

# ERES COMPLIANCE AND DATA INTEGRITY ISSUES IN e-TRIALS

Carol A. Connell, RN, DBA  
Associate Director  
Development Operations Team Leader  
Global Research & Development  
Pfizer, Inc.

**Abstract:** *There are many issues to consider when conducting remote data capture or electronic trials (e-trials). This article outlines the components of the Food and Drug Administration's regulations concerning the use of electronic records and electronic signatures (ERES), highlights the regulations that affect investigator sites, describes the roles and process changes necessary to conduct an e-trial, identifies sponsor/contract research organization considerations affecting ERES compliance, and discusses the impact of an e-trial when conducting quality assurance audits.*

The use of computerized data in clinical trials has generally been limited to a centralized database with independent data entry from the paper case report form (CRF) into the database and subsequent analysis of the data. However, advances in the technology and acceptable methods of ensuring the relative security of the data have provided us with options, including the electronic case report form (e-CRF). Trials that use this technology have been dubbed "e-trials" or remote data capture (RDC) trials. Along with the technology comes an array of issues that require attention and may alter the traditional processes used in conducting clinical trials within Good Clinical Practices (GCPs). The Food and Drug Administration (FDA) worked with industry to develop regulations (21 CFR Part 11) that address uniform standards to ensure that electronic records and signatures are as accurate, secure, and reliable as paper records and handwritten signatures. Electronic records must be maintained securely and meet data integrity, retention, and inspection requirements.

The FDA's guidance document, entitled *Computerized Systems Used in Clinical Trials* ([www.fda.gov/ora/compliance\\_ref/part11/](http://www.fda.gov/ora/compliance_ref/part11/)), focuses on ensuring the integrity of electronic data records originating at clinical sites, but also applies to those systems used by sponsors, contract research organizations (CROs), and data management centers.

Part 11 of the regulations applies to "records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in agency regulations . . ." and defines electronic signatures as "computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature." Electronic signatures must be unique to the individual and require a user ID and password. Alternately, biometrics (e.g., retinal scan, or thumb print) can be used as a unique identifier. A scanned image of a handwritten signature is not considered an electronic signature. The electronic signature must be accompanied in the electronic record by statement that lists the printed name of the signer, date and time, and the meaning of the signature (i.e., "approved by", "reviewed by", or "agreed to by"). Anyone using

electronic signatures in an FDA filing (e.g., investigators, sponsors, CROs) must provide an affidavit with a handwritten signature, notifying the FDA that they will be using electronic signatures and that the electronic signatures will be the equivalent of a handwritten signature.

## The Application and Principles of ERES

ERES regulations apply to:

- Source documents that are created in hardcopy and then entered into a computer system,
- Direct entry by a human into a computerized system,
- Automatic, computerized entry into a database (e.g., diary information collected on a Palm Pilot that is transferred into a computer), and
- The electronic signatures affixed to these electronic records.

If the data are entered directly into the electronic system, the electronic record becomes the source document. The regulations are specific and require that certain processes and procedures be implemented to ensure the integrity of the data in each of these instances.

Table 1 outlines the four principles of ERES. The hardware and software used to create, modify, maintain, archive, retrieve, or transmit data must be documented, and this documentation must be retained in the specific study records. As with all study-related files, the FDA can, and probably will, inspect the records and files intended to support a submission. These system documents must be available, along with documentation of system validation and documentation of staff training on the systems.

All original entries made in the database and all subsequent changes, with the reason for that change, are maintained.

Record retention is necessary to enable reconstruction of the trial, facilitate evaluation of the data, and meet retention regulations. The original, or a certified copy of the source documents, including any query resolution documents, must be retained along with the data collected on case report forms. When the original data are entered directly into the computerized

systems. Depending on the type of system, certain requirements apply. An open system is one in which the person who is responsible for the content of the database cannot control access to the system. For example, an open system could be a database on a remote server that is accessed over the Internet into which eCRF data is entered by a study coordinator. The study coordinator (the person responsible for the content in the database) cannot control who is granted access to the database or the structure of the database. Closed systems are controlled by the person who is responsible for the content and are usually maintained on private computer systems, like a visit tracking system maintained on a clinic's personal computer if an external group cannot access that system. Open systems, which include all systems that use the Internet, require more safeguards, such as encryption when sending data across telephonic lines, than those required for closed systems.

Data integrity issues are paramount to ensuring the validity of the data and its analysis. When data are altered in an electronic record system, the original data must remain visible within the system. The number of users who can alter the data must be limited. There must be an automatic audit trail that logs in the date, time, and source of every entry, decision, or change in the data that cannot be controlled by the user. Additionally, the system must be tested and validated.

