

Compliant Electronic Data for Clinical Research

Patricia L. Rossman, BS, MT, SBB, CSQE
Vice President, Clinical Operations
Pharmaceutical Services Group

Abstract: *The U.S. Food and Drug Administration (FDA's) acceptance of electronic data from clinical trials depends upon the agency's ability to verify the quality and integrity of the data. Electronic data must meet the same fundamental elements of data quality as paper data (attributable, legible, contemporaneous, original, and accurate). This article describes requirements for computerized systems used in clinical trials and how to make spreadsheets and databases compliant with 21 CFR Part 11 and International Conference on Harmonization (ICH) guidelines. It covers the FDA's Guidance for Industry: Computerized Systems Used in Clinical Investigations and ICH E6 guidelines. A checklist for determining whether a study is compliant with the FDA guidance and best practices for computerized systems is described.*

(Body Text)

FDA Requirements for Compliant Electronic Clinical Data

Electronic data for clinical research must have quality and integrity in order to be compliant with FDA regulations. The FDA's acceptance of electronic data from clinical trials for decision-making purposes depends on its ability to verify the data's quality and integrity during onsite audits, according to 21 CFR 312, 511.1(b), and 812 (Table 1).

The regulation defines quality by stating that: "Such electronic source data and source documentation must meet the same fundamental elements of data quality as paper data." The data must be attributable to the person who entered them. They must be legible, so that anyone can read and understand them. The data must be contemporaneous, that is, entered soon after or as an observation is being made. They must be original and accurate.

Data integrity requires an audit trail for any data that are changed, by either a person or a computer, mistakenly or on purpose. The audit trail shows who changed the data, what change they made, when they made the change, and in some cases, why they changed the data.

In May 2007, the FDA published a *Guidance for Industry: Computerized Systems Used in Clinical Investigations*, which provides more information about what the agency means by compliant electronic data (Table 2). The principles outlined in the guidance should be used for computerized systems that contain any data that are relied on by an applicant in support of a marketing application. For example, the part of electronic hospital medical records that are used in a clinical trial (such as eligibility criteria, concomitant medications, and laboratory tests) are considered a source record and the data the applicant relied on in a marketing application.

The guidance also covers computerized laboratory information management systems that capture analytical results of tests conducted during the clinical trial. The recommendations are applicable to computerized systems that create source documents or electronic records that satisfy the requirements in 21 CFR 312 or 812, such as case histories (21 CFR 312 covers drugs and 812 covers devices).

This guidance also applies to recorded source data transmitted from automated instruments (such as HPLC or LC-MS-MS) directly to a computerized system, or when source documentation is created in hard copy (e.g., a paper case report form) and later entered into a computerized system or automatically recorded by a computerized system (e.g., an ECG reading or a driving simulation instrument).

A Checklist for Complying with the FDA Guidance

A simple checklist is very useful in determining whether a study is compliant with the FDA guidance. A sample checklist developed by the author, which can be modified as desired, made every recommendation in the guidance into a question, followed by columns for the answer, objective evidence, risk, and mitigation of the risk. The first section of the checklist is the study protocol. The first question is, “Does the study protocol identify each step at which a computerized system will be used to create, modify, maintain, archive, retrieve, or transmit source data?” The answer is either yes or no. The objective evidence for this question is a copy of the protocol, which either does or does not indicate where electronic records are used.

Then the next column is the risk, which is the reason the compliance assessment is necessary. The risk column should use some type of scale (e.g., 1-5, 1-100, or moderate, minimal, or maximum), which should be explained in instructions for using the checklist. One important element of the risk assessment is to determine the regulatory risk of the FDA not accepting the data if the site does not comply with this particular part of the guidance. In addition, risk includes business risk, patient safety risk, and other risks. Thus, even if a site does not have a high regulatory risk, if the sponsor is requiring the site to be compliant with 21 CFR Part 11 or the guidance on computerized systems, then the site may have a business risk of the sponsor not placing future studies at the site. Mitigating risk is the key. Site staff should know how to mitigate or lessen risk in the areas of greatest risk.

Simply doing this assessment lessens the site’s risk. During an audit or inspection, most regulatory bodies will ask if an assessment was done for any areas where they find non-compliance. The next question will be whether the site has a plan for achieving compliance. If a site has a plan and timeline for filling compliance gaps, this may partially satisfy an auditor or inspector.

The second question on the checklist under the category of study protocol is, “Is the computerized system designed to satisfy the processes assigned to these systems for use in the specific study protocol?” For example, are the data recorded in the right units? Is blinding maintained? This question really asks whether the computer system being used meets the needs of the specific trial, and complies with the protocol. That is one of the tenants of validation: does the system meet the requirements? The objective evidence, if the answer is “yes,” would be some test cases that show in all types of circumstances that the system truly records data in the right units and complies with the protocol.

