As clinical trials increase in number and complexity, electronic solutions claim a growing presence in the effort to improve data collection, transmission, storage and retrieval. Sponsors are moving towards electronic alternatives to introduce speed and greater reliability into these data-driven processes that, historically, have been paper-based.

This transition raises significant challenges, most notably, how to implement electronic solutions so that the resulting electronic records are considered equivalent to paper records, and electronic signatures are considered equal to handwritten ones. In recognition of this concern, the Food and Drug Administration (FDA) issued 21 Code of Federal Regulations (CFR) Part 11 on August 20, 1997 (1). Known as “Electronic Records; Electronic Signatures (ERES)”, or more simply “Part 11”, this final rule establishes regulations and criteria for acceptance by the FDA of electronic records, electronic signatures and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. It applies to records and systems meeting any FDA records requirement – including laboratory, manufacturing and clinical data management systems.

The final rule is the result of a six-year process, starting in 1991, when members of the pharmaceutical industry met with the FDA to explore how they could accommodate paperless record systems under the current good manufacturing practice (cGMP) regulations in 21 CFR Parts 210 and 211. Out of these meetings came: a task force; a working subgroup; a 1992 publication in the Federal Register that the FDA was considering the use of electronic identification and signatures; a proposed rule in 1994; and ultimately, the final rule three years later.

21 CFR Part 11 Overview

The final rule is divided into three Subparts: General Provisions, Electronic Records and Electronic Signatures. Within these three sections, Part 11 states the scope of the rule, provides definitions, and states that people using the system are to employ procedures and controls designed to ensure the authenticity, integrity and – when appropriate – confidentiality of electronic records. In addition, systems must be in place so that the signer cannot easily repudiate the signed record as not genuine.

Part 11 Subpart B (Electronic Records) lists eleven components that define the types of procedures and controls needed to comply with these requirements. A sampling of these elements appears in Table 1.

This section distinguishes between open and closed systems, and explains how each configuration must comply with the eleven components. According to Part 11, when access to the system is controlled by people who are responsible for the content of those electronic records, the system is considered to be closed. The open system is an environment in which system access is not controlled by individuals responsible for the content of electronic records appearing on the system.
Security

Validation of systems to ensure accuracy, reliability, and certifiability of Electronic Signatures

Certification of Systems

Standard Operating Procedures

Records Inspection

Data Entry

System Controls

General Principles

Training of Personnel

Innovations in Clinical Trials does an investigator achieve this audit trail while also discerning the date and time of operator entries and actions that create, modify or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

Consequently, open systems may require more measures to ensure the authenticity, integrity and confidentiality of the records from the point of their creation to the point of their receipt.

The final part of the rule, Subpart C, addresses the electronic signature and defines it as “a computer data compilation of any symbol or series of symbols, executed, adopted, or authorised by an individual to be the legally binding equivalent of the individual's handwritten signature.” This section further explains the components of electronic signatures, and delineates between signatures that are based on biometrics and those that are not. According to the rule, whether or not an electronic signature is based on biometrics, steps must be taken to ensure that it cannot be used by anyone but the owner of that signature.

(Biometrics refers to the use of automated methods to verify an individual’s identity based on measurement of that individual’s physical features and/or repeatable actions that are unique to that individual. Examples include fingerprints, voice patterns, retinal or iris scanning, facial recognition and hand geometry.)

Interpreting the rule

As with any new rule, questions arise during the implementation phase. For example, Subpart B, Section §11.10(e) refers to the creation of a secure audit trail to “independently record the date and time of operator entries and actions that create, modify or delete electronic records”. How, exactly, does an investigator achieve this audit trail while also protecting the authenticity, integrity and confidentiality of those electronic records? Who shall maintain it? How are the electronic records in the audit trail to be archived and protected to enable their accurate and ready retrieval throughout the records retention period and beyond? [Sec §11.10(c)]

These questions and many others require official input from the FDA to avoid the rule dissolving into a confusing, labyrinth of self-serving, individual interpretations. FDA input came in the form of Computerized Systems Used in Clinical Trials (2), a Guidance for Industry released in April 1999. According to the Guidance, it was developed for two related purposes: to address requirements of 21 CFR Part 11, and to provide the agency's current thinking on issues pertaining to computerized systems used to create, modify, maintain, archive, retrieve or transmit clinical data intended for submission to the FDA.

