# Guidance for Industry

## COMPUTERIZED SYSTEMS USED IN CLINICAL TRIALS

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Biologic Evaluation and Research (CBER)
Center for Drug Evaluation and Research (CDER)
Center for Devices and Radiological Health (CDRH)
Center for Food Safety and Nutrition (CFSAN)
Center for Veterinary Medicine (CVM)
Office of Regulatory Affairs (ORA)
April 1999

# TABLE OF CONTENTS

# GUIDANCE FOR INDUSTRY

# COMPUTERIZED SYSTEMS USED IN CLINICAL TRIALS[1]

## I. INTRODUCTION

This document addresses issues pertaining to computerized systems used to create, modify, maintain, archive, retrieve, or transmit clinical data intended for submission to the Food and Drug Administration (FDA). These data form the basis for the Agency's decisions regarding the safety and efficacy of new human and animal drugs, biologics, 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 from these trials meet the highest standards of quality and integrity and conform to FDA's regulations. FDA's acceptance of data from clinical trials for decision-making purposes is dependent upon its ability to verify 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 individuals responsible for observing and recording the data. In an automated system, attributability could be achieved by a computer system designed to identify individuals responsible for any input.

This guidance addresses how these elements of data quality might be satisfied where computerized systems are being used to create, modify, maintain, archive, retrieve, or transmit clinical data. Although the primary focus of this guidance is on computerized systems used at clinical sites to collect data, the principles set forth may also be appropriate for computerized systems at contract research organizations, data

[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 guidance document are available from Division of Compliance Policy, HFC-230, 5600 Fishers Lane, Rockville, MD 20857, (Tel) 301-827-0420, (Internet) http://www.fda.gov/ora/compliance_ref/bimo/default.html

management centers, and sponsors. Persons using the data from computerized systems should have confidence that the data are no less reliable than data in paper form.

Computerized medical devices, diagnostic laboratory instruments and instruments in analytical laboratories that are used in clinical trials are not the focus of this guidance. This guidance does not address electronic submissions or methods of their transmission to the Agency.

This guidance document reflects long-standing regulations covering clinical trial records. It also addresses requirements of the Electronic Records/Electronic Signatures rule (21 CFR part 11).

The principles in this guidance may be applied where source documents are created (1) in hardcopy and later entered into a computerized system, (2) by direct entry by a human into a computerized system, and (3) automatically by a computerized system.

## II. DEFINITIONS

**Audit Trail** means, for the purposes of this guidance, a secure, computer generated, time-stamped electronic record that allows reconstruction of the course of events relating to the creation, modification, and deletion of an electronic record.

**Certified Copy** means 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, which creates or modifies, or an action which deletes, an electronic record or portion of an electronic record. An example is pressing the key of a keyboard that causes information to be saved to durable medium.

**Computerized System** means, for the purpose of this guidance, computer hardware, software, and associated documents (e.g., user manual) that create, modify, maintain, archive, retrieve, or transmit in digital form information related to the conduct of a clinical trial.

**Direct Entry** means recording 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 subject's body weight.

**Electronic Case Report Form (e-CRF)** means an auditable electronic record designed to record information required by the clinical trial protocol to be reported to the sponsor on each trial subject.

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

**Electronic Record** means 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** means 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.

**Software Validation** means confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through the software can be consistently fulfilled. For the purposes of this document, design level validation is that portion of the software validation that takes place in parts of the software life cycle before the software is delivered to the end user.

**Source Documents** means 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.

**Transmit** means, for the purposes of this guidance, to transfer data within or among clinical study sites, contract research organizations, data management centers, or sponsors. Other Agency guidance covers transmission from sponsors to the Agency.

## III. GENERAL PRINCIPLES

A. Each study protocol should identify at which steps a computerized system will be used to create, modify, maintain, archive, retrieve, or transmit data.

B. For each study, documentation should identify what software and, if known, what hardware is to be used in computerized systems that create, modify,

maintain, archive, retrieve, or transmit data. This documentation should be retained as part of study records.

