



SOCIETY FOR CLINICAL DATA MANAGEMENT, INC.

Dockets Management Branch
Food & Drug Administration
HFA-305
5630 Fishers Lane
Room 1061
Rockville, MD 20852

December 29, 2004

Reference: Docket Number 2004D-0440

Dear Sir/Madam:

The Society for Clinical Data Management (SCDM) is pleased to submit the attached Comment Document on the September 29, 2004 issued Draft Guidance for Industry: Computerized Systems Used in Clinical Trials. SCDM represents over 1200 data management professionals from all facets of the drug development process. Members represent pharmaceutical, biotechnology, device, contract research, academic research, and technology organizations. This comment document also represents comments submitted by our colleagues in the Data Management and Biomedical (DMB) Society, which represent data management professionals in France. As the majority of the work that our members perform is affected by this guidance document, the SCDM board of trustees felt that our collective comments were necessary. This was felt to be especially important as clinical trials are being conducted more and more frequently with technically advanced systems.

The overall SCDM body feels that the finalization of this guidance document should NOT take place until the tenets of 21 CFR Part 11 have been addressed with more specificity by the agency. SCDM notes the continual reference to enforcement discretion and the various sections of Part 11 throughout this draft guidance document and, as such, makes it difficult to determine how to respond. With this discretion, it is difficult to determine the specific actions to take in ensuring compliant, qualified, and secured systems for clinical data collection.

SCDM looks forward to the agency's response to these comments and is prepared to answer any questions that might come as a result of your review. We look forward to an open dialogue toward seeking concurrence on methods to assure the collection of quality data that will help to improve the lives of patients.

Sincerely,

Jonathan R. Andrus, M.S., CQA
Chair, SCDM Comments Committee
Vice President, Quality Assurance & Compliance
Phoenix Data Systems, Inc.
Phone: 484.928.6034
Email: jandrus@pdsedc.com

2004D-0440

CR

I. Introduction

Line Number(s)	Comment
18 – 19: This document provides guidance about computerized systems that are used to create, modify, maintain, archive, retrieve, or transmit clinical data required to be maintained and/or submitted.....	Not sure that 'maintain' and 'archive' should be included on this list. It's not clear that the same stringent requirements should be in place for systems that just perform these functions (maintain/archive). This comment applies to all usage of the terms 'maintain' and 'archive.'

II. Background

Line Number(s)	Comment
65-67: The principles in this guidance may be applied where supporting data or source documents 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.	Please clarify whether or not this section applies to data that are created / measured by a medical device. Does it matter if the medical device, including it's software, is approved under a 510k and used in accordance with it's "labeling"?
65-67	Please clarify whether or not this section applies to data that are created through ECG carts at a site. Site's ECG carts and central ECG management systems that generate the ECG waveform files for RDA submissions have not been "validated" by Sponsors. They are, however, approved medical devices.
65-67	Please clarify whether or not this section applies to data that are extracted from a site's electronic medical record.

III. General Principles

Line Number(s)	Comment
<p>76-77: We recommend that each study protocol identify at which steps a computerized system will be used to create, modify, maintain, archive, retrieve, or transmit data.</p>	<p>Are you speaking about the official investigational protocol used for the conduct of the trial? If so, this information is often not known at the time the protocol is finalized. Often, within the realm of data management, additional study related documents are developed in the form of a data management plan to address these particular topics.</p>
<p>78-81: For each study we recommend that documentation identify what software and hardware are to be used in computerized systems that create, modify, maintain, archive, retrieve, or transmit data. We also recommend that this documentation be retained as part of the study records.</p>	<p>This information is an additional requirement and burden. Since this information is fairly consistent from trial to trial within an organization, we feel that this guidance document should drop the reference to study specific documentation and the agency encourage the sponsor organization to make the documentation available upon request and focus this text on system level documentation and not study level documentation.</p>
<p>89-96: Under 21 CFR 312.62, 511.1(b)(7)(ii) and 812.140, the clinical investigator must retain records required to be under part 312, § 511.1(b) and § 812, respectively, for a period of time specified in these regulations. Retaining the original source document or a certified copy of the source document at the site where the investigation was conducted can assist in meeting these regulatory</p>	<p>There is much debate in the industry regarding web-based systems and the statement "Retaining the original source document or a certified copy of the source document at the site where the investigation was conducted can assist in meeting these regulatory requirements." Please confirm that a web-based EDC system where a site enters data over the web and the database is</p>

