

# Interpretation of Regulatory Requirements by Technology Providers

The Case for Electronic Source Data

Stephen A. Raymond and Gerald F. Meyer

The authors contrast two views on the regulations concerning electronic source data.

## Regulations and guidance concerning e-source data

(The authors have italicized words central to the discussion.)

### 21 CFR § 312.62 Investigator recordkeeping and record retention

(a) Disposition of drug. An investigator is required to *maintain* adequate records of the disposition of the drug, including dates, quantity, and use by subjects. If the investigation is terminated, suspended, discontinued, or completed, the investigator shall return the unused supplies of the drug to the sponsor, or otherwise provide for disposition of the unused supplies of the drug under 312.59.

(b) Case histories. An investigator is required to *prepare and maintain* adequate and accurate case histories that record all observations and other data pertinent to the investigation on each individual administered the investigational drug or employed as a control in the investigation. Case histories include the case report forms and supporting data including, for example, signed and dated consent forms and medical records including, for example, progress notes of the physician, the individual's hospital chart(s), and the nurses' notes.

(c) Records retention. An investigator shall *retain* records required to be maintained under this part for a period of 2 years following the date a marketing application is approved for the drug for the indication for which it is being investigated; or, if no application is to be filed or if the application is not approved for such indication, until 2 years after the investigation is discontinued and FDA is notified.

### ICH Guideline for Good Clinical Practice (E6)

Although many constituencies want clinical trials to be accomplished more quickly, the combined actions of three parties determine how well and how quickly clinical trials can be accomplished—sponsors, regulatory agencies, and technology providers. FDA did its part to facilitate development and adoption of technology several years ago. With participation from both sponsors and technology vendors, FDA personnel

developed regulations that were approved and issued on 21 March 1997. These were designed to facilitate the use of computer systems and data processing technology by both sponsors and the FDA.

FDA's intent is stated in the preamble to 21 CFR 11 (The Rule on Electronic Records and Signatures) as follows:

These regulations, which apply to all FDA program areas, are intended to permit the widest

§ 2.10 All clinical trial information should be recorded, handled, and stored in a way that allows its accurate reporting, interpretation, and verification.

§ 2.11 The confidentiality of records that could identify subjects should be protected, respecting the privacy and confidentiality rules in accordance with the applicable regulatory requirement(s).

§ 4.9.4 The investigator/institution should *maintain* the trial documents as specified in Essential Documents for the Conduct of a Clinical Trial (see section 8.) and as required by the applicable regulatory requirement(s). The investigator/institution *should take measures to prevent accidental or premature destruction of these documents.*

§ 4.9.7 Upon request of the monitor, auditor, IRB/IEC, or regulatory authority, the investigator/institution *should make available for direct access* all requested trial-related records.

§6.4.9 [A description of the trial design should include] the identification of any data to be recorded directly on the CFs (i.e. no prior written or electronic record of data) and to be considered to be source data.

§ 8.1 Introduction: ...Trial master files should be established at the beginning of the trial, both at the investigator/institution's site and at the sponsor's office. A final close-out of a trial can only be done when the monitor has reviewed both investigator/institution and sponsor files and confirmed that all necessary documents are in the appropriate files.

Any or all of the documents addressed in this guideline may be subject to, and *should be available for, audit* by the sponsor's auditor and inspection by the regulatory authority(ies).

§ 8.3 During the Clinical Conduct of the Trial "...the following should be added to the files during the trial as evidence that all

possible use of electronic technology....[21 CFR 11 Summary]

The purpose of this rule is to permit the use of a technology that was not contemplated when most existing FDA regulations were written....[21 CFR 11 § XVI A, Objectives]

Subsequent public statements by the authors of this rule emphasized that these regulations were intended to be flexible and facilitate the continued and further development of new technology.

FDA's action was a boon to providers of electronic systems for data capture, correction, review, and archiving in clinical trials intended for submission to the agency. These providers now had a covenant: if their system complied with 21 CFR 11, then the FDA would accept electronic records and electronic signatures in place of paper records, and sponsors could be confident enough to execute their impor-

tant clinical trials with electronic systems. So far, so good.

### Technology providers interpret regulations

When developing an electronic clinical trial system, a technology provider must interpret regulations in detail. It's part of the job. Otherwise FDA or other regulators would have to invent and specify everything, and technology providers would simply build to order.

When it comes to converting regulatory provisions to system specifications, programmers do not have one luxury that lawyers have. Lawyers, like politicians, write for people and can thus presume, rightly or wrongly, a degree of common sense.

