Data Management Requirements for Data Collection Sites

The following clinical trial data management requirements must be met in order to ensure the authenticity and integrity of data.

1. Data Management Operations

1.1 Data Collection Staff

1.1.1 Create and keep on file current job descriptions of data collection staff.

1.1.2 Ensure that the assigned data collection 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 for data collection. 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)

At a minimum the following processes and SOP topics must be established at each data collection site to support the coordination of data management activities:

- Computer Room, Hardware, and Data Security, including system user account maintenance
- Data Acquisition, Entry, and Processing
- Data Queries and Data Error Correction
- Data Collection Training
- Data Quality Management
- Data Storage

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 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

Choose a computer system that is of sufficient size and speed to be able to efficiently support the data collection activities.

2.2 Physical Security

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

2.3 Data Security

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

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

2.3.2 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.

2.4 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; how the software will be restored/replaced; 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).

2.5 Data Processing

2.5.1 Data Entry

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.

2.5.2 Data Error Correction

A. Develop a process for how data errors are detected. Include how quality control reviews are performed and how often the reviews are performed.

B. Develop a process for how data errors are corrected. Include tracking of data queries (data clarifications) and how data errors are documented, tracked, resolved, and corrected.

3. Data Storage

Develop a plan for data storage, both electronic and hard copy. Include 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 storage is documented, and how records will be accessible for inspection by the sponsor, regulatory agencies, or other authorized individuals.