Guidance for Industry

Computerized Systems Used in Clinical Investigations

U.S. Department of Health and Human Services
Food and Drug Administration (FDA)
Office of the Commissioner (OC)
May 2007

Contains Nonbinding Recommendations

Guidance for Industry
Computerized Systems Used in Clinical Investigations

Additional copies are available from:

Office of Training and Communication
Division of Drug Information
Center for Drug Evaluation and Research (CDER)
(Tel) 301-827-4573
http://www.fda.gov/cder/guidance/index.htm
or
Office of Communication, Training and
Manufacturers Assistance
Center for Biologics Evaluation and Research
http://www.fda.gov/cber/guidelines.htm
(Tel) 800-835-4709 or 301-827-1800
or
Office of Communication, Education, and Radiation Programs
Division of Small Manufacturers, International, and Consumer Assistance
Center for Devices and Radiological Health
http://www.fda.gov/cdrh/ggpmain.html
Email: dsmica@fda.hhs.gov
Fax: 240.276.3151
(Tel) Manufacturers and International Assistance: 800.638.2041 or 240.276.3150
or
Office of Food Additive Safety
Center for Food, Safety and Applied Nutrition
(Tel) 301-436-1200
http://www.cfsan.fda.gov/guidance.html
or
Communications Staff, HFV-12
Center for Veterinary Medicine
(Tel) 240-276-9300
http://www.fda.gov/cvm/guidance/published
or
Good Clinical Practice Programs
Office of the Commissioner

U.S. Department of Health and Human Services
Food and Drug Administration
Office of the Commissioner (OC)
May 2007

TABLE OF CONTENTS

Guidance for Industry[1]
Computerized Systems Used in Clinical Investigations

I. INTRODUCTION

This document provides to sponsors, contract research organizations (CROs), data management centers, clinical investigators, and institutional review boards (IRBs), recommendations regarding the use of computerized systems in clinical investigations. The computerized system applies to 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. Because the source data[2] are necessary for the reconstruction and evaluation of the study to determine the safety of food and color additives and safety and effectiveness of new human and animal drugs,[3] and medical devices, this guidance is intended to assist in ensuring confidence in the reliability, quality, and integrity of electronic source data and source documentation (i.e., electronic records).

This guidance supersedes the guidance of the same name dated April 1999; and supplements the guidance for industry on *Part 11, Electronic Records; Electronic Signatures — Scope and Application* and the Agency's international harmonization efforts[4] when applying these guidances to source data generated at clinical study sites.

---

[1] This guidance has been prepared by the Office of Critical Path Programs, the Good Clinical Practice Program, and the Office of Regulatory Affairs in cooperation with Bioresearch Monitoring Program Managers for each Center within the Food and Drug Administration.

[2] Under 21 CFR 312.62(b), reference is made to records that are part of case histories as "supporting data"; the ICH *E6 Good Clinical Practice* consolidated guidance uses the term "source documents." For the purpose of this guidance, these terms describe the same information and have been used interchangeably.

[3] Human drugs include biological drugs.

[4] In August 2003, FDA issued the guidance for industry entitled *Part 11, Electronic Records; Electronic Signatures-Scope and Application* clarifying that the Agency intends to interpret the scope of part 11 narrowly and to exercise enforcement discretion with regard to part 11 requirements for validation, audit trails, record retention, and record copying. In 1996, the International Conference on Harmonisation of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH) issued *E6 Good Clinical Practice: Consolidated Guidance.*

FDA's guidance documents, including this guidance, do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word *should* in Agency guidances means that something is suggested or recommended, but not required.

II. BACKGROUND

There is an increasing use of computerized systems in clinical trials to generate and maintain source data and source documentation on each clinical trial subject. Such electronic source data and source documentation must meet the same fundamental elements of data quality (e.g., attributable, legible, contemporaneous, original,[5] and accurate) that are expected of paper records and must comply with all applicable statutory and regulatory requirements. FDA's acceptance of data from clinical trials for decision-making purposes depends on FDA's ability to verify the quality and integrity of the data during FDA on-site inspections and audits. (21 CFR 312, 511.1(b), and 812).

