Guidance for Industry

Computerized Systems Used in Clinical Trials

DRAFT GUIDANCE

This guidance document is being distributed for comment purposes only.

Draft released for comment on June 18, 1997.

Comments and suggestions regarding this draft document should be submitted within 60 days of publication in the *Federal Register* of the notice announcing the availability of the draft guidance. Submit comments to Dockets Management Branch (HFA-305), Food and Drug Administration, 12420 Parklawn Dr., rm. 1-23, Rockville, MD 20857. All comments should be identified with the docket number listed in the notice of availability that publishes in the *Federal Register*. For questions regarding this draft document contact James F. McCormack, Ph.D. (301) 827-0425, Internet Address jmccorma@ora.fda.gov

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Drug Evaluation and Research (CDER)
Center for Biologics Evaluation and Research (CBER)
Center for Devices and Radiological Health (CDRH)
Center for Food Safety and Applied Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
Office of Regulatory Affairs (ORA)
Month, Year

Table of Contents

I. INTRODUCTION 1

II. DEFINITIONS 2

III. GENERAL PRINCIPLES 3

IV. STANDARD OPERATING PROCEDURES 4

V. DATA ENTRY 5
- A. Electronic Signatures 5
- B. Audit Trails 5
- C. Date/Time Stamps 6

VI. SYSTEM DESIGN 6

VII. SECURITY 7
- A. Physical Security 7
- B. Logical Security 8

VIII. SYSTEM DEPENDABILITY 8

IX. SYSTEM CONTROLS 9
- A. Software Version Control 9
- B. Change Control 9
- C. Contingency Plans 10
- D. Backup and Recovery 10

X. TRAINING OF PERSONNEL 10
- A. Qualifications 10
- B. Training 10
- C. Documentation 11

XI. RECORDS INSPECTION 11

XII. CERTIFICATION OF ELECTRONIC SIGNATURES 11

XIII. REFERENCES 12

Draft - Not for Implementation

GUIDANCE FOR INDUSTRY[1]

COMPUTERIZED SYSTEMS USED IN CLINICAL TRIALS

I. INTRODUCTION

This document addresses issues pertaining to computer systems used to generate, collect, maintain, and transmit clinical data intended for submission to the Food and Drug Administration (FDA) in support of marketing or research applications. These data form the basis for the Agency's decisions regarding the safety and effectiveness of new human and animal drugs, biologicals, medical devices, and certain food and color additives. As such, these data have broad public health significance and must be of the highest quality and integrity.

FDA established the Bioresearch Monitoring (BIMO) Program of inspections and audits to monitor the conduct and reporting of clinical trials to ensure that data meet the highest standards of quality and integrity and conform to FDA's regulations for clinical trials. FDA's acceptance of data from clinical trials for decision-making purposes is dependent upon its ability to validate the quality and integrity of such data during its onsite inspections and audits. To be acceptable, the data should meet certain fundamental elements of quality whether collected or recorded electronically or on paper. Data should be attributable, original, accurate, contemporaneous and legible. For example, attributable data can be traced to the individual responsible for observing and recording the data. In an automated system, such an element could be addressed by a computer system designed to record the identity of the individual responsible for any input.

The guidance offered in this document is intended to address how these elements of data quality might be satisfied in a clinical environment where computerized systems are being used to generate, record, and maintain data. Persons using the data from computerized systems should have confidence that the data are at least as reliable as data in paper form.

This guidance has been prepared by an Agency working group representing the Bioresearch Monitoring Program Managers from each Center within FDA and the Office of Regulatory Affairs. As with other guidance documents, the FDA does not intend this guidance document to

---

[1]This guidance has been prepared by an Agency working group representing the Bioresearch Monitoring Program Managers for each Center within the Food and Drug Administration and the Office of Regulatory Affairs. This guidance document represents the Agency's current thinking on the use of computer systems in clinical trials. It does not create or confer any rights for or on any person and does not operate to bind FDA or the public. An alternative approach may be used if such approach satisfies the requirements of the applicable statute, regulations, or both. Additional copies of this draft guidance document are available from the Drug Information Branch, Division of Communications Management, HFD-210, 5600 Fishers Lane, Rockville, MD 20857, (Tel) 301-827-4573, (Internet) http://www.fda.gov/cder/guidance.htm.

be all-inclusive and cautions that not all information will apply to all situations.

This guidance should not supplant discussions between Centers and sponsors regarding format and content of electronic applications before the submission of marketing or research applications or before the initiation of trials. Modifications may be necessary for specific protocols. Due to the unique nature of clinical trials, FDA Centers have the responsibility to determine the acceptability of a protocol.

II. DEFINITIONS

Audit Trail is a secure time stamped record that allows reconstruction of the course of events relating to the creation, modification, and deletion of an electronic study record.

