Computerized Systems in Clinical Trials: Data Quality and Data Integrity

An Overview of Best Practices from PEACH

Earl W. Hulihan, Senior Vice President, Regulatory Affairs
Medidata Solutions Worldwide
'ehulihan@mdsol.com'
direct: 1,610,393,1109
The views and opinions expressed in the following PowerPoint slides are those of the individual presenter and should not be attributed to Drug Information Association, Inc. (“DIA”), its directors, officers, employees, volunteers, members, chapters, councils, Special Interest Area Communities or affiliates, or any organization with which the presenter is employed or affiliated.

These PowerPoint slides are the intellectual property of the individual presenter and are protected under the copyright laws of the United States of America and other countries. Used by permission. All rights reserved. Drug Information Association, DIA and DIA logo are registered trademarks or trademarks of Drug Information Association Inc. All other trademarks are the property of their respective owners.
Rationale - Latin America perspective:

• 25% outsource to Latin America
• 56% indicate that LA easier to work with
• 89% feel LA significant to USA’s future
• 49% believe infrastructure capability, language capability, education and skilled workforce key

**Harris Interactive poll of 1000 Executives, September, 2010**
Trials conducted by:

- academic institutions
- government organizations
- companies from the device, pharmaceutical, and biotech industries

for the purpose of human welfare
A set of policies, processes and procedures required for planning and execution (production / development / service) in the core business area of an organization. QMS integrates the various internal processes within the organization and intends to provide a process approach for project execution. QMS enables the organizations to identify, measure, control and improve the various core business processes that will ultimately lead to improved business performance.” (ISO 9001:2008).
• Management
  – provides support and oversight
  – establish a quality system that includes policies, procedures, and processes
  – include a process by which to capture, quantify, and analyze performance

*If properly done, it will allow for continual improvement*
Key Attributes & Elements

• **QMS**
  – adapt and evolve along with the organizations business, regulatory, and quality objectives

• **Metrics**
  – standards for measuring performance within a system or process
  – should not be a stagnant
  – include
    • personnel qualification and training
    • controlling and defining processes
    • document management
    • system validation
    • quality review
Risk Assessment & Management

- Identify
  - what can go wrong?
- Analyze
  - probability of occurrence of each & its severity
- Mitigate
  - risk mitigation plan
- Maintain & Monitor
  - ongoing process & based upon feedback

The cycle is repeated
Computerized System

• Includes all
  – Hardware, software, people, procedures, processes, facilities, et. al. (both directly or indirectly related to trial, e.g., Investigator and when outsourced)
  – Each has
    • stakeholders
    • lifecycle

All must be controlled to achieve data integrity and ensure subject safety
Requires Qualification

A Technology Infrastructure

EDC Local Server Room
- Standby Database Server
- Domain Controller/Backup Server
- Monitoring Server
- Web Server
- LAN Switches
- DMZ NETWORK
- Switch
- Leased Line
- INTERNAL NETWORK

EDC Remote Server Room
- Domain Controller/File Server
- Database Server
- Web Server
- LAN Switches
- DMZ NETWORK
- Switch
- Leased Line
- INTERNAL NETWORK

Internet

Investigator Sites
- ISD Line
- Switch
SDLC and SLC

- Phase 1: Project Initiation
- Phase 2: Requirements
- Phase 3: Design Specifications
- Phase 4: Implementation
- Phase 5: Testing
- Phase 6: Installation & Acceptance
- Phase 7: Operation & Maintenance
- Phase 8: Decommissioning
Life Cycle of Electronic Records

- Record Definition - content, intended use, applicable standards, naming conventions, format, metadata
- Record Storage - location, structure and design
- Record Access - privacy, security, legal classification, access methods
- Record Protection - stewardship, backup & restore, disaster recovery
- Record Retention - retention period, short and long term preservation methods to meet requirements for applicable regulatory authorities
• System not properly validated
• Unauthorized access to electronic records
• Unauthorized modification of electronic records
• Unauthorized or inappropriate deletion of records
• Data corruption to render the record inaccessible
• Loss of data, including metadata, during a process (e.g., transmission, archival, migration)
• The person or system modifying the data is not recorded or is not identifiable
• The time and date the data was modified is not recorded or is not accurate (including capture of local time zones, when necessary, to distinguish between multiple sites)
• The original data are not retained
• A reason for change is not recorded
• Establish a comprehensive information security policy
• Establish an internal security organization and control external party use of the stakeholder’s organization information
• Establish responsibility for the organization’s assets and use an information classification system
• Emphasize security prior to employment, during employment, and at employment termination
• Use security areas to protect facilities and equipment
• Establish procedures and responsibilities, control third-parties access and ability to change, plan for the future, protect against malicious code, backup information, protect networks, protect the exchange of data
Control access to information, user access rights and encourage good access practices. Control access to networked services and operating systems. Control access to applications and information. Protect mobile and telecommuting facilities.