In March 1997, FDA issued 21 CFR part 11, which provides criteria for acceptance by FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. After the effective date of 21 CFR part 11, significant concerns regarding the interpretation and implementation of part 11 were raised by both FDA and industry. As a result, we decided to reexamine 21 CFR part 11 with the possibility of proposing additional rulemaking, and exercising enforcement discretion regarding enforcement of certain part 11 requirements in the interim.

This guidance finalizes the draft guidance for industry entitled *Computerized Systems Used in Clinical Trials,* dated September 2004 and supplements the guidance for industry entitled *Part 11, Electronic Records; Electronic Signatures – Scope and Application* (Scope and Application Guidance), dated August 2003. The Scope and Application Guidance clarified that the Agency intends to interpret the scope of part 11 narrowly and to exercise enforcement discretion with regard to part 11 requirements for validation, audit trails, record retention, and record copying. However, other Part 11 provisions remain in effect.

The approach outlined in the Scope and Application Guidance, which applies to electronic records generated as part of a clinical trial, should be followed until such time as Part 11 is amended.

[5] FDA is allowing original documents to be replaced by copies provided the copies are identical and have been verified as such (See, e.g., FDA Compliance Policy Guide # 7150.13). See Definitions section for a definition of original data.

III. SCOPE

The principles outlined in this guidance should be used for computerized systems that contain any data that are relied on by an applicant in support of a marketing application, including computerized laboratory information management systems that capture analytical results of tests conducted during a clinical trial. For example, the recommendations in this guidance would apply to computerized systems that create source documents (electronic records) that satisfy the requirements in 21 CFR 312.62(b) and 812.140(b), such as case histories. This guidance also applies to recorded source data transmitted from automated instruments directly to a computerized system (e.g., data from a chemistry autoanalyser or a Holter monitor to a laboratory information system). This guidance also applies when source documentation is created in hardcopy and later entered into a computerized system, recorded by direct entry into a computerized system, or automatically recorded by a computerized system (e.g., an ECG reading). The guidance does not apply to computerized medical devices that generate such data and that are otherwise regulated by FDA.

IV. RECOMMENDATIONS

This guidance provides the following recommendations regarding the use of computerized systems in clinical investigations.

A. Study Protocols

Each specific study protocol should identify each step at which a computerized system will be used to create, modify, maintain, archive, retrieve, or transmit source data. This information can be included in the protocol at the time the investigational new drug application (IND), Investigational Device Exemption (IDE), or Notice of Claimed Investigational Exemption for a New Animal Drug containing the protocols is submitted or at any time after the initial submission.

The computerized systems should be designed: (1) to satisfy the processes assigned to these systems for use in the specific study protocol (e.g., record data in metric units, blind the study), and (2) to prevent errors in data creation, modification, maintenance, archiving, retrieval, or transmission (e.g., inadvertently unblinding a study).

B. Standard Operating Procedures

There should be specific procedures and controls in place when using computerized systems to create, modify, maintain, or transmit electronic records, including when collecting source data at clinical trial sites. A list of recommended standard operating procedures (SOPs) is provided in Appendix A. Such SOPs should be maintained either on-site or be remotely accessible through electronic files as part of the specific study records, and the SOPs should be made available for use by personnel and for inspection by FDA.

C. Source Documentation and 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 part 312, § 511.1(b), and part 812, for a period of time specified in these regulations. This requirement applies to the retention of the original source document, or a copy of the source document.

When source data are transmitted from one system to another (e.g., from a personal data assistant to a sponsor's server), or entered directly into a remote computerized system (e.g., data are entered into a remote server via a computer terminal that is located at the clinical site), or an electrocardiogram at the clinical site is transmitted to the sponsor's computerized system, a copy of the data should be maintained at another location, typically at the clinical site but possibly at some other designated site. Copies should be made contemporaneously with data entry and should be preserved in an appropriate format, such as XML, PDF or paper formats.