Certified Copy is a copy of original information that has been verified, as indicated by dated signature, as an exact copy having all of the same attributes and information as the original.

Commit means a saving action that creates or modifies, or an action that deletes, an electronic record or portion of an electronic record. For example, pressing the "Enter" key of a keyboard after information is typed to enter the information into the record.

Computerized System includes computer hardware, software, and associated documents that generate, collect, maintain, or transmit in digital form information related to the conduct of a clinical trial.

Direct Entry means recording of data where an electronic record is the original capture of the data. Examples are the keying by an individual of original observations into the system, or automatic recording by the system of the output of a balance that measures subjects' body weight.

Electronic Case Report Form (e-CRF) is an auditable permanent electronic record designed to record all of the protocol required information to be reported to the sponsor on each trial subject.

Electronic Patient Diary is an electronic record into which a subject participating in a clinical trial directly enters observations or directly responds to an evaluation checklist.

Electronic Record is any combination of text, graphics, data, audio, pictorial, or any other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

Electronic Signature is a computer data compilation of any symbol or series of symbols, executed, adopted, or authorized by an individual to be the legally binding equivalent of the

individual's handwritten signature.

Source Data is all information in original records and certified copies of original records of clinical findings, observations, or other activities in a clinical trial necessary for the reconstruction and evaluation of the trial. Source data are contained in source documents (original records or certified copies).

Source Documents are original documents and records including, but not limited to, hospital records, clinical and office charts, laboratory notes, memoranda, subjects' diaries or evaluation checklists, pharmacy dispensing records, recorded data from automated instruments, copies or transcriptions certified after verification as being accurate and complete, microfiches, photographic negatives, microfilm or magnetic media, x-rays, subject files, and records kept at the pharmacy, at the laboratories, and at medico-technical departments involved in the clinical trial.

III. GENERAL PRINCIPLES

A. When original observations are entered directly into a computer system, the electronic record is the source data.

B. A computerized system should ensure that all applicable regulatory requirements for record keeping and record retention in clinical trials are met with at least the same degree of confidence as is provided with paper systems.

C. Clinical investigators should retain copies of all records and underlying data sent to a sponsor or contract research organization including query resolution correspondence.

D. Any correction to a record required to be maintained should not obscure the original entry; this applies to both written and electronic corrections.

E. Changes to data that are stored on electronic media will always require an audit trail, per 21 CFR 11.10(e). For changes made at the research site, the clinical investigator's documentation should include who made the changes, and when, how, and why they were made.

F. The FDA may audit any and all records that might support submissions to the Agency, regardless of how they were created or maintained.

G. Data should be retrievable in such a fashion that all information regarding each individual subject in a study is attributable to that subject.

H. A computerized system should be designed so that all requirements outlined in a study

protocol are satisfied (e.g., upper or lower limits for laboratory analyses, requirements that the study be blinded) and so that requirements for the preparation and maintenance of case histories are not adversely affected by creation or storage by electronic means.

I. Study protocols should state which computerized systems are to be used for generation, collection, maintenance, and transmission of data.

J. Security measures should be in place to prevent unauthorized access to the data and the data collection device.

IV. STANDARD OPERATING PROCEDURES

Standard operating procedures (SOPs) pertinent to the use of the computerized system should be available at the clinical site.

SOPs should be established for, but not limited to:

- System Setup/Installation
- Data Collection
- System Maintenance
- Data Backup and Recovery
- Security
- Change Control

V. DATA ENTRY

A. Electronic Signatures

1. The data entry system should be designed so that individuals need to enter electronic signatures, such as combined password/usernames or biometric-based electronic signatures, before entering information for a given data entry session.

2. Each entry to an electronic record, including any change, should be made under the electronic signature of the individual making that entry.

a. In systems where an individual is entering data directly, the printed name of that individual should be visible on the data entry screen throughout the data entry session. This is intended to preclude the possibility of a different individual inadvertently entering data under someone else's name.

b. If the name displayed on the screen during a data entry session is not that of the person entering the data, then that individual should log on under his or her own name before continuing.

3. Passwords should not be shared among individuals

4. Passwords should be changed at regular intervals.

5. When someone leaves a workstation, the person should log off the system. Failing this, an automatic log off may be appropriate for long idle periods. For short periods of inactivity, an automatic screen saver with password could be coupled with a locked keypad or pointing device.

B. Audit Trails

1. 21 CFR 11.10(e) requires persons who use electronic record systems to maintain an audit trail to protect the authenticity, integrity, and, when appropriate, the confidentiality of electronic records. According to the regulation:

a. Persons must use secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records.

b. Record changes must not obscure previously recorded information.

c. Audit trail documentation must be retained for a period at least as long as that required for the subject electronic records (e.g., the study data and records to which they pertain) and must be available for agency review and copying.