Areas Covered by the Guidance

The FDA guidance covers existing requirements, discussing the requirements in a way that is easier to understand. The guidance basically describes industry best practices.

The section on standard operating procedures (SOPs) covers using computerized systems to create, modify, maintain, or transmit electronic records. The guidance provides an appendix with a list of SOPs for electronic record keeping, including back-up and restoration, contingency planning, training, access to the system, and security.

The guidance touches on some additional areas:

- Source documentation and retention
- Internal security safeguards
- Audit trails
- Date/time stamps
- External security safeguards
- Direct entry of data
- Retrieving data
- Dependability system documentation
- System controls
- Change controls
- Training of personnel.

Source documentation and retention requires that the site keep a copy of any electronic records that it transmits to a sponsor or elsewhere. The section on internal security safeguards covers the unique user IDs and passwords for the system, and for internal security. The policy on electronic security must state that IDs and passwords cannot be shared, and should require that passwords be changed periodically. The best way to do this is by using software that forces staff members to change their passwords. The policy should also cover the procedure for deleting access to people who are no longer working on the study or working for the company. This is often overlooked; however both the FDA and the Health Insurance Portability and Accountability Act require it.

The audit trail shows who created the data and when they created them, as well as who made any changes and when they made the changes. This relates to the FDA requirement that data (electronic or paper) be attributable.

Automated date and time stamps are important because they are more reliable than having a person enter the date and time. Also, automated date and time stamps are easier to validate. For example, in a Phase I facility, best practice is to have a centralized clock date and time stamp actions.

The section on external security safeguards covers items such as ensuring that the computer system is free from hacking, unauthorized access, and database manipulation. The section on direct entry of data covers ensuring that the roles of people who use the system are well-defined and that no one has a higher level of access than necessary.

Change control is very important, yet, it is often overlooked. Study coordinators are usually not experts at handling change control. Someone else, such as staff from the information technology department, should be responsible for the electronic record security. However, information technology staff members in many hospitals and academic medical centers do not know the FDA regulations. Study coordinators are responsible for knowing whether computerized systems used in clinical trials are compliant, however, they need assistance in fixing problems.

Change control means that once everything is validated in a certain state, nothing is changed unless there is an assessment of the impact of that change. Any change is documented and everyone involved with the computerized system must know about the change and be trained on any new procedures.

Training is another area that the guidance covers. Study staff must be trained on computerized systems that are used in clinical trials.

Other Regulations and Guidelines

21 CFR Part 11, the ICH E6 Guidelines, and the FDA guidance on general principles of software validation are also applicable to computerized systems in clinical trials. 21 CFR Part 11 has been around for a long time. The FDA's thinking on the enforcement of Part 11 has changed. The FDA published, and rescinded, several guidances on Part 11. The *Guidance for Industry: Part 11, Electronic Records; Electronic Signatures — Scope and Application*, published in 2003, basically provides an overview of what the FDA thinks is important in relation to Part 11.

Many of these rules concerning electronic records and electronic signatures have been in effect since 1977; however, the FDA may not enforce audit trail and validation requirements in some situations. Those situations include older systems that were in effect before the regulation was published. The approach for computerized systems used in clinical trials outlined in the scope and application guidance should be followed until such time as Part 11 is amended.

The ICH E6 guidelines provide substantive information (Table 3) and discuss electronic records in detail. For example, Section 493 states that:

“Any change or correction to a CRF should be dated, initialed, and explained and should not obscure the original entry.”

This requirement is met by an audit trail. This applies to both electronic and written changes and corrections. Section 493 goes on to state:

“Sponsors should provide guidance to investigators and/or the investigators' designated representatives on making such corrections. Sponsors should have written procedures to assure

that changes or corrections in CRFs made by sponsor's designated representatives are documented, are necessary, and are endorsed by the investigator. The investigator should retain records of the changes and corrections."

Section 5.1.3 states that: "Quality controls should be applied to each step of data handling to ensure that all data are reliable and have been processed correctly." This means that a second person should look at any data entry, transmission, or manipulation. Quality control is important in the ICH guidelines.

The sponsor's responsibilities when using electronic trial data handling in remote electronic trial data systems are described in Section 5.5.3. These responsibilities include ensuring and documenting that the electronic data processing systems conform to the sponsor's established requirements for completeness, accuracy, reliability, and consistently- intended performance. This is validation.

