



2004D-0440  
Dockets Management Branch (HFA-305)  
Food and Drug Administration  
5630 Fischers Lane, Room 1061  
Rockville, MD 20852

U.S.A.

Basel, December 29, 2004  
Roche Comments on "Draft Guidance for Industry on Computerized Systems Used in Clinical Trials" (docket No 2004D-0440)

Dear Madam, Dear Sir,

On behalf of F. Hoffmann-La Roche Ltd, we would like to thank the FDA for the opportunity to provide comments for the "Draft Guidance for Industry on Computerized Systems Used in Clinical Trials" (docket No 2004D-0440). The comments are attached to this cover letter.

By way of background, Roche is a leading healthcare company with a uniquely broad spectrum of innovative products. Our products and services address prevention, diagnosis and treatment of diseases, thus enhancing well-being and quality of life. The company employs around 65,000 people and sells its products in over 150 countries.

The focus of Roche is not solely the diagnosis and treatment of manifest disease. The integrated healthcare approach is increasingly offering ways of identifying and targeting diseases early, when their damaging effects can still be prevented. Arranged in two operative divisions, our global mission today and tomorrow is to create exceptional added value in healthcare. These two units are Pharmaceuticals and Diagnostics.

Yours sincerely,

F. Hoffmann-La Roche Ltd

Dr. Peter Trindler  
Deputy Head of Global Quality

Dr. Peter Bosshard  
Global Quality Manager

2004D-0440

C 14

**Comment: 1 , Page: 2**

**Line: Footnote 2**

**Current Text:** Part 11 also applies to electronic records submitted to the Agency under the requirements of Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in Agency regulations.

**Suggested Text:** Part 11 also **may apply** to electronic records submitted to the Agency under the requirements of Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in Agency regulations.

**Remarks:** Part 11 should only be applied if both parties agree

## II BACKGROUND

**Comment: 2 , Page: 3**

**Line: 50**

**Current Text:** For example, data should be attributable, legible, contemporaneous, original and accurate.

**Suggested Text:** For example, data should be attributable, legible, contemporaneous and accurate.

**Remarks:** MAJOR! The term original is not applicable here. In electronic environments copies may be difficult to distinguish from the original. So this new requirement would causes costly enhancements and changes to systems, where the original and the copy are identical.

**Page: 3**

**Comment: 3 , Line: Footnote 4**

**Current Text:** 4 FDA is allowing original documents to be replaced by certified copies provided the copies are identical and have been verified as such. (see FDA Compliance Policy Guide # 7130.13). See "Definitions" section for a definition of original data.

**Suggested Text:** REMOVE

**Remarks:** To be consistent with the text above.

**Comment: 4 , Page: 3**

**Line: 66**

**Current Text:** The principles in this guidance may be applied where supporting data or 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.

**Remarks:** There should be reference, which are the originals in either case if the term original is kept (see comment 3 and 4). It should also be possible to destroy a hardcopy after entry into the computer, if it can be show that the hardcopy was correctly moved to the computer (e.g. scanning a hardcopy as \*.PDF or \*.TIF file), as it is already possible for microfilm.

## III GENERAL PRINCIPLES

**Comment: 5 , Page: 4**

**Line: 76/77**

**Current Text:** 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.

**Suggested Text:** - (remove sentence)

**Remarks:** It might not be possible for multi center trials, using central and local labs

and other service providers like IVRS etc. to identify exactly the Soft- and Hardware to be used during a study as long as this requirement or suggestion is not meant to be on a very high and generic level like e.g.: "for randomization purposes we will use an IVRS service provider" etc. The study protocol is maybe the wrong place to describe this information because a study protocol serves as a document describing the purpose of the investigation and how a study is going to be run. Furthermore the content of a study protocol is precisely defined and therefore it could be the wrong document for defining which steps need to be done electronically.

**Comment:** 6 , Page: 4

**Line:** 78/79

**Current Text:** 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.

**Suggested Text:** For each study, we recommend that computerized systems that create, modify, maintain, archive, retrieve, or transmit data are validated and their hardware and software are described.

**Remarks:** Details of Software and hardware may not be known in advance, especially if supported by external partners.

**Comment:** 7 , Page: 4

**Line:** 82-88

**Current Text:** 3. We recommend that computerized systems 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, the study blinded) and (2) to preclude errors in data creation, modification, maintenance, archiving, retrieval, or transmission.

4. It is important to design a computerized system in such a manner so that all applicable regulatory requirements for record keeping and record retention in clinical trials are met with the same degree of confidence as is provided with paper systems.