The Guidance is organised around the principle that in order for these data to be acceptable to the agency, they should meet certain fundamental elements of quality, whether collected electronically or on paper. Data in source documents should be Attributable, Legible, Contemporaneous, Original, and Accurate – ALCOA for short. The Guidance describes how computerized systems, standard operating procedures and validation processes should be designed to generate data that are ALCOA. The elements discussed in the Guidance are listed in Table 2.

Table 2

Overview of Guidance for Industry: Computerized Systems Used in Clinical Trials

- General Principles
- Standard Operating Procedures
- Data Entry
- System Features
- Security
- System Dependability
- System Controls
- Training of Personnel
- Records Inspection
- Certification of Electronic Signatures

Key highlights of the Guidance

All parts of the Guidance merit attention, but some sections have gained particular visibility, such as Data Entry, System Features and System Dependability.

* Although data must meet certain quality standards whether collected electronically or on paper, the Guidance focuses on issues surrounding electronic collection and recording.

What is a Digital Signature?

A digital signature is made up of two components, a one-way hash and an encryption key system, authenticating the identity of the sender, and assuring the reader that the document he or she is reading is identical to the one that was signed. These elements also prevent the signer from repudiating that digital signature.

A one-way hash is a technologically term that refers to the transforming of a string of characters to encrypt and de-encrypt digital signatures. The signer creates a hash and then uses the key system to encrypt that hash. This system is composed of a private and public key. Both are produced mathematically and are related, but neither can be derived from the other. The private key belongs solely to the signer, whereas the public one, as the name suggests, is publicly known.

The recipient makes a hash of the received data or message and opens it with the public key. If the hashes match, the received message is valid. If the signer has modified the encrypted message, the public key will not open it.

Digital signatures may eventually be a good method to satisfy requirements of data authentication, integrity and confidentiality, but presently, there are various unresolved issues. The private key must be stored either on a computer or on a smart card. Strict controls are needed to prevent fraudulent use by another individual. The creation of the private key requires absolute confirmation of the identity of its owner. Ideally, this should be done in person, thereby creating an administrative burden. Also, for investigative sites housing data locally, which is the vast majority of sites, validation of that software is required.

Sources: www.whatis.com and www.phaseforward.com
Data Entry, Section 5 in the Guidance, takes a look at electronic signatures, audit trails, and date and time stamps – subjects mentioned in the final rule. A proper electronic signature is the first step in making sure that individuals have the authority to proceed with data entry. It is also a tool used to ensure data attributability. The Guidance suggests that attributability results when all entries to electronic records, including all changes, are made under the electronic signature of the individual authorised to make that entry. The person’s name is to be displayed during the data entry session; passwords are to be changed at prescribed intervals; individuals are not to share their passwords; and when leaving the data entry station, the individual is to log off, or the system should log off automatically after a period of inactivity.

The electronic signatures executed to electronic records are to be linked to their respective electronic records to ensure that they cannot be removed, transferred or falsified (§11.70). The preamble of 21CFR Part11, which is essential to interpreting the final rule, is flexible on the method of linkage. It states: “While requiring electronic signatures to be linked to their respective electronic records, the final rule affords flexibility in achieving that link through use of any appropriate means, including use of digital signatures and secure relational database references.”

The digital signature is a type of electronic signature that can serve to link the signature to the document being signed. It can be time- and date-stamped and cannot be imitated by anyone else. When open systems are used, additional controls may be needed to ensure that digital signatures satisfy the data requirements (§11.30). A secure relational database reference means that the signature and the data are securely linked within the database. Use of this method requires proper security to assure that database access is adequately controlled and audited.

Audit trails must be developed to ensure the authenticity, integrity and confidentiality of electronic records. They must also record all operator entries and actions that create, modify or delete e-records, and include a date and time stamp. Through the audit trail, data can be retrieved, and if necessary, the study can be reconstructed by the FDA.

