Comply with Federal Regulations

Controlling the Electronic Transfer of Clinical Trial Data:

Practical Advice

The FDA... must have the same degree of confidence in the results of computerized systems as it has in the results of paper-based systems.

by
Leonard A. Grunbaum
President
META Solutions, Inc.

Title 21 CFR Part 11, the regulation relating to electronic records and electronic signatures, lays out the requirements to enable the Food and Drug Administration (FDA) to have the same degree of confidence today that it had in the "good old days" of paper-based systems, with all of the attendant paper records, bulging file cabinets, and the like. The regulation was deemed necessary because the electronic transfer of clinical trial data – in reality, the use of computerized systems to support the entire research and development process – is here and has been for some time. Nevertheless, the Agency still must provide timely review and approval of safe and effective new medical products, conduct efficient audits of required records and, when necessary, pursue regulatory actions.[1]

Electronic Case Report Form systems, distributed processing systems, web-based systems for capturing data, Internet chat rooms for individuals involved in a given clinical trial, and the use of e-mail to communicate data are just some of the examples of technology involved in the electronic transfer of clinical trial data. The reason for using such technology is fairly simple: Companies need to increase processing effectiveness and efficiency to minimize expenses and maximize profitability. The impact of this phenomenon is not so simple. While technology has advanced significantly, the mandate of the FDA – to promote and protect the public health – has remained constant; it must have the same degree of confidence in the results of computerized systems as it has in the results of paper-based systems.

Effective and efficient compliance with the regulation involves several major factors. The first, of course, is to understand the regulation's requirements and the meaning behind them. These are the rules of the game, and if you want to play in this

league you must understand the rules. Next, one must be familiar with current Agency thinking with respect to enforcement. This is important in providing a context within which to make the cost/benefit decisions required when developing an implementation strategy. The final element is developing the implementation strategy itself.

This article provides an easy-to-understand analysis of the regulation and the Agency's current thinking regarding enforcement, as well as practical advice to help you develop an effective and efficient compliance strategy.

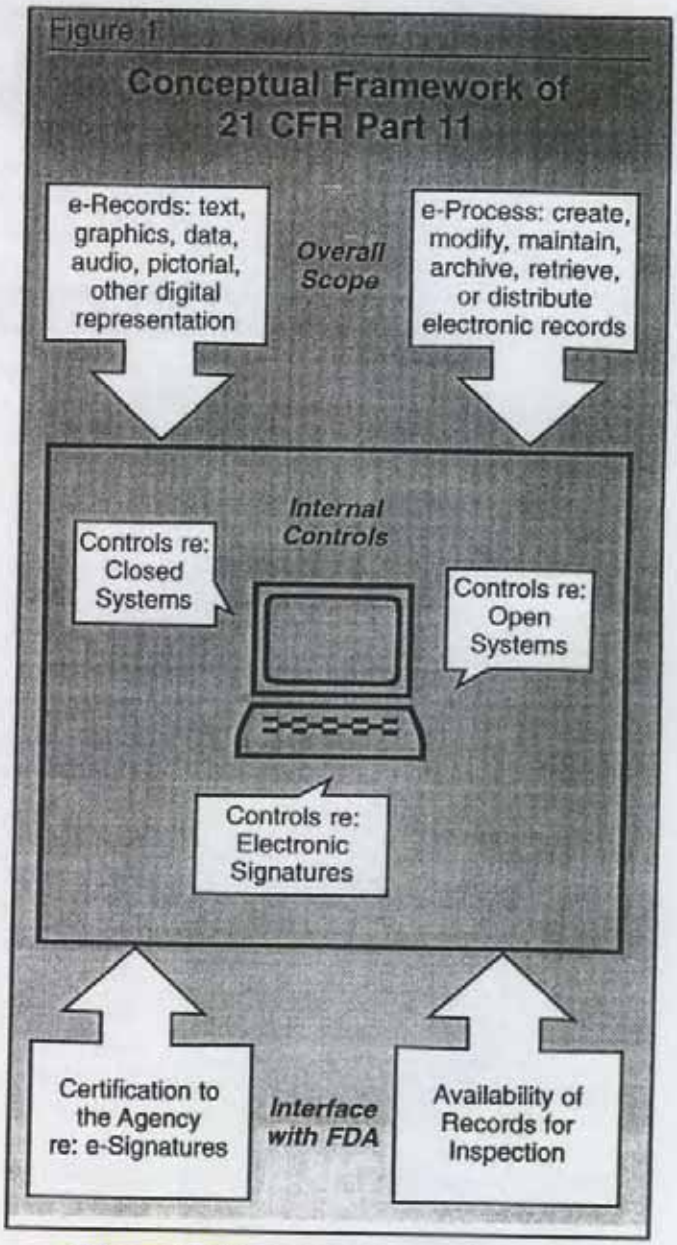
What Does the Regulation Say?