D. Internal Security Safeguards

1. Limited Access

Access must be limited to authorized individuals (21 CFR 11.10(d). This requirement can be accomplished by the following recommendations. We recommend that each user of the system have an individual account. The user should log into that account at the beginning of a data entry session, input information (including changes) on the electronic record, and log out at the completion of data entry session. The system should be designed to limit the number of log-in attempts and to record unauthorized access log-in attempts.

Individuals should work only under their own password or other access key and not share these with others. The system should not allow an individual to log onto the system to provide another person access to the system. We also recommend that passwords or other access keys be changed at established intervals commensurate with a documented risk assessment.

When someone leaves a workstation, the person should log off the system. Alternatively, an automatic log off may be appropriate for long idle periods. For short periods of inactivity, we recommend that a type of automatic protection be installed against unauthorized data entry (e.g., an automatic screen saver can prevent data entry until a password is entered).

2. Audit Trails

It is important to keep track of all changes made to information in the electronic records that document activities related to the conduct of the trial (audit trails). The use of audit trails or other security measures helps to ensure that only authorized additions, deletions, or alterations of information in the electronic record have occurred and allows a means to reconstruct significant details about study conduct and source data collection necessary to verify the quality and integrity of data. Computer-generated, time-stamped audit trails or other security measures can

also capture information related to the creation, modification, or deletion of electronic records and may be useful to ensure compliance with the appropriate regulation.

The need for audit trails should be determined based on a justified and documented risk assessment that takes into consideration circumstances surrounding system use, the likelihood that information might be compromised, and any system vulnerabilities. Should it be decided that audit trails or other appropriate security measures are needed to ensure electronic record integrity, personnel who create, modify, or delete electronic records should not be able to modify the documents or security measures used to track electronic record changes. 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. Original information should not be obscured though the use of audit trails or other security measures used to capture electronic record activities.

3. Date/Time Stamps

Controls should be established to ensure that the system's date and time are correct. 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. Any changes to date or time should always be documented. We do not expect documentation of time changes that systems make automatically to adjust to daylight savings time conventions.

We recommend that dates and times include the year, month, day, hour, and minute and encourage synchronization of systems to the date and time provided by international standard-setting agencies (e.g., U.S. National Institute of Standards and Technology provides information about universal time, coordinated (UTC)).

Computerized systems are likely to be used in multi-center clinical trials and may be located in different time zones. For systems that span different time zones, it is better to implement time stamps with a clear understanding of the time zone reference used. We recommend that system documentation explain time zone references as well as zone acronyms or other naming conventions.

E. External Security Safeguards

In addition to internal safeguards built into a computerized system, external safeguards should be put in place to ensure that access to the computerized system and to the data is restricted to authorized personnel. Staff should be kept thoroughly aware of system security measures and the importance of limiting access to authorized personnel.

Procedures and controls should be put in place to prevent the altering, browsing, querying, or reporting of data via external software applications that do not enter through the protective system software.

You should 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.

We also recommend that controls be implemented to prevent, detect, and mitigate effects of computer viruses, worms, or other potentially harmful software code on study data and software.

F. Other System Features

1. Direct Entry of Data

We recommend that you incorporate prompts, flags, or other help features into your computerized system to encourage consistent use of clinical terminology and to alert the user to data that are out of acceptable range. You should not use programming features that automatically enter data into a field when the field is bypassed (default entries). However, you can use programming features that permit repopulation of information specific to the subject. To avoid falsification of data, you should perform a careful analysis in deciding whether and when to use software programming instructions that permit data fields to be automatically populated.

2. Retrieving Data

The computerized system should be designed in such a way that retrieved data regarding each individual subject in a study is attributable to that subject. Reconstruction of the source documentation is essential to FDA's review of the clinical study submitted to the Agency. Therefore, 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.

It is not necessary to reprocess data from a study that can be fully reconstructed from available documentation. Therefore, the actual application software, operating systems, and software development tools involved in the processing of data or records need not be retained.