**Suggested Text:** - (remove sentences)

**Remarks:** This requirement would not be necessary as it is just a repetition and its content is already included in the definition of validation itself: "documented evidence to demonstrate a system is fit for its intended, predefined use".

The term "designed" could be interpreted that these systems only have to be designed to meet compliance and further validation is not needed. If the term "validation" is used in requirement 2 (Lines 78-81) this would include the design implicitly in the definition.

**Comment:** 8 , Page: 4,7

**Line:** 107, 213

**Current Text:** audit trial

**Suggested Text:** audit trail

**Remarks:** misspelling

**Comment:** 9 , Page: 4

**Line:** 101

**Current Text:** 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.

**Suggested Text:** This could be supported by an audit trail or by other measures such as physical, logical, or procedural security solutions 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.

**Remarks:** The definition of an audit trail should not be modified.

**Comment:** 10 , Page: 4

**Line:** 107-109

**Current Text:** 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.

**Suggested Text:** We recommend that an audit trail additionally includes a reason why changes were made to the electronic record, if such changes are not self explanatory.

**Remarks:** The information about who and when changes addition and deletions were made are already part of the audit trail definition in 21 CFR 11.10 (e). It is important that the audit trail may be edited in order to add a reason.

#### IV OVERALL APPROACH TO MEETING PART 11 REQUIREMENTS

**Comment:** 11 , Page:

**Line:** 118 - 129

**Current Text:** As described in the FDA guidance entitled Part 11, Electronic Records; Electronic Signatures- Scope and Application (August 2003), while the re-examination of part 11 is underway, FDA intends to exercise enforcement discretion with respect to part 11 requirements for validation, audit trail, record retention, and record copying. That is, FDA does not intend to take enforcement action to enforce compliance with these requirements of part 11 while the agency re-examines part 11. Note that part 11 remains in effect and that the exercise of enforcement discretion applies only to the extent identified in the FDA guidance on part 11. Also, records must still be maintained or submitted in accordance with the underlying requirements set forth in the Federal Food, Drug, and Cosmetic Act (Act), the Public Health Service Act (PHS Act), and FDA regulations (other than part 11), which are referred to in this guidance document as predicate rules, and FDA can take regulatory action for noncompliance with such predicate rules. Specific details about the Agency's approach to enforcing part 11 can be found in the Part 11 Scope and Application guidance.

**Suggested Text:** The FDA guidance entitled Part 11, Electronic Records; Electronic Signatures- Scope and Application (August 2003) applies. This means enforcement discretion with respect to part 11 requirements for validation, audit trail, record retention, and record copying. The agency recommends consideration of the corresponding predicate rules which include the Federal Food, Drug, and Cosmetic Act, the PHS Act, and regulations governing good clinical practice and human subject protection (21 CFR parts 50, 56, 312, 511, and 812).

**Remarks:** This paragraph can be shortened because a reference to the guideline "Part 11 ... - Scope and Application" should be sufficient.

V STANDARD OPERATING PROCEDURES

Comment: 12 , Page: 5

Line: 137-139

**Current Text:** We recommend that SOPs be established for the following:

**Suggested Text:** We recommend that the following topics should be covered in one ore more SOPs:

**Remarks:** Frequently Change Control and System Maintenance are combined.  
Alternative Recording Methods and contingency are also logically combined.

VI DATA ENTRY

A Computer Access Controls

Comment: 13 , Page: 6

Line: 154

**Current Text:** To ensure that individuals have the authority to proceed with data entry, data entry systems must be designed to limit access so that only authorized individuals are able to input data

**Suggested Text:** To ensure that individuals have the authority to enter data, data entry systems must be designed to limit access so that only authorized individuals are able to input data, modify or delete it.

**Remarks:** Modification and deletion of data should also be foreseen. For records which are the source only the individual inputting the data can modify the data providing a reason for the modification.

Comment: 14 , Page: 6

Line: 159 - 166

**Current Text:** 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.

We recommend that individuals work only under their own password or other access key and not share these with others. We 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.

When someone leaves a workstation, we recommend that the SOP require that person to log off the system. Alternatively, an automatic log off may be appropriate for long idle periods. For short periods of inactivity, we recommend that some kind of automatic protection be installed against unauthorized data entry. An example could be an automatic screen saver that prevents data entry until a password is entered.

**Suggested Text:** Each user of the system should 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 the data entry session.

Individuals should work only under their own password or other access key. Passwords should not be shared with others. Individuals should not log onto the system to provide another person access to the system. Passwords should be changed at established intervals.

