inspection by the sponsor, regulatory agencies, or other authorized individuals.

5. Data Audits

Develop a process facility personnel will follow in the event of a data audit by a regulatory authority or a clinical trial sponsor. Include how to prepare for the data audit, how data audits are scheduled, who is notified upon the inspector's arrival at the facility, what documentation to expect from the inspector, how facility personnel should conduct themselves during the audit, how document and sample requests from the inspector should be handled, how a response to the regulatory authority/sponsor will be generated, and how remediation of contingencies will be performed and documented.