C. Source documents should be retained to enable a reconstruction and evaluation of the trial.

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

E. The design of a computerized system should ensure that all applicable regulatory requirements for recordkeeping and record retention in clinical trials are met with the same degree of confidence as is provided with paper systems.

F. Clinical investigators should retain either the original or a certified copy of all source documents sent to a sponsor or contract research organization, including query resolution correspondence.

G. Any change to a record required to be maintained should not obscure the original information. The record should clearly indicate that a change was made and clearly provide a means to locate and read the prior information.

H. Changes to data that are stored on electronic media will always require an audit trail, in accordance with 21 CFR 11.10(e). Documentation should include who made the changes, when, and why they were made.

I. The FDA may inspect all records that are intended to support submissions to the Agency, regardless of how they were created or maintained.

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

K. Computerized systems should be designed: (1) So that all requirements assigned to these systems in a study protocol are satisfied (e.g., data are recorded in metric units, requirements that the study be blinded); and, (2) to preclude errors in data creation, modification, maintenance, archiving, retrieval, or transmission.

L. Security measures should be in place to prevent unauthorized access to the data and to the computerized system.

## IV. STANDARD OPERATING PROCEDURES

Standard Operating Procedures (SOPs) pertinent to the use of the computerized system should be available on site.

SOPs should be established for, but not limited to:

- System Setup/Installation
- Data Collection and Handling
- System Maintenance
- Data Backup, Recovery, and Contingency Plans
- Security
- Change Control

## V. DATA ENTRY

A. Electronic Signatures

1. To ensure that individuals have the authority to proceed with data entry, the data entry system should be designed so that individuals need to enter electronic signatures, such as combined identification codes/passwords or biometric-based electronic signatures, at the start of a data entry session.

2. The data entry system should also be designed to ensure attributability. Therefore, each entry to an electronic record, including any change, should be made under the electronic signature of the individual making that entry. However, this does not necessarily mean a separate electronic signature for each entry or change. For example, a single electronic signature may cover multiple entries or changes.

    a. The printed name of the individual who enters data should be displayed by 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 by 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. Individuals should only work under their own passwords or other access keys and should not share these with others. Individuals should not log on to the system in order to provide another person access to the system.

4. Passwords or other access keys should be changed at established 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, there should be some kind of automatic protection against unauthorized data entry. An example could be an automatic screen saver that prevents data entry until a password is entered.

B. Audit Trails

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

   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. A record is created when it is saved to durable media, as described under "commit" in Section II, Definitions.

   b. Audit trails 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. Clinical investigators should retain either the original or a certified copy of audit trails.

4. FDA personnel should be able to read audit trails both at the study site

and at any other location where associated electronic study records are maintained.

5. Audit trails 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 the system's date and time are correct.

2. 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.

3. Dates and times are to 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.

4. Clinical study computerized systems will likely be used in multi-center trials, perhaps located in different time zones. Calculation of the local time stamp may be derived in such cases from a remote server located in a different time zone.

## VI. SYSTEM FEATURES

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

1. Prompts, flags, or other help features within the computerized system should be used to encourage consistent use of clinical terminology and to alert the user to data that are out of acceptable range. Features that automatically enter data into a field when that field is bypassed should not be used.

2. Electronic patient diaries and 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 unexpected result. 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, as documented in the audit trail.

C. Retrieval of Data

1. Recognizing that computer products may be discontinued or supplanted by newer (possibly incompatible) systems, it is nonetheless vital that sponsors retain the ability to retrieve and review the data recorded by the older systems. This may be achieved by maintaining support for the older systems or transcribing data to the newer systems.

2. When migrating to newer systems, it is important to generate accurate and complete copies of study data and collateral information relevant to data integrity. This information would include, for example, audit trails and computational methods used to derive the data. Any data retrieval software, script, or query logic used for the purpose of manipulating, querying, or extracting data for report generating purposes should be documented and maintained for the life of the report. The transcription process needs to be validated.