Programmers write for machines, and their regulatory interpretations tend to reach a deep level of detail. They cannot ask FDA to certify each judgment they make, nor could the agency respond to

hundreds of such questions. Therefore, system developers must somehow address the needs of sponsors, regulators, and site personnel who will use the system to conduct many different types of clinical studies ranging in complexity and size from single site/single patient trials to trials with several thousand patients and hundreds of sites. The system has to comply with FDA (and international) regulations. This is actually fairly challenging. Any semantic or functional contradictions in the regulations and guidance must be resolved. And the specificity of a particular solution will *amplify* each element of the regulations in the sense of expanding the depth of detail while it will simultaneously *limit* the generality of the regulatory requirement in the sense of arriving at a specific realized implementation.

Immersed in the various urgencies of system develop-

ment, product sales, trial execution, and competition, a system designer at a particular provider may find it difficult to remember or imagine that various implementations might meet a general regulatory objective. This very difficulty shows the value of FDA's statements concerning its desire to preserve flexibility and thus fertilize invention, novelty, and ultimately the optimization of clinical research. At any point in time it may well be that the combination of individual requirements that must simultaneously be met will substantially narrow the set of acceptable technical implementations. Multiple objectives in conjunction with the state of the art may imply only one solution, or even, dreadfully, none. The technical challenge is akin to the many-body problem in physics, and this "multi-problem problem" for technology providers in clinical research can, by its sheer size and difficulty,

new relevant information is documented as it becomes available.

§ 8.3.13 Source documents Located in Files of Investigator/Institution

§ 8.3.14 Signed; dated, and completed case report forms (CRFs) (Copy) Located in Files of Investigator/Institution (Original) Located in Files of Sponsor

§ 8.3.15 Documentation of CRF corrections (Copy) Located in Files of Investigator/Institution (Original) Located in Files of Sponsor

### 21 CFR Part 11 Electronic Records and Signatures

#### § 11.1 Scope

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2 unless paper records are specifically required.

#### § 11.10 Controls for closed systems.

(c) *Protection of records to enable their accurate and ready retrieval throughout the retention period.*

#### § 11.30 Controls for open systems.

...Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt.

### Guidance for Industry: Computer Systems Used in Clinical Trials (CSUCT) Revised September 27, 2001

#### I. Introduction

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.

#### III. General Principles

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

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

5. 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.

6. 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.

#### V. Data Entry

##### B. 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.

#### VIII. System Dependability

##### A. Systems documentation

Systems documentation should be *readily available at the site* where clinical trials are conducted.

#### XI. Records Inspection

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.

lead to a kind of provincialism. A particular solution may appear to be the only solution.

The providers thus become regulatory experts of a certain sort. Because of their detailed immersion in regulations, their viewpoints can help clarify and extend regulatory understanding. However, as described above, structural attributes lead providers to include details or language in their extended interpretations that are not explicitly provided for in the regulations themselves (amplification and/or limitation).

### Centralized storage of data was questioned

We want to comment on a particular example of such an interpretation and try to draw some general lessons. In his May 2001 Technology Viewpoint column (“e-source: To e or not to e,” *Applied Clinical Trials*, May 2001, p. 36), Paul Bleicher suggested that data maintained at a central location, with no local archive at the investigator site, would not comply with FDA requirements for electronic source (e-source) documents. This idea has also been presented at various conferences. In our opinion, his views interpret and reword (amplify and limit) regulations to arrive at a narrow view that is neither conservative nor correct. Unless countered, this kind of interpretation may delay or prevent adoption of technology for e-source in clinical trials, which would be unfortunate and ironic given the original intent stated by the regulators themselves.

We wish to present a view in counterpoint that the integrity of data stored centrally can fulfill what regulations actually say concerning the obligations of the site and e-source. We think that centralized systems using digital and handwritten signatures linked to e-source documents lessen the burden for sites, and move the industry toward a trans-

forming acceleration of research much greater than the incremental improvement that has come from using the Web for electronic case report forms (eCRFs) transcribed from paper source documents.

### Local control doesn't mean local storage

A primary obstacle to the adoption of e-source, according to Dr. Bleicher's column, was “the requirement that a site maintain

## Technology providers sometimes include details or language in their interpretations that are not explicitly provided for in the regulations themselves.

archival control of data.” He also wrote: “If the electronic CRF is the primary source document, the investigator must maintain control of that CRF to ensure attributability.” He suggested a possible technical approach: “To establish control, the investigator can create the electronic record on a computer that is physically located at his or her site or institution.” Then he amplified and limited the regulations by writing: “In any case, the electronic record cannot be stored with the sponsor or the sponsor's representative—such as a CRO or technology vendor—because attributability would be lost.”