When someone leaves a workstation he should log off or a time out or automatic log off may be appropriate for long idle periods. For short periods of inactivity, we recommend that some kind of automatic protection be installed against unauthorized data entry. An example could be an automatic screen saver that prevents data entry until a password is entered.

**Remarks:** The word “recommendation” was considered to be weaker than the term “should”. For these elementary requirements a stronger formulation may be adequate.

**Comment:** 15 , Page: 6

**Line:** 168

**Current Text:** When someone leaves a workstation, we recommend that the SOP require that person to...

**Suggested Text:** When someone leaves a workstation, we recommend that this person ...

**Remarks:** It is not clear which SOP would require the individuals.

**B Audit Trails or other Security Measures**

**Comment:** 16 , Page: 6

**Line:** 176-187

**Current Text:** Section 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. As clarified in the Part 11 Scope and Application guidance, however, the Agency intends to exercise enforcement discretion regarding specific part 11 requirements related to computer-generated, time-stamped audit trails (§ 11.10(e), (k)(2) and any corresponding requirement in § 11.30). Persons must still comply with all applicable predicate rule requirements for clinical trials, including, for example, that records related to the conduct of the study must be adequate and accurate (§§ 312.57, 312.62, and 812.140). It is therefore important to keep track of all changes made to information in the electronic records that document activities related to the conduct of the trial. 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.

**Suggested Text:** Even though Part 11 Scope and Application guidance includes audit trail in the enforcement discretion, persons must still comply with all applicable predicate rule requirements for clinical trials. This includes e.g., that records related to the conduct of the study must be adequate and accurate (§§ 312.57, 312.62, and 812.140).

**Remarks:** Shorter

**Comment:** 17 , Page: 6

**Line:** 191-196

**Current Text:** In order for the Agency to review and copy this information, FDA personnel should be able to review audit trails or other documents that track electronic record activities both at the study site and at any other location where associated electronic study records are maintained. To enable FDA's review, information about the creation, modification, or deletion of electronic records should be created incrementally, and in chronological order.

**Suggested Text:** - (remove sentence)

**Remarks:** This may technically not be achievable using certain database's audit trail

tables. However, it is advisable that the audit trail functionality is described in detail upon an inspection.

**Comment: 18 , Page: 7**

**Line: 202-206**

**Current Text:** We recommend that any decision on whether to apply computer-generated audit trails or other appropriate security measures be based on the need to comply with predicate rule requirements, a justified and documented risk assessment, and a determination of the potential effect on data quality and record integrity. Firms should determine and document the need for audit trails based on a risk assessment that takes into consideration circumstances surrounding system use, the likelihood that information might be compromised, and any system vulnerabilities.

**Suggested Text:** Remove either this one or the “General Principles” Item 7 (Line 97-109)

**Remarks:** Because it is redundant

**Comment: 19 , Page: 7**

**Line: 211-213**

**Current Text:** we recommend that personnel who create, modify, or delete electronic records not be able to modify the documents or security measures used to track electronic record changes. 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.

**Suggested Text:** we recommend that personnel who create, modify, or delete electronic records not be able to modify the “who” and the “when” but should enter a “why” for changes that are not self explanatory.

**Remarks:** The entry of a reason is a modification of the audit trail. Reasons should only be entered if they are meaningful.

**C Date/Time Stamps**

**Comment: 20 , Page: 7**

**Line: 238**

**Current Text:** We also recommend that dates and times include the year, month, day, hour, and minute.

**Suggested Text:** For functionalities like e-signatures and audit trails it might be considered to take also seconds and fragments.

**Remarks:** The time is actually not so important. It is more important that it is possible to find out the sequence in which certain events had happened. In addition it might be considered to recommend that the date should be – as far as technically possible – unambiguous. This means the EU and the US format should be overcome by abbreviating the month with letters. So 12/6 is 12JUN or DEC6. If it is technically not possible for some legacy systems the date format should be specified with the date (MMDD 1206 for Dec 06)

**Comment: 21 , Page: 7**

**Line: 236**

**Current Text:** We do not expect documentation of time changes that systems make automatically to adjust to daylight savings time conventions.

**Suggested Text:** Add: Consider that automatic time changes may lead to data loss because of overwriting. E.g, When the hour is moved one hour back the values of the monitoring data of animal cages may be overwritten for the last hour.

**Remarks:** self explanatory.

**Comment:** 22 , **Page:** 8

**Line:** 242

**Current Text:** 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.

**Suggested Text:** For systems that span different time zones, it is important to see the sequence afterwards. The time zone is not so important, however if used, system documentation should explain time zone references, zone acronyms, location, southern or northern hemisphere, naming conventions, difference to the system time.