<p>requirements. It can also assist in the reconstruction and evaluation of the trial throughout and after the completion of the trial. When original observations are entered directly into a computerized system, the electronic record is the source document.</p>	<p>stored on a server in a different location is acceptable provided that the site has access to their data via the web during the trial, and receives a copy of their data on a CD that they can view in multiple software at the close of the trial. Does the Agencies view change for Patient reported outcomes data, or data where the EDC system is the source?</p>
<p>91-93</p>	<p>Please clarify what is meant by 'certified copy'. Is this clinical data only? Audit trails? Design documentation as suggested on lines 196-198? Define what is necessary, from a documentation standpoint, at the site at the start, during and at the conclusion of a study.</p>
<p>95-96</p>	<p>What about data collected from a blood pressure monitoring system, pH meter, or heart rate monitor where a small tear strip paper may be produced?</p>
<p>101-104: An audit trail that is electronic or consists of other physical, logical, or procedural security measures to ensure that only authorized additions, deletions, or alterations of information in the electronic record have occurred may be needed to facilitate compliance with applicable records regulations.</p>	<p>Please confirm that systems that create (write records) and do not allow updates, deletions, or changes in any way to existing data do not require an audit trail.</p>
<p>107-109: We recommend that audit trails or other security methods used to capture electronic record activities document who made the changes, when, and why changes</p>	<p>Audit trails at the record or field level?</p>

<p>were made to the electronic record.</p>	
<p>107-109</p>	<p>Reason for change is not a Part 11 requirement and should not be included in this guidance document. Consistency with the Scope and Application Guidance implies narrowing the Scope, not broadening it. The part 11 requirement states: “Use of <u>secure, computer-generated, time-stamped</u> audit trails to <u>independently record</u> the date and time of operator entries and <u>actions that create, modify, or delete electronic records</u>. Record changes shall not obscure previously recorded information.... hold <u>individual</u> accountable and responsible for actions initiated under their electronic signatures”</p>
<p>112-114: To ensure the authenticity and integrity of electronic records, it is important that security measures be in place to prevent unauthorized access to the data in the electronic record and to the computerized system.</p>	<p>There is a need for some definition about what is meant by ‘security measures.’</p>

IV. Overall Approach to Meeting Part 11 Requirements

Line Number(s)	Comment
<p>121-123: That is, FDA does not intend to take enforcement action to enforce compliance with these requirements of part 11 while the agency reexamines part 11.</p>	<p>Please clarify. This section seems to say that 21 CFR Part 11 is still in place but will not be enforced.</p>

V. Standard Operating Procedures

Line Number(s)	Comment
-----------------------	----------------

<p>137-146: We recommend that standard operating procedures (SOPs) pertinent to the use of the computerized system be available on site. We recommend that SOPs be established for the following:</p> <ul style="list-style-type: none"> • System Setup/Installation • Data Collection and Handling • System Maintenance • Data Backup, Recovery, and Contingency Plans • Security • Change Control • Alternative Recording Methods (in the case of system unavailability) 	<p>Please distinguish between SOPs recommended for Data Centers (Sponsors) and Clinical Investigational Sites.</p>
<p>137-146</p>	<p>Additions to this list should be:</p> <ul style="list-style-type: none"> - user training - site selection criteria

VI. Data Entry

Line Number(s)	Comment
<p>159-166: Therefore, we recommend that each user of the system have an individual account into which the user logs-in at the beginning of a data entry session, inputs information (including changes) on the electronic record, and logs out at the completion of data entry session.</p> <p>We recommend that individuals work only under their own password or other access key and not share these with others. We</p>	<p>The guidance should be more insistent on the need for individual accounts. The use of the term "must," should be considered.</p>

<p>recommend that individuals not be allowed 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.</p>	
<p>185-187: Computer-generated, time-stamped audit trails or information related to the creation, modification, or deletion of electronic records may be useful to ensure compliance with the appropriate predicate rule.</p>	<p>It would be useful to define when data are created. For example: Data may be created when it is first created (keyed) or data may be created when it is validated (when the investigator clicks on the submit button at the end of a page committing data keyed into the database).</p>
<p>196-198: To facilitate FDA's inspection of this information, we recommend that clinical investigators retain either the original or a certified copy of any documentation created to track electronic records activities.</p>	<p>Copies of the full audit trail for a large project may be unmanageable. This suggestion may make more sense if it called on Sponsors and vendors to be able to recreate the audit trail from archive in the event of an audit. Systems handle audit trails differently, dependent on the way that the audit trail is captured within the system (whether at the form or data field level), will determine the performance and optimization of the deliverable.</p>
<p>213-215: We recommend that audit trails or other security methods used to capture electronic record activities document who made the changes, when, and why changes were made to the electronic record.</p>	<p>Remove reason for change, it is not a part 11 requirement.</p>
<p>220-224: Signed and dated printed versions of electronic records that identify what,</p>	<p>The guidance provided in this section is in need of further clarification. Upon reading</p>