The article went on to note that Web-based data entry was “difficult to reconcile with primary source data entry” and to advise that with “central-server” systems it was “always advisable to have separate source documents” and that “a site without physical ownership and control of its database does not meet the GCP requirement for investigator control of the data...”

Similarly for handheld devices: “If it is primary source data the site must maintain an archival copy...making it necessary to archive the memory card or a certified copy at the site.”

And for interactive voice response (IVR) systems: “No obvious workaround is available to secure investigator control of IVR generated data.”

Ultimately the article constituted an interpretation of regulations and guidance that seemed

to stipulate reliance on local storage systems and to restrict compliant capture of e-source to offline RDE with “a consistent method of local storage.” For diary data, which is a familiar form of e-source, the article amplifies regulations to require physical storage devices at the location of a site so that such data can be “kept for archival purposes.” While the article acknowledges that Web-based direct entry of e-source into eCRFs under digital signatures could address attributability, such an approach is faulted on the grounds that the sponsor could delete the electronic record and signature.

The point of local storage would be to support manual authentication processes including field-by-field source document verification in the same manner now done with paper to prove that centralized data agrees with data at the site. This would continue the most expensive and burdensome chore required to generate integrity in paper systems.

### Regulations don't specify local archiving

In support of an alternative view, consider which regulations bear on this issue and what they actually say. (See the accompanying box.)

Taken together, the regulations and guidance bearing on electronic records and e-source in clinical trials concern data integrity. Both the Rule on Electronic Records and Signatures and Guidance for Industry: Computer Systems Used in Clinical Trials (CSUCT) emphasize the agency's intent to set forth the steps needed for computer systems to ensure that the pedigree of the data with electronic records would be as trustworthy as with paper records. The predicate rules spell out that data and record integrity are important, and that case history data, including source data and CRFs, are to be “prepared,” “maintained,” and “retained” by the investigator.

A system compliant with 21 CFR Part 11 that is designed to provide the sites with ready access and the capability to enter, edit, review, authenticate, and maintain all of their electronic records for a clinical trial might well meet the regulatory requirements and guidance currently issued. To fulfill the criteria for data quality mentioned in the Guidance, such a system should ensure that electronic records are attributable, legible, contemporaneous, original, and accurate (ALCOA) and that they are protected in such a way as to “enable their accurate and ready retrieval throughout the record retention period.”

In addition to what the regulations do say, consider what they don't say. Many of the terms used in Dr. Bleicher's column, including the phrases “controlled certified copy,” “investigator controlled data,” “physical ownership and control,” “local control,” “local copy,” “local archival



control,” and “archival control of data” do not appear anywhere in the regulations. Only the terms “prepare,” “maintain,” and “retain” appear in the regulations.

### **Control without local storage is possible**

Sponsors executing clinical trials with electronic data collection (EDC) technology providers regularly stipulate that the EDC systems used by the sites specifically provide controlled access by the site to its records. They set forth in their requirements specifications exactly who shall have the capability to enter electronic records, edit and review them, and make changes in the data. In preparing a particular trial, the EDC system applications are validated to ensure that only such designated personnel (usually site personnel and investigators who have signed the 1572) can control (prepare, maintain) the data during the trial. Physical access to the devices is not a necessary component of maintaining the electronic record. Instead, access to the information is needed. If an investigator has all of the components of an electronic record in a secure form on his or her desktop at will, then the case for data integrity is good and one can legitimately say that the site has maintained and retained that record.

Precedents with paper records that fulfill the records retention requirement include the storage of the records in a central facility (on or off-site), and the use of contractors, such as Iron Mountain, to store records in secure warehouses. Laboratory data is often held offsite in computerized systems that are under contract to the sponsor. Regulations indicate that the site should have ready access to such data, and specifically that FDA inspectors should have access to such data for purposes of review at the site. But nowhere does it appear that the only satisfactory

solution to meeting such requirements is for the site to physically possess local hardware on which its electronic records are stored.