According to the Guidance and to the final rule, audit trails are to be retained for a period at least as long as required for the electronic records in question, and must be available for agency review and copying. Study-related records – electronic or paper-based – must be retained by the investigator for a period of two years following the date a marketing application is approved for the indication under investigation, or is either abandoned or not approved (Table 3). The investigator must maintain the associated audit trail, or a certified copy of it, for the same duration. This could easily translate into ten years or more. International Conference on Harmonisation (ICH) guidelines for Good Clinical Practice suggest that records can be retained even longer. Section 4.9.5 describes a retention period similar to what is stated in Table 3, but adds that records may need to be kept longer if required by the applicable regulatory requirements or sponsor.

<table>
<thead>
<tr>
<th>Table 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>“An investigator shall retain records for a period of two 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 two years after the investigation is discontinued and FDA is notified.”</td>
</tr>
<tr>
<td>Source: 21 Code of Federal Regulations Part 312.62(c)</td>
</tr>
</tbody>
</table>

Questions arise as to how all aspects of the data, audit trail and system configurations can be maintained for such a lengthy period. Sponsors and investigative sites would be hard-pressed to sustain old computer systems and the ability to run older versions of software for this exclusive purpose. To address this concern, Sections 6C and 6D of the Guidance suggest that the data and metadata can be migrated to newer systems, as long as the migration pathway is validated and carefully done to maintain data integrity. Anything less can result in the loss of data formatting, metadata and footnotes that provide additional interpretation. Once data are migrated, originals are generally destroyed, and any changes to the data are permanent.

An effective migration process might involve archiving data and metadata in a widely-used, standard, text-based format. Extensible Markup Language (XML) – a set of technologies and guidelines for designing text formats that structure data – is a good choice as it enables the saving of data and metadata in text-based files, and is easy to use on the Web. This format should be readable through

---

1 According to the Guidance, a certified copy refers to a copy of original information that has been verified, as indicated by dated signature, as an exact copy having all of the same attributes and information of the original.

---

Innovations in Clinical Trials
many generations of technological advance, as it allows people to read data without the program that produced it (3).

XML can be modified to manage the structure and components of clinical trial data through the development of a clinical trial Document Type Definition (DTD). A DTD defines a structure for “generic” XML that encompasses the various data structures needed to transmit clinical trial data. By sending a DTD along with an electronic document, clinical trial data can be transferred from user to user, computer to computer and application to application, without the need for data mapping. Several vendors have developed DTDs. Also, the Clinical Data Interchange Standards Consortium (CDISC), a non-profit organisation that develops worldwide industry standards to improve electronic data quality, has developed and published the Object Data Model Version 1.1, a model for developing a common DTD for the entire industry that, among other things, supports data archiving.

Data migration requires a strategic plan that is constantly being evaluated. This includes documenting and monitoring the data types used as well as the hardware, software and file structures. As new technology is introduced, users should make decisions about the need to migrate old data.

**What is computer system validation?**

As electronic processes become the preferred method of data collection, transmission and archiving, sponsors and investigators need a way to confirm that the hardware and software systems handling those electronic records and associated electronic signatures are maintaining data integrity, are performing as intended, and will continue to perform over the life-time of those systems. The approach, known as validation, is a series of steps only hinted at in the Guidance. In fact, the Guidance provides a brief definition of software validation (Table 4) and mentions validation just three times, using vague statements such as: “The transcription process needs to be validated” [Sec 6(c)]; or “The impact of any change to the system should be evaluated and a decision made regarding the need to re-validate.” [Sec 8(c)]. No further explanation is offered.

So how, exactly, is the computer system validated? Although a detailed discussion is beyond the scope of this article, the mentioning of a few basic points is in order. First, systems require rigorous formal testing of all components, traceability throughout the process and ongoing management oversight. Responsible parties need to: develop a validation plan; determine best practices; ensure that clinical data accurately reflect source data; test computers at the investigative sites, network connections and the central server (if one is used); plan for disaster recovery of data from the system, application or network; and develop standard operating procedures (SOPs) for initial system set-up and installation, data back-up and retrieval, and change control. Many of these points are also alluded to in ICH Section 5.5, Trial Management, Data Handling, Recordkeeping, and Independent Data Monitoring Committee.