3. Dependability System Documentation

For each study, documentation should identify what software and hardware will be used to create, modify, maintain, archive, retrieve, or transmit clinical data. Although it need not be submitted to FDA, this documentation should be retained as part of the study records and be available for inspection by FDA (either on-site or remotely accessible).

4. System Controls

When electronic formats are the only ones used to create and preserve electronic records, sufficient backup and recovery procedures should be designed to protect against data loss. Records should regularly be backed up in a procedure that would prevent a catastrophic loss and ensure the quality and integrity of the data. Records should be stored at a secure location

specified in the SOP. Storage should typically be offsite or in a building separate from the original records.

We recommend that you maintain backup and recovery logs to facilitate an assessment of the nature and scope of data loss resulting from a system failure.

5. Change Controls

The integrity of the data and the integrity of the protocols should be maintained when making changes to the computerized system, such as software upgrades, including security and performance patches, equipment, or component replacement, or new instrumentation. The effects of any changes to the system should be evaluated and some should be validated depending on risk. Changes that exceed previously established operational limits or design specifications should be validated. Finally, all changes to the system should be documented.

G. Training of Personnel

Those who use computerized systems must determine that individuals (e.g., employees, contractors) who develop, maintain, or use computerized systems have the education, training and experience necessary to perform their assigned tasks (21 CFR 11.10(i)).

Training should be provided to individuals in the specific operations with regard to computerized systems that they are to perform. 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.

We recommend that computer education, training, and experience be documented.

DEFINITIONS

The following is a list of definitions for terms used in, and for the purposes of, this guidance document.

Audit Trail: For the purpose of this guidance, an *audit trail* is a process that captures details such as additions, deletions, or alterations of information in an electronic record without obliterating the original record. An audit trail facilitates the reconstruction of the course of such details relating to the electronic record.

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

Computerized System: A *computerized system* includes 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: *Direct entry* is recording data where an electronic record is the original means of capturing the data. Examples are the keying by an individual of original observations into a system, or automatic recording by the system of the output of a balance that measures subject's body weight.

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

Original data: For the purpose of this guidance, *original data* are those values that represent the first recording of study data. FDA is allowing original documents and the original data recorded on those documents to be replaced by copies provided the copies are identical and have been verified as such (see FDA Compliance Policy Guide # 7150.13).

Source Documents: 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 a clinical trial.

Transmit: *Transmit* is to transfer data within or among clinical study sites, contract research organizations, data management centers, sponsors, or to FDA.

REFERENCES

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

FDA, *Compliance Program Guidance Manual,* "Compliance Program 7348.810 – Bioresearch Monitoring - Sponsors, Contract Research Organizations and Monitors," February 21, 2001.

FDA, *Compliance Program Guidance Manual*, "Compliance Program 7348.811 - Bioresearch Monitoring - Clinical Investigators," September 30, 2000.

FDA, *Good Clinical Practice VICH GL9.*

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

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

http://www.fda.gov/ic/ohrt/irbs/default.htm

FDA, *E6 Good Clinical Practice: Consolidated Guidance*. http://www.fda.gov/cder/guidance/959fnl.pdf.

FDA, *Part 11, Electronic Records; Electronic Signatures — Scope and Application,* 2003.

FDA, *General Principles of Software Validation; Guidance for Industry and FDA Staff*.

APPENDIX A

STANDARD OPERATING PROCEDURES

Standard operating procedures (SOPs) and documentation pertinent to the use of a computerized system should be made available for use by appropriate study personnel at the clinical site or remotely and for inspection by FDA. The SOPs should include, but are not limited to, the following processes.

- System setup/installation (including the description and specific use of software, hardware, and physical environment and the relationship)
- System operating manual
- Validation and functionality testing
- Data collection and handling (including data archiving, audit trails, and risk assessment)
- System maintenance (including system decommissioning)
- System security measures
- Change control
- Data backup, recovery, and contingency plans
- Alternative recording methods (in the case of system unavailability)
- Computer user training
- Roles and responsibilities of sponsors, clinical sites and other parties with respect to the use of computerized systems in the clinical trials