**Remarks:** This could be important if daylight savings time might influence a clinical trial for a drug, and hence this needs to be documented.

## VII SYSTEM FEATURES

### A Systems Used for Direct Entry of Data

**Comment:** 23 , **Page:** 8

**Line:** 256-259

**Current Text:** We recommend against the use of features that automatically enter data into a field when the field is bypassed.

**Suggested Text:** We recommend against the use of features that automatically enter data into a field when the field is bypassed, unless the content of the field is self evident.

**Remarks:** It might be beneficial if the system can enter a subject number of a study and the rest of the data is automatically and correctly, filled in automatically and consistently. It is not feasible to enter all the patient details manually each time into each form field.

### B Retrieval of Data and Record Retention

## VIII SYSTEM SECURITY

**Comment:** 24 , **Page:** 9

**Line:** 291 - 299

**Current Text:** SOPs should be developed and implemented for handling and storing the system to prevent unauthorized access. Controlling system access can be accomplished through the following provisions of part 11 that, as discussed in the part 11 guidance, FDA intends to continue to enforce:

- Operational system checks (§ 11.10(f));
- Authority checks (§ 11.10(g));
- Device (e.g., terminal) checks (§ 11.10(h)); and
- The establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures (§ 11.10(j)).

**Suggested Text:** Move. Combine with V Standard Operation Procedures, p 5. line 144.

**Remarks:** Consistency with SOPs

**Comment:** 25 , **Page:** 9

**Line:** 305

**Current Text:** 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.

**Suggested Text:** implemented to prevent the data from being altered via external software applications that do not enter through the protective system software.  
**Remarks:** Browsing, querying or reporting may be required by external applications (sometimes called enhancements) if the basic application does not provide these features. This should be accepted if these external applications are validated (that means there is access control, user procedures etc.)

**Comment:** 26 , Page: 9

**Line:** 307-309

**Current Text:** We recommend that a cumulative record be available that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges. We recommend that the record be kept in the study documentation, accessible at the site.

**Suggested Text:** We recommend that a cumulative record be available that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges, during the normal documentation retention times. ~~We recommend that the record be kept in the study documentation, accessible at the site.~~

**Remarks:** As clinical data may be kept for several years and data may be accessed and processed by different applications at different sites it is impossible to consolidate access information in any point of time down to a study level and report this back to the site where the study was conducted. This would result in a significant amount of redundant "access reports" during the years.

**Comment:** 27 , Page: 9

**Line:** 315-317

**Current Text:** If any of the software programs are changed, we recommend that the system be evaluated to determine the effect of the changes on logical security.

**Suggested Text:** If any of the software programs are changed, we recommend that the system be evaluated to determine the effect of the changes on logical security, based on a risk based approach

**Remarks:** It is not feasible to do this type of evaluation after every small bug fix from Microsoft change or virus update.

## IX SYSTEM DEPENDABILITY

**Comment:** 28 , Page: 9

**Line:** 329

**Current Text:** 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.

**Suggested Text:** 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.

**Remarks:** In multicentre trials this is not feasible

**Comment:** 29 , Page: 10

**Line:** 351

**Current Text:** If validation is required, FDA may ask to see the regulated company's documentation that demonstrates software validation.

**Suggested Text:** If validation is required, FDA may ask to see the regulated company's documentation that demonstrates computerized system validation.  
**Remarks:** Hardware, people and processes should also be included

**Comment:** 30 , **Page:** 10

**Line:** 352

**Current Text:** The study sponsor is responsible for making any such documentation available if requested at the time of inspection at the site where software is used.

**Suggested Text:** The study sponsor is responsible for making any such documentation available if requested at the time of inspection to the inspector (~~at the site where software is used~~).

**Remarks:** Availability of copies of specifically requested documents (e.g. via Fax, scanned copies etc.) should be acceptable during inspections.

#### B Off-the-Shelf Software

**Comment:** 31 , **Page:** 10-11

**Line:** 377 - 383

**Current Text:** While the Agency has announced that it intends to exercise enforcement discretion regarding specific part 11 requirements for validation of computerized systems, persons must still comply with all predicate rule requirements for validation. We suggested in the guidance for industry on part 11 that the impact of computerized systems on the accuracy, reliability, integrity, availability, and authenticity of required records and signatures be considered when you decide whether to validate, and noted that even absent a predicate rule requirement to validate a system, it might still be important to validate in some instances.