D. Reconstruction of Study

FDA expects to be able to reconstruct a study. This applies not only to the data, but also how the data were obtained or managed. Therefore, all versions of application software, operating systems, and software development tools involved in processing of data or records should be available as long as data or records associated with these versions are required to be retained. Sponsors may retain these themselves or may contract for the vendors to retain the ability to run (but not necessarily support) the software. Although FDA expects sponsors or vendors to retain the ability to run older versions of software, the agency acknowledges that, in some cases, it will be difficult for sponsors and vendors to run older computerized systems.

## 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 computerized system and to the data is restricted to authorized personnel.

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

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

B. Logical Security

1. Access to the data at the clinical site should be restricted and monitored 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. There should be a cumulative record that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges. The record should be in the study documentation accessible at the site.

3. If a sponsor supplies computerized systems exclusively for clinical trials, the systems should remain dedicated to the purpose for which they were intended and validated.

4. If a computerized system being used for the clinical study is part of a system normally used for other purposes, efforts should be made to ensure that the study software is logically and physically isolated as necessary to preclude unintended interaction with non-study software. If any of the software programs are changed the system should be evaluated to determine the effect of the changes on logical security.

5. Controls should be in place to prevent, detect, and mitigate effects of computer viruses on study data and software.

## VIII. SYSTEM DEPENDABILITY

The sponsor should ensure and document that computerized systems conform to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance.

A. Systems documentation should be readily available at the site where clinical trials are conducted. Such documentation should provide an overall description of computerized systems and the relationship of hardware, software, and physical environment.

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

1. For 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 (either original validation documents or on-site vendor audit documents) of this design level validation by the vendor, and should have itself performed functional testing (e.g., by use of test data sets) and researched known software limitations, problems, and defect corrections.

   In the special case of database and spreadsheet software that is (1) purchased off-the-shelf, (2) designed for and widely used for general purposes, (3) unmodified, and (4) 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 should have itself 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 includes:

   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; and,

c. Test results and an evaluation of how these results demonstrate that the predetermined design specification has been met.

C. 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 maintain the integrity of the data or the integrity of protocols.

2. The impact of any change to the system should be evaluated and a decision made regarding the need to revalidate. Revalidation should be performed for changes that exceed operational limits or design specifications.

3. All changes to the system should be documented.

## 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 continuing the study by alternate means in the event of failure of the computerized system.

C. Backup and Recovery of Electronic Records

1. Backup and recovery procedures should be clearly outlined in the SOPs and be sufficient to protect against data loss. Records should be backed up regularly in a way that would prevent a catastrophic loss and ensure the quality and integrity of the data.

2. Backup records should be stored at a secure location specified in the SOPs. Storage is typically offsite or in a building separate from the original records.

3. Backup and recovery logs should be maintained to facilitate an assessment of the nature and scope of 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.

C. Documentation

Employee education, training, and experience should be documented.

## XI. RECORDS INSPECTION

A. FDA may inspect all records that are intended to 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 Agency 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

As required by 21 CFR 11.100(c), persons using electronic signatures to meet an FDA signature requirement shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

As set forth in 21 CFR 11.100(c), the certification shall 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. 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. An acceptable certification may take the following form:

> "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."

## XIII. REFERENCES


FDA, *Software Development Activities,* 1987.

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

FDA, *Guidance for Industry: Good Target Animal Practices: Clinical Investigators and Monitors,* 1997.

FDA, *Compliance Program Guidance Manual,* "Compliance Program 7348.810 - Sponsors, Contract Research Organizations and Monitors," October 30, 1998.

FDA, *Compliance Program Guidance Manual,* "Compliance Program 7348.811 - Bioresearch Monitoring - Clinical Investigators," September 2, 1998.

FDA, *Information Sheets for Institutional Review Boards and Clinical Investigators*, 1998.

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

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

FDA, *[draft] Guidance for Industry: General Principles of Software Validation*, draft 1997.

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