Key security measures for electronic records include: limited access to authorized users, documented user-training for all users, password or biometric confirmation of user ID, automatic log-off after the system is idle for a period of time, personnel log-out when leaving the workstation, and encryption of data sent over the Internet. Other security measures relating to both electronic records and electronic signatures include: not sharing

**TABLE 1**  
Four Principles of ERES

1. Provision of System Documentation
  - For all hardware and software including systems used to create, modify, maintain, archive, retrieve, or transmit data
  - Must be retained as part of study records
2. System and Database Security
  - Preventive security measures
  - Pre-determined user rights, IDs, and passwords
  - System "time-outs" that require new log-ins
  - Biometric validation of authorized users
3. Maintenance of Data Integrity
  - Retrievable and identifiable data
  - Data must be attributable to a specific subject
  - Audit trails identifying who altered the data, why it was altered, and when
  - Ability to reconstruct the trial
4. FDA inspection of records
  - All records and files intended to support submissions

All study data must be retrievable and identifiable. Subject data collected in the study must be identified and relate to the actual subject within the database. The integrity of the data must be maintained through security measures, user rights for categories of users determined before the start of the trial, system time-outs built into the system that require a new system log-in, password or biometric validation of authorized users, and audit trails to identify who made entries and other alterations in the database and when.

system, the electronic record is the source document. Many sponsors do not allow this practice; they will require paper source documents or electronic source documents maintained in a separate system to be completed prior to entering data electronically. When an electronic personal data assistant (PDA) is used to collect patient diary data, the PDA and any associated synchronized files are the source documents.

Electronic systems used for data storage are defined as open or closed

IDs or passwords, not allowing one person to log-on for another, linking electronic signatures to the document signed, and implementing safeguards to immediately detect and report unauthorized attempts to enter systems or use signatures. In an emergency (e.g., if the investigator is incapacitated), a person can “authorize” another person to use his/her signature. The process used requires that at least two people collaborate to affix the signature, and the signature must contain information that identifies that someone else attached the electronic signature.

Documents created by word processors or fax machines are not considered electronic records if they are used to type a report or to transmit a paper report. However, if data are sorted, analyzed, or in any way modified, such as sorted columns in Word or calculated fields in Excel, and these data are used in a submission to the FDA, they become an electronic record that must comply with regulations. Systems that track compliance to standard operating procedures (SOPs) are governed by these regulations, as documentation of compliance to SOPs is a required component of regulatory submission. FDA requires a paper affidavit, signed with the traditional handwritten signature, stating that the electronic signature has the same legal significance as the traditional handwritten signature. This is usually submitted prior to or at the time of FDA submission of the study data.

SOPs relating to the creation, maintenance, alteration, transmittal, and retention of an archival copy of the data for review and inspection, must be created and maintained. Documentation must be maintained that describes how the systems used in the specific clinical trial comply with Part 11. An original or a certified copy of source documents must be maintained with the study records, as would be done in a traditional paper trial.

Likewise, electronic records must be maintained for the same amount of time as paper documents, and all records and data must be available upon request for inspection.

#### **Important Points**

If data or records are stored electronically, you cannot avoid compliance with Part 11 by simply printing the data on paper and handwriting a signature. If an electronic system is used to create, modify, maintain, archive, retrieve, or distribute data or records, those records and their related systems are required to comply with Part 11.

However, there are no regulations that require sites to use electronic records. It is totally acceptable for a site to use solely paper records and handwritten signatures, but it is not acceptable to use electronic records without the electronic signature component. Table 2 points out key points to remember.

If your site is not compliant, assess your systems and determine which systems must be compliant. Immediately implement as many safeguards as possible (e.g., time-outs and log-outs necessitating the re-entry of a password to gain access to the system are relatively easy to program). Once the systems have been identified, create a written plan with a timetable and milestones for bringing all systems into compliance. Work aggressively to achieve compliance within your timeline, and if you happen to be audited before you are fully compliant, you may be treated with some leniency by the auditors, especially if your plan has been well thought out and you are within your timelines. Additionally, there are consultants who can help you review your systems and help you develop viable plans to achieve compliance.

**TABLE 2**  
Points to Remember About ERES

- Electronic records are the equivalent of paper records
- Electronic signatures are the equivalent of traditional handwritten signatures
- Electronic records and signatures may be submitted to FDA in lieu of or in combination with paper records and handwritten signatures
- Handwritten signatures affixed to printed copies of electronic records are not acceptable

#### **The Need for Immediate Compliance**

21 CFR Part 11 went into effect in August 1997, yet, many sites are still not compliant. Non-compliant sites can be sanctioned with warning letters and FDA Form 483s. Noncompliance is considered a data integrity issue. If the FDA feels that your system is out of compliance to the point where it has compromised the integrity of the data, the agency could reject all of the data from the trial or the site.