Validation of the data entry mechanism at investigative sites is a function of the system architecture. There are four site-based system configurations for data collection:

1. Systems with local PC applications and data,
2. Systems with local PC applications and off-site database,
3. Systems with no local applications and off-site database, and
4. Systems with local server and synchronisation to off-site server.

An investigative site that houses software and data locally will face substantially more validation issues and will need to adopt more SOPs than a site using thin-client architecture, meaning there is no local software, merely a Web browser, and data residing on a central server. For example, a site with local PC applications and local data needs to validate all aspects of the hardware and software as well as develop associated SOPs such as one for system lockdown to prevent someone from walking off with the system, or loading or downloading additional software that could modify or compromise the integrity of the data contained within. Thin clients only have to validate and develop SOPs for the Web browser and the operating system.

A Draft Guidance entitled Guidance for Industry 21 CFR Part 11; Electronic Records; Electronic Signatures Validation (4) was released in August 2001, and provides a sense of the many issues surrounding validation. It focuses on the...
principle that in order for the system to consistently perform as intended, the end-user must first establish what those needs and intended uses are. Once this has been established, the system user must obtain evidence that the computer system implements those needs correctly and that they are traceable to the system design requirements and specifications. A sampling of key principles appears in Table 5.

A final note
As clinical partners gear up for greater use of e-solutions in clinical studies, a lot of thought must be directed towards their implementation in accordance with 21 CFR Part 11, the Electronic Records; Electronic Signatures final rule. Whereas the rule details required steps that must be taken before the FDA will consider electronic records affixed with electronic signatures to be equivalent to their paper and handwritten alternatives, the Guidance provides further definition and the agency’s current thinking on the subject.

The Guidance covers a whole host of subjects (ranging from standard operating procedures to audit trails to data archiving) so that the resulting data, like paper data, are attributable, legal, contemporaneous, original and accurate. It also makes the point that electronic solutions may seem more elusive and less physical than paper documents, yet electronic signatures on electronic source documents are every bit as legally binding as their paper relatives. The Guidance discusses that safeguards must be in place so that access to data and the computer systems generating them is restricted to authorised personnel. The intent is to maintain the authenticity, integrity and confidentiality of the data and avoid fraud.

Going forward, Part 11 compliance issues will continue to surface, as evidenced by its impact on various systems configurations and the fact that a new draft guidance has been released, focusing on validation. One section of that draft guidance discusses the challenges inherent in trying to validate the Internet – an infrastructure that is beyond the control of any one individual or company, yet is destined to be involved in all aspects of data handling and the systems designed to handle those data.

<table>
<thead>
<tr>
<th>Table 5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Some Key Principles from the Draft Guidance</strong></td>
</tr>
<tr>
<td><strong>21 CFR Part 11; Electronic Records; Electronic Signatures Validation</strong></td>
</tr>
<tr>
<td>• System Requirements Specifications</td>
</tr>
<tr>
<td>• Validation Plan, Procedures and Report</td>
</tr>
<tr>
<td>• Equipment Installation</td>
</tr>
<tr>
<td>• Key Testing Considerations</td>
</tr>
<tr>
<td>• What Software Testing Should Include</td>
</tr>
<tr>
<td>• Extent of Validation</td>
</tr>
<tr>
<td>• Change Control</td>
</tr>
<tr>
<td>• Considerations for Commercial, Off-the-Shelf Software</td>
</tr>
<tr>
<td>• Internet Validation</td>
</tr>
</tbody>
</table>

Paul Bleicher is Chairman and CEO of Phase Forward Incorporated. He brings to Phase Forward more than 11 years of experience in the design, implementation and analysis of clinical trials from both the sponsor and clinical investigator perspective. Before founding Phase Forward, he was Vice President, Clinical Affairs, at Alpha-Beta Technology, Inc.; prior to this, he served as a Medical Monitor and Director of Early Phase Services at PAREXEL International. Dr Bleicher currently serves on the Drug Information Association Steering Committee of the Americas; he also serves on the Editorial Board of Applied Clinical Trials. He obtained an MD and PhD (Microbiology) from the University of Rochester and also trained in Internal Medicine and Dermatology at Harvard Medical School, where he was a founding scientist of the Harvard/MGH Cutaneous Biology Research Center.

References