### **Paper and electronic records are different**

It is useful to consider how different e-records are from paper records. Our habits of thought concerning physical possession of paper, which confers access to information on the paper, should not obscure the much weaker link between physical possession of digital storage media and access to that data. A look at a paper CRF page reveals the logically related fields, the data in the fields, handwritten commentary and marginalia, and any signatures. By physically preventing people from looking at the

## **What matters is the full story on data integrity and security, not physical possession.**

paper, one can do a pretty good job of protecting the information. However, a look at a hard drive is not the key to access. By cryptographically linking data fields, audit trails, and electronic or handwritten signatures on electronic records, access to electronic records can be controlled by software running in the devices needed to interpret the altered bits on the storage media. Electronic records can be accessed remotely as quickly as they can locally, and possibly more securely given the potential exposure of computer systems at local sites to environmental hazards, maladroitness IT management, and cyber-attack. What matters is the full story on data integrity and security, not physical possession.

### **Centrally stored data can have integrity**

In a nutshell, the notions

concerning “local copies” emerge from a reasonable desire to ensure that data captured at a site and sent to a sponsor or sponsor representative is not subsequently altered by the sponsor. This is the point of source document verification and database verification. It is why an FDA inspector during an audit must be able to compare the values in a locked database against some local accessible values maintained by the site and presumed to have an unimpeachable pedigree. The process of holding a local copy of source data (and a local copy of CRFs sent to sponsors) all makes sense for paper, where the physical properties of paper are relied on to hold the data on certain fields “together” and where handwritten

signatures can be linked to data fields and auditable changes to data only by the physical properties of the paper.

However, the regulations simply state that investigators shall “prepare” and “maintain” case histories (source data and CRFs) during a trial and “retain” them afterwards for a specified period. Various requirements are intended to ensure data security and integrity for electronic records, but none of them specifically mandates a “controlled certified copy.” The records of sessions that FDA has with vendors carry a notice that they reflect only the views of individuals present at the meetings and not of FDA. So one looks primarily to the regulations and the guidance. These do constitute what FDA in the full force of its deliberations “wants.” Such wants include technical flexibility and best solutions. The Rule on

Electronic Records and Signatures and CSUCT are specific about the objectives for data integrity, system controls, authority controls, and data quality.

Below are some of the features and approaches that can be combined to make the case for integrity and security of electronic source and compliance with regulations without using local storage and without requiring field-by-field source document verification. The example is that of handhelds that send diary data directly to a centralized Web server. During the trial the site can access the data for review and approval (maintenance) via the Web:

1. Data is attributable because it is captured on devices that are assigned to subjects and electronically registered to a specific trial.

2. Data can be authorized and confirmed to be from a subject by using handwritten signatures executed on the handhelds for each report and linked cryptographically to that report in a centralized store.

3. Such tamper-proof electronic records can be protected from deletion at the central server by technical security and processes that require the willing collaboration of at least two individuals. The effectiveness of such protection can be validated.

4. Sites “prepare” diaries as part of their case histories by teaching the subjects how to use the handhelds and by making sure the subjects comply with schedules and constraints for completing and transmitting diary records.

5. Sites “maintain” diary data by reviewing it using secure Web sessions and by virtue of the constraints built into the system that prevent anyone but duly trained and authorized site staff from entering or editing subject data. Such constraints are part of the requirements



specifications and are confirmed by system validation.

6. System validation also takes the place of field-by-field source document verification, since data entered on the handheld is validated to be accurately and completely transmitted and parsed into the datastore and/or database.

7. Sites “retain” diary data after the trial by receiving a certified CD-ROM or other nonvolatile record that includes all the data, metadata, and trial documentation necessary for an audit of the trial at the site. The CD-ROM can handle confidential data (with password protection), support computer generated audit trails, and permit “reconstruction” of the trial as it occurred at each site.

8. Such diary data in tandem with electronic source data signed with digital signatures (or handwritten signatures attached to electronic records) by site personnel can provide a nearly paperless system that exceeds the quality of paper data and is also more convenient to use.

### **Some disadvantages are not substantial**

Last May’s column mentioned two “disadvantages” of e-source that we question. The first “disadvantage” was that electronic capture complicates the interaction between a doctor and a subject more than paper does. Therefore the clinical investigators won’t use it. Certainly this is simply a technical matter. Whatever the method of capture is, it must in no way make it more complicated for the doctor or study coordinator to use than paper. This is not a conclusive “disadvantage,” just an opinion about technologies with which the author was familiar. The second “disadvantage” mentioned was that e-source brings “increased risk of data entry errors.” This is an unproven assertion. It may be

true that data typed into a keyboard or entered on a PDA is more prone to error than data written to paper, but the proof offered (the common error of misdialing a phone number) is not very compelling evidence. People can make errors of the hand: I think I’m writing 180, but my hand writes 108. But with electronic capture, such entry errors may in fact be dramatically

## **More data would probably be entered correctly if data entry personnel were spared double or triple transcription and could focus on the moment of original entry.**

minimized using real-time confirmation and other accuracy-enhancing techniques, including numerical selection instead of writing numbers. The idea that anyone would automatically know whether 108 mm Hg or 180 mm Hg was correct during source document verification (SDV) is questionable.