2. Personnel who create, modify, or delete electronic records should not be able to modify the audit trails.

3. Audit trails in computer-assisted clinical trials should be retained as part of the basic electronic study records.

4. Audit trail files should be retained wherever the records covered by the audit trails are maintained.

5. Audit trail files should be created incrementally, in chronological order, and in a manner that does not allow new audit trail information to overwrite existing data in violation of § 11.10(e).

C. Date/Time Stamps

1. Controls should be in place to ensure that, upon each boot-up, the system's date and time are correct and that the date and time are not changed by unauthorized means.

2. The system's date and time should be used to generate the date and time applied to audit trails and records.

3. Dates and times should be local to the activity being documented and should include the year, month, day, hour, and minute. The Agency encourages establishments to synchronize systems to the date and time provided by trusted third parties. Clinical study data collection devices will likely be used in multi-center trials, perhaps located in different time zones. When a data-handling device is transported to the site of use, it is important that its time be checked and correctly set to local time.

The ability to change the date or time should be limited to authorized personnel and such personnel should be notified if a system date or time discrepancy is detected. Changes to date or time should be documented.

VI. SYSTEM DESIGN

A. Systems used for direct entry of data should include features that will facilitate the collection of quality data.

1. Prompts, flags or help features within the data collection device should be used to ensure that clinical terminology or adverse event terms are consistent with the specific study protocol. Such features should also alert the user to data that are out of acceptable range.

2. Electronic patient diaries and electronic case report forms (e-CRFs) should be designed to allow users to make annotations. Annotations add to data quality by allowing ad hoc information to be captured. This information may be valuable in the event of an adverse reaction or outlier. The record should clearly indicate who recorded the annotations and when (date and time).

B. Systems used for direct entry of data should be designed to include features that will facilitate the inspection and review of data.

Data tags (e.g., different color, different font, flags) should be used to indicate which data have been changed or deleted.

C. Recognizing that computer products may be discontinued, sponsors should make certain that continued support for the automated system is available to ensure data integrity is maintained over the life of the study, and as necessary for record retrieval and review. Such support should cover all versions of application software, operating systems, compilers, linkers, and other development tools involved in processing data or records.

VII. SECURITY

A. Physical Security

1. In addition to internal safeguards built into the system, external safeguards should be in place to ensure that access to the data collection device and to the data is restricted to authorized, trained personnel.

2. Staff should be thoroughly aware of system security measures and the importance of limiting access to authorized personnel.

3. Names of authorized staff members, their titles, and a description of their access privileges should be in the study documentation.

4. SOPs should be in place for handling and storing the system to prevent unauthorized access.

5. External safeguards should include lock-and-key storage of the data and collection devices.

B. Logical Security

1. Access to the database at the clinical site should be restricted through the system's software with its required log-on, security procedures, and audit trail. The data should not be altered, browsed, queried, or reported via external software applications that do not enter through the protective system software.

2. If a sponsor or contract research organization supplies a computerized system exclusively for a clinical trial, the system should remain dedicated to the purpose for which it was intended and validated.

3. If a computerized system being used for the clinical study is part of the system normally used by the practitioner, efforts should be made to ensure that the software is logically and physically isolated as necessary to preclude unintended interaction with non-study software. The system should be reevaluated if any of the software programs are

changed.

VIII. SYSTEM DEPENDABILITY

A. Documentation should be readily available at the site where clinical trials are conducted, to provide an overall description of computerized operations and the relationship of hardware, software, and physical environment in these computerized operations.

B. The sponsor should ensure and document that the electronic data processing system conforms to the sponsor's established requirements for completeness, accuracy, reliability, and consistent performance for the intended purpose.

C. The FDA inspects documentation, possessed by a regulated company, that demonstrates validation of software. The study sponsor is responsible for making such documentation available for inspection at the study site if requested. Clinical investigators are not generally responsible for validation unless they originated or modified software.

1. In the case of software purchased off-the-shelf, most of the validation should have been done by the company that wrote the software. The sponsor or contract research organization should have documentation of this design level validation by the vendor, and should have itself performed functional testing (e.g., by use of test data sets).

In the special case of database and spreadsheet software (1) that is purchased off-the-shelf, (2) that is designed for and widely used for general purposes, (3) is unmodified, and (4) is not being used for direct entry of data, the sponsor or contract research organization may not have documentation of design level validation. However, the sponsor or contract research organization itself should have performed functional testing (e.g., by use of test data sets) and researched known software limitations, problems, and defect corrections.