<p>when, and by whom changes were made to the electronic record. When using this method, it is important that appropriate controls be utilized that ensure the accuracy of these records (e.g., sight verification that the printed version accurately captures all of the changes made to the electronic record).</p>	<p>this section, it is unclear to SCDM as to what FDA is recommending with respect to electronic records.</p>
<p>225–227: Signed and dated printed standard electronic file formatted versions (e.g., pdf, xml or sgml) of electronic records that identify what, when, and by whom changes were made to the electronic record.</p>	<p>This section can be interpreted in two ways.</p> <ol style="list-style-type: none"> 1) Are you recommending that personnel print out electronic records and make handwritten changes? 2) Are you asking sponsors to print out the full audit trail? <p>Exactly how should the audit trail be displayed? Final screen representation? All combined in one representation for each page of data? At what level (record/data field) should the audit trail be displayed?</p>
<p>233–245: We recommend that controls be put in place 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. We recommend that someone always document changes to date or time. We do not expect documentation of time changes that systems make automatically to adjust to daylight savings time conventions.</p> <p>We also recommend that dates and times</p>	<p>What about monitors/clinical research associates who travel and have individual clinical study databases on their laptops where they might enter queries or other relevant review related data in varying timezones? Should they be procedurally instructed to make timezone changes?</p>

<p>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.</p> <p>Clinical study computerized systems are likely be used in multi-center 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.</p>	
---	--

VII. System Features

Line Number(s)	Comment
<p>256 – 259: We recommend that prompts, flags, or other help features be incorporated into the computerized system to encourage consistent use of clinical terminology and to alert the user to data that are out of acceptable range. We recommend against the use of features that automatically enter data into a field when the field is bypassed.</p>	<p>What about fields that are populated but still require the user to tab through the field before the field is populated so that they can see that it was a derived data value?</p>
<p>256-259</p>	<p>What about electronic case report form translation when the clinical trial is not performed in the investigator's native language?</p>
<p>279 – 280: Therefore, actual application</p>	<p>Operation should read "operating."</p>

software, operation systems, and software development tools involved in processing of data or records do not need to be retained.	
---	--

VIII. System Security

Line Number(s)	Comment
287-289: We recommend that staff be kept thoroughly aware of system security measures and the importance of limiting access to authorized personnel.	Who is responsible for ensuring that staff be thoroughly aware of system security measures? The sponsor or the site?
291-292: SOPs should be developed and implemented for handling and storing the system to prevent unauthorized access.	Who is responsible for developing these procedures?
303-305: We recommend that procedures and controls be implemented to prevent the data from being altered, browsed, queried, or reported via external software applications that do not enter through the protective system software.	If possible, please distinguish between the varying phases of data collection to data analysis, and when these controls need to be applied.
311-317: If a sponsor supplies computerized systems exclusively for clinical trials, we recommend that the systems remain dedicated to the purpose for which they were intended and validated. If a computerized system being used for a clinical study is part of a system normally used for other purposes, we recommend that efforts be made to ensure that the study software be logically and physically isolated as necessary to preclude unintended interaction with non-study software. If any of the software	Note should be provided here to distinguish EDC systems that make use of web browsers or terminal services. This thin-client solution should not require isolation from other normal work functions on that computer.

<p>programs are changed, we recommend that the system be evaluated to determine the effect of the changes on logical security.</p>	
<p>319-320: We 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.</p>	<p>This recommendation may be extended to a suggested SOP for virus protection.</p>
<p>N/A</p>	<p>It is important to emphasize the investigators' computerized system. Especially the distinction between investigators working in a health center (hospital, SMO) and investigators working in "town" (general practitioner, specialist) must be made.</p> <p>Indeed, it is easier to have safe computerized environment for investigators working in a health center. For individual investigators working in town, the clinical study sponsor and the investigator may be linked by a "contract" that specify the use of the investigator's computerized system for the clinical study.</p> <p>It is important to enforce best practices:</p> <ul style="list-style-type: none"> ▪ user ID & password for each user, ▪ use of anti-virus, including periodic virus definition updates