Identify information system security requirements and application’s process information correctly. Use cryptographic controls to protect information and control development and support processes. Protect and control the organization’s system files and Establish technical vulnerability management.

Report information security events and weaknesses and manage information security incidents and improvements.

Use continuity management to protect information.

Comply with legal requirements by performing security compliance reviews and carrying out controlled information system audits.
• Information in a clinical trial must be fairly and lawfully processed
• Information can only be processed for limited purposes and not in any way incompatible with those purposes
• The information must be adequate, relevant and not excessive
• The information must be accurate
• The information can be kept for only as long as is necessary for its business purpose
• All the information must be processed in line with the individual’s rights
• The information must be kept secure
• If the information is going to be transferred to countries without adequate data protection laws, the transferring agent must demonstrate adequate mitigation
Outsourcing

- Decide what should be outsourced: create a list of requirements & involve personnel and departments
- Evaluation & Selection: use qualification questionnaire, reference checks, phone interview, onsite visit, discuss n-tier outsourcing
- Management: how the staff will be trained and managed, definition of the procedural controls needed to conduct the work, communication and escalation process, description of the types of information technologies expected to be used, quality metrics to be collected and reported, schedule for implementation, change management program
- Completion: records and data custody and retention, access to software and related documentation, project documentation and deliverables
- Follow the same life cycle principles
- Special considerations for laboratories
  - Reference ranges (single location)
  - Reference ranges (multiple locations)
- Designated laboratory contact
• Follow the same life cycle principles
• Special considerations for laboratories
  – Reference ranges (single location)
  – Reference ranges (multiple locations)
• Designated laboratory contact
Computerized Data Collection

- eCRF - Electronic Case Report Form
- ePRO - Electronic Patient-(Subject) Reported Outcome
- EMR/EHR - Electronic Medical Record/Electronic Health Record
- Video Records
- Data Warehousing
- Other Systems & Processes at the Later Stages of Clinical Research
- Submission of data to regulatory authorities and reviewers
- Post-marketing
- Registration Management
- Submission Management
Selection of the system:

Will the system meet the needs of all trials and yet-to-be-developed protocols?

Cost in terms of resources - Is new infrastructure required? Are additional resources to maintain and implement the system required?

Vendor risk: What is the experience of the vendor in this arena? What is the experience of the sponsor with the vendor (does the sponsor already use other products, such as IVRS)? Is the vendor able to support the product long term? Is the vendor financially viable? Consider product pricing, scalability, integration opportunities (with, for example, SAS, IVRS, Safety, CTMS, CDMS), and flexibility to configure to business processes.
Stakeholder contribution and input

For the investigator, systems should provide ease of use and workflow for the investigator and site-related personnel. Any system cannot be viewed by the site as an annoyance or hindrance to the process; the system must be viewed as an asset to the process of evaluating and treating clinical trial subjects during the trial.

Real-time access to the data collected must maintain the necessary confidentiality required by the clinical trial (i.e. blinded clinical trials have different requirements than unblinded clinical trials). Only specified stakeholders should have system permissions to alter data and the management of user access rights to the system should be documented in procedures.

For all stakeholders training, which is required by industry and regulatory authorities alike, is key to the success of any system.
Audit trail capability of the system

The ability to re-create the trial is dictated by regulatory requirements and general scientific principles. One tool used to support this requirement and a key aspect of maintaining data integrity is an audit trail. The audit trail capabilities of the system(s) should be understood by the sponsor, clinical investigator and regulators.

Privacy laws and regulations

Transmission of data across country borders may be in direct conflict to privacy laws and regulations, which change from country to country. Certain country requirements guide data entry values particularly on Protected Health Information (PHI) data points, which have implications on how data are collected and analyzed. This impacts how systems should be designed to capture this information.
Subject rights

Informed consent needs to contain references to all data collection computerized systems that the subject will interact with (e.g., ePRO, eDC, video). While obtaining informed consent from a subject is currently a manual documentation process, there exists the potential to manage this electronically as the clinical trial process evolves.