# Computerized Systems Used in Medical Device Clinical Investigations

## Presented by Jonathan Helfgott

Consumer Safety Officer

Division of Bioresearch Monitoring

Office of Compliance

Center for Devices and Radiological Health

# Objectives

- Understand FDA's requirements and expectations for Sponsors, Clinical Investigators, and others using Computerized Systems in Medical Device Clinical Investigations

# Overview

I.     Users and Examples of Computerized Systems used in Clinical Investigations

II.     FDA Regulatory Requirements & Expectations

III.     Recommendations from FDA Guidance

# Computer Systems in Clinical Investigations are Used By:

- Clinical Investigators (CIs)
- Sponsors
- Institutional Review Boards (IRBs)
- Study Coordinators (Monitors)
- Statisticians
- Data Managers
- Contract Research Organization (CROs)

# Examples of Computerized Systems Used in Clinical Investigations:

- Electronic Case Report Forms (eCRFs)
- Electronic Patient Reported Outcomes (ePRO)
  - Interactive Voice Response System (IVRS)
- Adverse Event Reporting Systems (AERS)
- Laboratory Information Management Systems (LIMS)
- Systems that automatically record data by integrating data from a medical device such as an ECG, Holter- Monitor, MRI, etc…

# Which Computerized System Should the Sponsor Choose?

- Design their own systems?
- Vendor-Purchased Systems?
- Hybrid- Electronic/Paper Systems?

# FDA Regulatory Requirements

- 21 CFR 812.140(a) requires that participating Clinical Investigators maintain "accurate, complete, and current records relating to the Investigator's participation in an investigation"

- 21 CFR 812.140(b) requires Sponsors to maintain "accurate, complete, and current records relating to an investigation"

# FDA Regulatory Requirements

- All 21 CFR Part 812 regulations apply equally to both paper records and electronic records

- The use of computerized systems in clinical investigations does not exempt IDEs from any Part 812 regulatory requirement

# FDA Guidance, May 2007: "Computerized Systems Used in Clinical Investigations"

- Applies to computerized systems used for records in electronic form that are used to create, modify, maintain, archive, retrieve, or transmit clinical data required to be maintained, or submitted to the FDA

# FDA Guidance, May 2007: "Computerized Systems Used in Clinical Investigations"

Recommendation Categories:

- Training of Personnel
- Internal/ External Security Safeguards
- Source Documentation and Retention
- Other System Features
- Standard Operating Procedures

# Training of Personnel

- All personnel who develop, maintain, or use the computerized systems should be trained

- Personnel must learn how to perform their assigned tasks

- Document the computer education, training, and experience

# Internal Security Safeguards

- Access must be limited to authorized individuals
- Each user should have an individual account
- Passwords should be changed at established intervals
- The system should limit and record the number of unauthorized log-in attempts
- Automatic log off for long idle periods

# External Security Safeguards

Controls should be established to:

- Prevent unauthorized external software applications from altering, browsing, querying, or reporting data

- Prevent, detect, and mitigate effects of computer viruses, worms, or other potentially harmful software code on study data and software

  (e.g.-firewalls, antivirus, etc…)

# Source Documentation & Retention

- When original observations are entered directly into a computerized system, the electronic record is the source document

- Under 21 CFR 312.62, 511.1(b)(7)(ii) and 812.140, the clinical investigator must retain records required to be maintained under parts 312, 511.1(b), and 812, for a period of time specified in these regulations

- Applies to the retention of the original source document or a copy of the source document

# Additional Recommendations

- During pre-IDE meetings, identify all source documents that will be kept electronically throughout the duration of the Clinical Investigation
  - It might be helpful to provide a detailed schematic of the data flow

    (e.g.-eCRF in XML format from clinical site→ Sponsor/CRO/Monitor→ Data Lock→ Statistical Review→ Clinical Report→ Submission to FDA)

# Source Documentation & Retention

- The information provided to FDA should fully describe and explain how source data were obtained and managed, and how electronic records were used to capture data

- Maintain a cumulative record that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges

- That record should be kept in the study documentation, accessible for use by appropriate study personnel and for inspection by FDA investigators

# Other System Features: *Direct Entry of Data*

- For direct entry of data, the system should incorporate prompts, flags, or other help features to encourage consistent use of clinical terminology and to alert the user to data that are out of acceptable range

# Other System Features:
## *Audit Trails*

- Computer-generated, time-stamped electronic audits trails are the preferred method for tracking changes to electronic source documentation

- Audit trails or other security methods used to capture electronic record activities should describe when, by whom, and the reason changes were made to the electronic record to ensure that only authorized additions, deletions, or alterations have occurred

- Ensure that audits cannot be overridden

# Standard Operating Procedures

Specific procedures and controls should be in place for:

- System setup/installation
- System operating manual (User's Manual)
- Validation and functionality testing
- Data collection and handling
- System maintenance (Service/Upgrade Logs)

# Additional Recommendations:

- Identify and document all the specified requirements for the system
- Ensure that the system is capable of consistently meeting all specified requirements
  - If a Vendor/CRO designed/maintained the system, did they provide you with a validation summary or report? Is there any documented User Site Testing?

# Additional Recommendations

- Identify all the computer and software components used in the system
  - The identification should be a detailed list that includes product names and specific version numbers to keep track of any modifications
- Sufficient backup and recovery procedures help protect against data loss at clinical sites (e.g. Redundant Servers or Hard-Drives)

# Conclusion

- The intent of FDA's regulatory requirements and guidance is to ensure that electronic records used in clinical investigations are accurate, complete, and current

- These requirements are important because data is used to support a product's safety and effectiveness