**Suggested Text:** -

**Remarks:** There is no enforcement discretion described in the scope and application guideline

**Comment:** 32 , **Page:** 11

**Line:** 285

**Current Text:** design level validation

**Suggested Text:** vendor testing

**Remarks:** Not all software companies perform a formal validation

**Comment:** 33 , **Page:** 11

**Line:** 388

**Current Text:** or on-site vendor audit documents

**Suggested Text:** evidence that a vendor audit was performed

**Remarks:** If the FDA routinely wants to see the vendor audit reports, these reports will be formulated in a way that it is presentable to the FDA. In order to maintain an effective auditing practice and efficient quality assurance principles the FDA should not demand to see the audit documents. If the FDA nevertheless wants to see these documents, it should be possible to send them via fax or e-mail to the inspected site.

**Line:** 385-392

**Current Text:** For most off-the-shelf software, the design level validation will have already been done by the company that wrote the software. Given the importance of ensuring valid clinical trial data,

**Suggested Text:** Specify what design level validation is.  
**Remarks:** Term is not defined in glossary.

**Comment:** 34 , **Page:** 11

**Line:** 404

**Current Text:** A written design specification that describes what the software is intended to do

**Suggested Text:** A written user requirement that describes what the software is intended to do

**Remarks:** User requirement is a more common term.

**Comment:** 35 , **Page:** 11

**Line:** 406

**Current Text:** A written test plan based on the design specification, including both structural and functional analysis

**Suggested Text:** -

**Remarks:** Structural test usually cannot be performed for COTS

**Comment:** 36 , **Page:** 11

**Line:** 409

**Current Text:** ...design specification

**Suggested Text:** User requirements

**Remarks:** See above

C Change Control

**Comment:** 37 , **Page:** 11

**Line:** 419

**Current Text:** ...what level of validation activities...

**Suggested Text:** ...what level of revalidation activities...

**Remarks:** Normally the same or a similar test is re-executed and therefore it is more in use to speak about revalidation.

X SYSTEM CONTROLS

**Comment:** 38 , **Page:** 12

**Line:** 443-444

**Current Text:** When electronic formats are the only ones used to create and preserve electronic records, the Agency recommends that backup and recovery procedures be outlined clearly in SOPs and be sufficient to protect against data loss

**Suggested Text:** When electronic formats are the only ones used to create and preserve electronic records, the Agency recommends that backup and recovery procedures be outlined clearly in SOPs or Service Level agreements and be sufficient to protect against data loss

**Remarks:** If the backup service is outsourced a Service level agreement is more appropriate.

**Comment:** 39 , **Page:** 12

**Line:** 447

**Current Text:** SOPs

**Suggested Text:** SOPs (see chapter SOPs)

**Remarks:** SOPs should be referred only in one place.

## XII COPIES OF RECORDS AND RECORD INSPECTION

Comment: 40 , Page: 13

Line: 493

**Current Text:** FDA expects to inspect, review, and copy records in a human readable form at your site, using your hardware and following your established procedures and techniques for accessing records.

**Suggested Text:** FDA expects to inspect, review, and copy records in a human readable form at your site, using your hard- and software and following your established procedures and techniques for accessing records.

**Remarks:** Software is quite often also necessary to inspect electronic records

## XIII CERTIFICATION OF ELECTRONIC SIGNATURES

Comment: 41 , Page: 13

Line: 500 - 519

**Current Text:** XIII. CERTIFICATION OF ELECTRONIC SIGNATURES

As required by 21 CFR 11.100(c), persons using electronic signatures to meet an FDA signature requirement must, 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 § 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 electronic signatures have the same legal significance as their traditional handwritten signatures. See the following example of a certification statement:

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.

**Suggested Text:** -

**Remarks:** Remove because it is completely redundant with 21 CFR Part 11.

## DEFINITIONS

Comment: 42 , Page: 14

Line: 533-535

**Current Text:** Attributable Data: Attributable data are those that 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.

**Suggested Text:** Attributable Data: Attributable data are those that can be traced to individuals responsible for observing and recording the data. In an automated system, attributability could be achieved by a function designed to identify individuals responsible for any input.

**Remarks:** A function should be sufficient. There is no need to have an individual computer system for this.

Comment: 43 , Page: 14

**Line:** 537-539

**Current Text:** Definition of an audit Trail

**Suggested Text:** Remove

**Remarks:** This is the identical definition as in 21 CFR Part 11.

**Comment:** 44 , **Page:** 14

**Line:** 544

**Current Text:** Computerized system:

**Suggested Text:** include personnel

**Remarks:** Personnel are a very important factor that should also be considered.