2. Documentation important to demonstrate software validation should include:

a. Written design specification that describes what the software is intended to do and how it is intended to do it.

b. A written test plan based on the design specification, including both structural and functional analysis.

c. Test results and an evaluation of how these results demonstrate that the predetermined criteria have been met.

D. Change Control

1. Written procedures should be in place to ensure that changes to the computerized system such as software upgrades, equipment or component replacement, or new instrumentation will not jeopardize the integrity of the data or the integrity of protocols.

2. All changes to the system should be documented. Changes that exceed operational limits or design specifications should precipitate revalidation.

IX. SYSTEM CONTROLS

A. Software Version Control

Measures should be in place to ensure that versions of software used to generate, collect, maintain, and transmit data are the versions that are stated in the systems documentation.

B. Contingency Plans

Written procedures should describe contingency plans for conducting the study by alternate means in the event of failure of the computerized system.

C. Backup and Recovery

1. Backup and recovery procedures should be clearly outlined in the standard operating procedures and be sufficient to protect against data loss.

Data should be backed up regularly in a way that would prevent a catastrophic loss.

2. Backup data should be stored at a secure location specified in the SOP and separate from the original records. This should include offsite storage.

3. Backup and recovery operations should be documented to permit an assessment of the nature and scope of possible data loss resulting from a system failure.

X. TRAINING OF PERSONNEL

A. Qualifications

1. Each person who enters or processes data should have the education, training, and experience or any combination thereof necessary to perform the assigned functions.

2. Individuals responsible for monitoring the trial should have education, training, and

experience in the use of the computerized system necessary to adequately monitor the trial.

B. Training

1. Training should be provided to individuals in the specific operations that they are to perform.

2. Training should be conducted by qualified individuals on a continuing basis, as needed, to ensure familiarity with the computerized system and with any changes to the system during the course of the study.

3. Training should include but is not limited to:

- System setup/installation
- Instruction in the proper use of equipment
- Data collection
- System maintenance
- Backup and recovery
- Security measures

C. Documentation

Employee qualifications, training and experience should be documented.

XI. RECORDS INSPECTION

A. The FDA may audit any and all records that might support submissions to the Agency, regardless of how they were created or maintained. Therefore, systems should be able to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the Agency. Persons should contact the appropriate Agency unit if there is any doubt about what file formats and media the Agency can read and copy.

B. The sponsor should be able to provide hardware and software as necessary for FDA personnel to inspect the electronic documents and audit trail at the site where an FDA inspection is taking place.

XII. CERTIFICATION OF ELECTRONIC SIGNATURES

When electronic signatures are used to meet an FDA signature requirement, persons using the system must submit a certification to the agency that the persons intend their electronic signatures to be legally binding, per 21 CFR § 11.100(c).

As set forth in 21 CFR 11.100(c), the certification is to be submitted in paper form signed with a traditional handwritten signature to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville Maryland 20857. The certification is to be submitted prior to or at the time electronic signatures are used. However, a single certification may cover all electronic signatures used by persons in a given organization. An acceptable certification would take the following format:

> Pursuant to Section 11.100 of Title 21 of the Code of Federal Regulations, this is to certify that [name of organization] intends that all electronic signatures executed by our employees, agents, or representatives, located anywhere in the world, are the legally binding equivalent of traditional handwritten signatures.

This "*certification*" is a legal document created by persons to acknowledge that their electronic signatures have the same legal significance as their traditional handwritten signatures.

XIII. REFERENCES

FDA, *Software Development Activities*, 1987.

FDA, *Guideline for the Monitoring of Clinical Investigations*, 1988.

FDA, *Conduct of Clinical Investigations: Responsibilities of Clinical Investigators and Monitors for Investigational New Animal Drug Studies*, 1992.

FDA, *Compliance Program Guidance Manual*, "Compliance Program 7348.810 - Sponsors, Contract Research Organizations and Monitors," August 18, 1994.

FDA, *Compliance Program Guidance Manual*, "Compliance Program 7348.811 - Bioresearch Monitoring - Clinical Investigations," August 18, 1994.

FDA, *Information Sheets for Institutional Review Boards and Clinical Investigators*, 1995.

FDA, *Glossary of Computerized System and Software Development Terminology*, 1995.

Organisation for Economic Cooperation and Development (OECD), *The Application of the Principles of GLP to Computerised Systems*, Environmental Monograph No. 116, Paris, 1995.

International Conference on Harmonisation; *"Good Clinical Practice: Consolidated Guideline"* *Federal Register*, Vol. 62, No. 90, 25711, May 9, 1997.

FDA, "21 CFR Part 11, Electronic Records; Electronic Signatures; Final Rule." *Federal Register,* Vol. 62, No. 54, 13429, March 20, 1997.