Options for compliance include maintaining records solely in paper form (which does not require compliance with ERES) or using only certain systems requiring compliance to Part 11 along with other systems and methods utilizing traditional paper records (in this case, ERES requirements apply only to the electronic systems).

At the start of a study, the site is required to determine which computer or other electronic systems will be used and document this in your study files; this includes

systems at your site and those provided by the CRO or sponsor. Regardless of who owns the systems, you must keep a record describing all systems. If no electronic systems are used in the study, a record of that should be made in a memo to the file, and that memo should be maintained in the study records.

### **Conducting Studies Using Remote Data Capture**

The paradigm for conducting studies using remote data capture is changed from that of paper trials. There is more preparation time at the start of a remote data capture trial, less database maintenance during the trial, more training required, and less cleaning at the end of the trial before database lock. It takes about three months to build the database, write the edit checks and program the crosschecks. During this time, roles and responsibilities are identified and user rights assigned (e.g., does this role require read, write, or query capabilities or some combination?). These systems provide the ability for continuous monitoring of safety data throughout the trial, and ongoing data cleaning. It is not unrealistic to expect that the time from last patient visit to database close will be significantly reduced, thereby reducing the time to final analysis and study report.

Planning for remote data capture studies is crucial. All parties must review and approve the e-CRF and the data management plan before the trial can move forward. The database, along with the rules, queries, and cross-checks, must be built and “go live” before the investigator meeting so that all site users (e.g., investigators and coordinators) can be thoroughly trained and qualified to use the system. Documentation of this training must be maintained in the study files. As staff transition off the project and new staff are brought on the project, they, too, must be trained and qualified to use the system. Once staff are trained

and certified, their user rights can be activated, depending on the role they are playing in the study. In a paper-based data management system, the site enters data into the source document. From there, the clinical research coordinator usually transposes those data onto a case report form. The monitor or clinical research associate (CRA) does source document verification and CRF querying of data discrepancies. Once the CRFs are relatively clean, they go to the data management center where a data entry person enters the data, usually using double data entry to reduce discrepancies between the CRF and the database. The clinical data manager generates the edit checks and prepares data queries that are sent to the site for resolution. Oftentimes, because it is not crucial to build the database in a paper trial prior to its start, these edit checks are run so late in the trial, that you cannot learn from the errors. Along with these issues is the fact that most databases require prolonged cleaning beyond the end of the trial. In an Internet-based data management process, source data, regardless of its origin, is entered into the database directly via the eCRF. The eCRFs are transmitted via the Internet through a firewall into the data management software system. Pre-programmed edit checks provide automatic feedback when data are entered incorrectly. The CRA and data manager interact regularly; in most trials, these functions become blended with the monitor performing various tasks traditionally performed by the data manager.

Using an Internet or web-based system, the query process is largely automatic, but there are usually provisions for reviewers (e.g., monitors and statisticians) to also enter manual queries. Some systems allow for new queries to be categorized as “open”. After the site responds, the query is categorized as “answered”. The monitor then reviews the query and either “closes” it or re-issues another query

asking for clarification. In the case of an automatic query, the system reviews the answer to the query and can close it if the rules have been satisfied.

The eCRA should embrace the technology and have the right tools. He/she should understand the technology and be able to fulfill a blended role (clinician, data manager, and troubleshooter). Sites selected for e-trials should: have the necessary connectivity (hardware and software); embrace the technology (be computer savvy and experienced with electronic data capture); and meet the traditional selection criteria for staff, time, facilities, and therapeutic expertise.

Preparation for the conduct of an e-trial is not limited to the data collection instruments, but includes multiple preparations and thought. Many documents must contain statements related to the e-trial. The protocol must contain a statement regarding the computer systems to be used. Subject information and informed consent should address data transfer and privacy. Paper and electronic affidavits must be appropriately completed. Sponsors and CROs should provide sites with guidance on 21 CFR 11.

### **Conclusion**

Electronic data capture, or e-trials, are subject to 21 CFR Part 11, otherwise known as ERES regulations. This brings new concerns and technology to the arena of clinical trial conduct. Security issues are paramount. Monitors are being asked to do tasks that were traditionally done by data managers and to assume the role of trainers along with other technology-related roles. There is potential for improved overall timelines, however, the overall work product of an e-trial requires at least as much effort as traditional trials. Design and development of a working database is completed early, before study start-up, with relatively little clean up at the end of the study.