In many audits and reviews of audits done of clinical studies, one of the authors (GM) has fomed the strong view that electronic source data does not bring with it an increased risk of data entry errors. It has been his experience that manually entered and transcribed data, lab values, CRF observations, and hospital records are all significantly more accurate when recorded electronically. Entry errors are not the unique province of e-source, and they certainly are not prevented by the use of paper source documents and SDV. The incidence of getting data values right from the start could probably be improved if data entry personnel were spared the additional burdens of double or

triple transcription and could focus a bit more attention on the moment of original entry. In any case, this “disadvantage” is not established.

### **Certified copies at sites are not essential**

While a site’s electronic records can certainly be stored locally to support e-source in a compliant way, the regulations do not

Part 11 have been implemented so that that claim is met.

### **Trusted third parties may provide centralized storage**

The idea that centralized servers maintained by persons other than site personnel can bring improved efficiency and reliability to clinical trials is probably correct. However, it is neither implied nor required by regulations that such “trusted third parties” be outside the pharmaceutical area or that they have contractual arrangements with the sites. As written in paragraph 41 of the preamble to 21 CFR Part 11:

The agency does not believe it is necessary to codify the basis or criteria for authorizing system access, such as existence of a fiduciary responsibility or contractual relationship. By being silent on such criteria, the rule affords maximum flexibility to organizations by permitting them to determine those criteria for themselves.

### **Centralization is one of many possibilities**

We do not believe centralized systems are the only acceptable method. We do believe that the objectives of the regulations can be achieved through such site client systems and that they have some advantages.

We believe that data integrity is best preserved when the trial data is centralized, protected, backed up, and restorable by a fully professional staff and by validated procedures. Some systems centralize the data onto servers that are physically protected (under lock and key) at network operating centers. The centers ensure reserve power (in the event of main power failure from city utilities) and proper, fireproof, and air-conditioned places for computer and telecom equipment needed for each study. Providers then ensure in a



## Guest Commentary

validated fashion that the sites can prepare, maintain, and retain the data on clinical subjects, and that they can also retain access to laboratory data and other clinical data streams from other collec-

Although technology providers are paid by sponsors, the conditions of payment can specify that they build, validate and provide EDC tools for studies that ensure data content is under control of

place) of centralized data storage, but preserves the key regulatory aspects that support approval and execution of actions on data as a responsibility of the investigator.

constraints that shape such commentary (including ours) and readily reserve to regulatory agencies the last and most authoritative word.

### Manual authentication of electronic data would continue the most expensive and burdensome chore required to generate integrity in paper systems.

tion paths. This ready access and review, provided electronically, corresponds to the review enabled by physical possession of paper records. The review capacity and familiarity with the data would not necessarily be enhanced, however, by the site's having physical possession of the storage devices on which the altered bits representing the electronic record repose.

the site. They can and often do act as third parties at the request of the sponsor to provide the secure tools for the sites to use to prepare, maintain and retain their clinical research data. This strategy brings the benefits (central administration, rapid implementation of validated mid-study corrections, restoration capability, and the existence of a single canonical electronic record in one

#### Don't amplify regulatory barriers

The technology for supporting data capture and management in its full range of complexity may have arrived. Its transforming benefits will emerge with fuller use of e-source and direct data capture, and we have presented a case that the approach of centralizing such data without local storage should not be dismissed presumptively.

While we have criticized Dr. Bleicher's article about e-source for "amplifying" regulatory barriers, we think that commentary from technology providers about regulations, including that article, has been and will be useful. We have mentioned the structural

During the past year, it has been reassuring to see sponsors rise to the required level of courage to assess the case for integrity of centralized data in spite of comments that fan the flames of concern. Such action on the part of FDA, sponsors, and technology providers seems to be the only way to move ahead.

**Stephen A. Raymond, PhD**, is chief scientific officer and quality officer with PHT Corporation, 500 Rutherford Avenue, Charlestown, Massachusetts 02129, (617) 973-1600, e-mail: sraymond@phtcorp.com.

**Gerald F. Meyer** is advisor for regulatory affairs at PHT Corporation, and a former acting director of FDA's Center for Drug Evaluation and Research.