Other sponsor responsibilities include maintaining SOPs for computerized systems used in clinical trials and ensuring that the systems are designed to permit data changes in such a way that there is an audit trail. The sponsor must maintain a security system that prevents unauthorized access to the data. This includes user ID and passwords, and an SOP on maintaining access. Maintaining a list of the individuals who are authorized to make data changes is another sponsor responsibility.

The sponsor must maintain adequate backup of the data. Data are usually backed up every night and once a week for the entire week. The weekly backups are stored off site, which means that a site can never lose more than one week's worth of data.

Section 5.5.4 states that: "If data are transformed during processing it should always be possible to compare the original data and observations with the processed data." This is also important for the FDA in relation to medical records. The FDA needs to be able to go back and verify sources in the electronic medical records.

The FDA also published *Guidance for Industry and FDA Staff: General Principles of Software Validation*, a detailed document. The preamble states:

"Although the primary purpose of this guidance outlines general validation principles that the FDA considers to be applicable to the validation of medical device software or the validation of software used to design, develop, or manufacture medical devices, it contains useful validation principles that can be applied to software used in the conduct of clinical trials."

Best Practices for Computerized Systems

Using best practices from the industry will enable sites to produce high-quality data with good data integrity (Table 4). SOPs are extremely important, and staff must be trained on the SOPs. Network security requires having a good information technology person to ensure that unauthorized people cannot get into the site's network. The site must have secure entry into the network. Application security and access roles are another best practice.

Validation of the network and all applications is crucial. Applications include electronic case report forms and other applications, such as laboratory information management systems that are sending results electronically. Validation starts with user requirements.

In the context of the regulated pharmaceutical industry and regulated computer systems, validation means proving in written test cases that the system does what it is supposed to do and does not do what it is not supposed to do. People tend to validate that the system is working, but forget to ensure that it does not do what it is not supposed to do, such as allowing people with lower access into higher access functions.

Validation must cover functional requirements and specifications, and test the system against the requirements and specifications. Change control, which has already been discussed, is another best practice.

A validation map starts out with a validation master plan that describes the resources, timeline, and implementation strategy. This includes outlining who will be responsible for various tasks and what will be validated. Validation is costly in terms of time and labor. Study coordinators cannot, and should not, do this on their own.

The validation map includes assessments of risk, Part 11, and general quality guidelines. The industry has embraced a risk-based approach to computerized validation whole-heartedly because it shows to what extent certain systems need to be validated. Systems with higher risk require more validation and systems with lower risk require less validation.

The Part 11 assessment can be done with a checklist, similar to the checklist used to assess compliance with the *Guidance for Industry: Computerized Systems Used in Clinical Investigations*. This assessment covers whether the system needs to be compliant with Part 11, and if so, which parts of the medical records will be used in the trial. Whether the medical records system may need to be compliant with Part 11 depends upon the protocol for each trial. Different protocols use different source data from the electronic medical records. Compliance with Part 11 will not happen overnight. Researchers must do the best that they can to move toward compliance. They should learn about the requirements, the site's systems, and the study. They should perform an assessment and develop a plan. This is the best way to manage a site from the data quality and regulatory perspectives.

The general quality guidelines assessment determines which data are involved with the site's trials. Requirements, based upon the protocol, should be written so that they can be tested.

The next step in the validation map is to write the test cases, which can be ordered in installation qualification, operational qualification, and performance qualification. The test cases must observe and record the system's configuration and the way in which it was put together, test the system's operations, and then test the system's performance.

Then test cases are executed and the answers are recorded. Staff members determine whether the answers match the predetermined expected results based on what the system is supposed to do. If there are any deviations, they must be fixed and the testing repeated to see if the remediation was appropriate and sufficient. Then the system goes live. Staff members monitor and troubleshoot the system for any glitches, and perform any necessary revalidation. Finally, the system is put under change control to maintain the validated state.

Excel™ Spreadsheets

Excel spreadsheets are very easy to use, however, there are some problems related to their use in clinical trials. In order to use them in a clinical trial for any function that comes under general quality guidelines, such as dosing, statistics, determining cohorts, or determining days for study visits, the Excel spreadsheets must be compliant with Part 11. They must be controlled to ensure subject safety.

For example, in one situation, someone used a computer that contained an Excel spreadsheet used for dosing. That person changed a macro and the dosing for the entire study was changed; subjects did not receive the dose that they were supposed to receive in the study. Researchers may not understand how critical the data contained in Excel spreadsheets can be to studies and how easy it is for data to be changed.

Access to Excel spreadsheets must be secure and have limited access, have audit trails, have date and time stamps, and be attributable and verifiable. Anyone can enter data on Excel spreadsheets, which do not show who entered or changed the data, so extra caution is necessary.