	<ul style="list-style-type: none"> ▪ firewall policies and usage ▪ regular backup (daily, weekly, etc) of “critical” data on separate media stored in a different location ▪ security updates for the operating system ▪ other best practices, as appropriate <p>During the investigators’ training, we suggest to remind him/her that he/she is responsible for the computer and devices used for the study.</p>
--	---

IX. System Dependability

Line Number(s)	Comment
329-331: We recommend that systems documentation be readily available at the site where clinical trials are conducted and provide an overall description of the computerized systems and the relationships among hardware, software, and physical environment	Please define system documentation. List the types of system documentation that you feel should be available at a clinical investigational site for an EDC system. Most sites are provided a training manual with trial specific screen shots and screen by screen instructions, and trial specific work flow.
353-354: Clinical investigators are not generally responsible for validation unless they originated or modified software.	How does this use of validation differ from the definition provided in the back of this document concerning software validation?
410-411: Additional guidance on general software validation principles can be found in FDA’s guidance entitled <i>General Principles of Software Validation; Final Guidance for Industry</i>	Is the reference to the <i>General Principles of Software Validation (GPSV): Final Guidance for Industry and FDA Staff</i> intended to be applied outside of device and radiological areas? If

<i>and FDA Staff.</i>	so, the applicability of this guidance document (GPSV) ought to be expanded to include the Centers for Drug and Biologic Research.
415-422: FDA recommends that written procedures be put in place to ensure that changes to the computerized system, such as software upgrades, including security and performance patches, equipment, or component replacement, or new instrumentation, will maintain the integrity of the data and the integrity of protocols. We recommend that the effects of any changes to the system be evaluated and a decision made regarding whether, and if so, what level of validation activities related to those changes would be appropriate. We recommend that validation be performed for those types of changes that exceed previously established operational limits or design specifications. Finally, we recommend that all changes to the system be documented.	Does this change control documentation need to be kept at the site also?

X. System Controls

Line Number(s)	Comment
NONE	

XI. Training of Personnel

Line Number(s)	Comment

470: We recommend that employee education, training, and experience be documented.	What about site personnel (non-employee) training documentation?
--	--

XII. Copies of Records and Record Inspections

Line Number(s)	Comment
490-492: For example, if you have the ability to search, sort, or trend records, copies given to FDA should provide the same capability if it is reasonable and technically feasible.	Please provide more specific guidance than 'if it is reasonable and technically feasible'. EDC systems are likely to have multiple features – such as automated error checking and conditional field navigation - that are not easy to recreate in a PDF format. It should be clear whether or not the agency expects these to be replicated - especially in cases where the electronic system itself is at the disposal of the inspector.

XIII. Certification of Electronic Signatures

Line Number(s)	Comment
507-513: As set forth in § 11.100(c)(1), the certification must be submitted in paper, 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 can be used to cover all electronic signatures used by persons in a given organization. This certification is created by persons to acknowledge that their	More information about this would be appreciated. Is it the sponsor or vendors' responsibility? Should EDC systems require that it be done before a site is granted access to the system? If a site is not comfortable signing on behalf of all employees, should the signatures be obtained on a user by user basis?

<p>electronic signatures have the same legal significance as their traditional handwritten signatures.</p>	
<p>515-519: Pursuant to Section 11.100 of Title 21 of the Code of Federal Regulations, this is to certify that <u> [name of organization] </u> 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.</p>	<p>When a site investigator marks a check box on a web based EDC CRF next to text "I approve the data as correct for this visit", is that an electronic signature if the EDC system displays the certification statement on the log-on screen?</p>
<p>515-519</p>	<p>Do the user ID's on an audit trail constitute an electronic signature if the employee's organization has appropriately filed the certification statement prior to implementing and using a part 11 compliant system, and the employees/sites have all read and signed a policy that they understand that they are accountable and responsible for their actions under their user ID and password in the system?</p>

Definitions

Line Number(s)	Comment
Not Applicable	Please provide a definition of contemporaneous.
Not Applicable	Please distinguish between open and closed systems.
Not Applicable	Please provide a definition of functional testing.

References

Line Number(s)	Comment
NONE	

General Comments

Line Number(s)	Comment
N/A	We feel that there needs to be clarification with respect to the term organization and that you specify which areas of the guidance document are related to individual sites versus sponsor/CRO organization. There needs to be a designation between sponsor, vendor and site. Perhaps a grid matrix section of the guidance document that outlines all of the required documentation and actions. This grid would be similar to those seen in ICH (e.g. Essential Documents).