As the number of Excel spreadsheets that are being used in a clinical trial and the amount of information on those spreadsheets increases, the risk of issues increases. Table 5 outlines security, traceability, and validation issues with Excel spreadsheets. Anyone can access the spreadsheets, typically, because many research staff members involved with a clinical trial will need to add information. Saved spreadsheets can be overwritten. Changes to validated formulas can occur undetected. Macros can be changed, causing unintended changes to other cells in the spreadsheet.

A system such as Excel is too changeable to be validated without additional controls.

There are several add-ons to Excel that can make Excel compliant with Part 11 in terms of system security and the audit trail (Table 6). DaCs™ and ExcelSafe™ are two such products that have a full audit trail and logical security. These products are cost effective because they can easily be put into existing worksheets or used with new

worksheets. Research staff members do not have to learn anything new. Spreadsheets can be emailed, however, unauthorized people cannot change them.

DaCs™ and ExcelSafe™ also allows security to be controlled. The program produces a secure user ID and password that must be changed periodically. A system administrator determines who has access to Excel and the levels of access.

There are other plug-in or add-on products that will provide an audit trail for Access and Lotus Notes, and increase compliance with Part 11. ComPac by Winchester is an add-on for Lotus Notes. It applies an audit trail and password security. Ofni makes a plug-in to make Access compliant with Part 11.

Conclusion

In order to be compliant with regulations, electronic data for clinical research must be attributable, legible, contemporaneous, original, and accurate. To meet FDA requirements, computerized systems must be validated, which is part of the definition of having data with quality and integrity and change controls must be implemented. Computerized systems must be secure and the data must be backed-up.

#

TABLE 1
Requirements for Compliant Electronic Clinical Trials Data

- FDA must be able to ability to verify the quality and integrity of electronic clinical trials data during on-site inspections and audits (21 CFR 312, 511.1(b), and 812)
- Electronic source data and source documentation must meet the same fundamental elements of data quality as paper data: attributable, legible, contemporaneous, original, and accurate

TABLE 2

Guidance for Industry: Computerized Systems Used in Clinical Investigations

- The guidance applies
 - To 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
 - To recorded source data transmitted from automated instruments directly to a computerized system
 - 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

TABLE 3
The ICH E6 Guidelines Related to Computerized Systems Used in Clinical Trials

- 4.9.3:
 - Any change or correction to a CRF should be dated, initialed, and explained (if necessary) and should not obscure the original entry (i.e., an audit trail should be maintained); this applies to both written and electronic changes or corrections (see section 5.18.4(n)). Sponsors should provide guidance to investigators and/or the investigators' designated representatives on making such corrections. Sponsors should have written procedures to assure that changes or corrections in CRFs made by the sponsor's designated representatives are documented, are necessary, and are endorsed by the investigator. The investigator should retain records of the changes and corrections.
- 5.1.3:
 - Quality control should be applied to each stage of data handling to ensure that all data are reliable and have been processed correctly
- 5.5.3:
 - When using electronic trial data handling and/or remote electronic trial data systems, the sponsor should:
 - (a) Ensure and document that the electronic data processing system(s) conforms to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance (i.e., validation)
 - (b) Maintain SOPs for using these systems
 - (c) Ensure that the systems are designed to permit data changes in such a way that the data changes are documented and that there is no deletion of entered data (i.e., maintain an audit trail, data trail, and edit trail)
 - (d) Maintain a security system that prevents unauthorized access to the data
 - (e) Maintain a list of the individuals who are authorized to make data changes (see sections 4.1.5 and 4.9.3)
 - (f) Maintain adequate backup of the data
 - (g) Safeguard the blinding, if any (e.g., maintain the blinding during data entry and processing)
- 5.5.4:
 - If data are transformed during processing, it should always be possible to compare the original data and observations with the processed data

TABLE 4
Best Practices for Computerized Systems

- SOPs
- Training
- Network security
- Application security and access roles
- Validation
- Change control

TABLE 5
Issues with Excel™ Spreadsheets

- Security:
 - Anyone can access the spreadsheet
 - Saved records (the spreadsheet) can be overwritten
- Traceability:
 - Changes to validated formulas can occur undetected
 - Retrospective changes to saved data can occur undetected
- Validation Concerns:
 - A system with these inherent concerns cannot be validated
 - Each spreadsheet is custom

TABLE 6
Add-ons to Make Excel Compliant with Part 11

- Full audit trail and logical security
- A viable and working solution
- Cost effective to implement in new and existing spreadsheets
- Can be integrated and embedded with other applications that use spreadsheets