21 CFR Part 11 provides "...the criteria under which the Agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper."[2] In other words, "[p]ersons using the data from computerized systems should have confidence that the data are no less reliable than data in paper form."[3] These criteria can be categorized as follows:

- **Overall Scope** – what the regulation applies to
- **Interface with FDA** – where and how the company and Agency deal directly with each other
- **Internal Controls** – the specific controls that the company implements to ensure trustworthiness and reliability of information

The conceptual framework of the regulation is illustrated in *Figure 1*.

Figure 1



Overall Scope

The perspective of the regulators is that computerization is performing exactly the same functions today as paper-based systems have in the past, and they have quantified the scope of the regulation to include all manifestations of electronic processing. Therefore, the regulation covers the following:

- Electronic records, which are "any combination of text, graphics, data, audio, pictorial, or other information represented in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system"[4] under any records requirements found in Agency regulations.
- Computer systems that are used to "create, modify, maintain, or transmit electronic records."[5]
- Electronic signatures – "a 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"[6] – which may be used when handwritten signatures are a less effective/efficient means of processing.

While the regulation seems broad in its scope, it does not apply if you are still exclusively using

paper-based systems to create, modify, maintain, or transmit records of regulatory significance. The problem here, of course, is that you are probably not using paper-based systems very much, if at all, since it is hard to be competitive in today's marketplace if you don't take advantage of technology. So, if you are processing data that has any regulatory significance, the regulation probably applies to you. More specifically, these regulations definitely apply if you are using a computer system to store an electronic representation of any information or process that is FDA-regulated.

Interface with FDA

The regulation identifies two specific instances wherein the company interfaces directly with the FDA. The first is the requirement for the company to certify to the Agency that electronic signatures "used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures."[7] The intent is to ensure that management and individuals who use electronic signatures are accountable for their signatures; that is, people would be as careful when affixing an electronic signature as they are when providing a handwritten signature. This is your way of informing the Agency that they can have confidence in the propriety of any electronic signatures they encounter in the course of inspecting your records.

Which brings up the second area of interface: the Agency inspection. The Agency must have the ability to inspect your records and systems to confirm that reliance can be placed on the information provided for review. Inspecting paper systems is relatively easy. Inspecting electronic processes, including magnetic media, is somewhat more complex. Therefore, you must have the "ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the Agency."[8] Think of it the same way as you think of a specimen supplied for a medical examination; there is no way to do a proper examination unless the appropriate fluids are available for testing. With respect to electronic records and signatures, there is no way to do a proper inspection unless the inspector can rely upon the completeness and accuracy of a readable copy of the electronic data.

Internal Controls

The regulation identifies specific controls that should be in place to help ensure "the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine."[9] These controls are as follows:

Controls for Closed Systems

The regulation identifies closed systems as "an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system."[10] The intent of Subpart B, § 11.10, is to indicate what controls companies should have to allow the Agency to rely on the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to be able to ensure that the signer cannot readily repudiate the signed record as not genuine. In summary, these controls are designed to ensure that:

- The system is developed and tested properly (section [a])
- Auditable records can be generated (section [b])
- Any record can be readily retrieved (section [c])
- Only authorized access to records is permitted (section [d])
- Appropriate audit trails are generated, retained, and auditable (section [e])
- Proper operational sequences are followed (section [f])
- Only authorized processing is permitted (section [g])
- Only complete and accurate data is transmitted from devices (section [h])
- Only qualified individuals are involved in the respective process (section [i])
- Appropriate policies are developed regarding individual accountability for electronic signatures* (section [j])
- Documentation is controlled (section [k])

**§ 11.50 and §11.70 provide additional guidance regarding policy requirements to foster accountability. The former section indicates that the system must have the ability to relate a signed electronic record to the following: the printed name of the signer, the date and time of execution, and the*

meaning of the signature (e.g., review, approval). This is to ensure that the signer is accountable for the electronic signature and that it can be effectively interpreted. The latter section provides the requirement for the system to inhibit the ability to use the electronic signature in an unauthorized way (e.g., cannot be copied or transferred). This is to ensure against electronic "forgery."

Controls for Open Systems

The regulation identifies open systems as "an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system."[11] An example of this would be an unsecured web-based system for transmitting data. Subpart B, § 11.30, states that the controls for closed systems apply to open systems as well. There is, however, the additional requirement to ensure the appropriate controls through the whole of the transmission process from the point of creation to the point of receipt. Thus, methods such as digital encryption would be required to maintain the authenticity, integrity, and when appropriate, the confidentiality of electronic records when they are transmitted over an open system.

Controls Regarding Electronic Signatures

Subpart C, § 11.200, requires that a company that plans to utilize electronic signatures use either biometric measures or a combination of identification codes and passwords. Biometrics – "a means of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable"[12] – should be designed to ensure uniqueness (i.e., usable only by the genuine owner). With respect to electronic signatures based on identification codes and passwords, controls must be in place to ensure that attempted unauthorized use of an individual's electronic signature requires collusion on the part of two or more individuals.

As provided for in Subpart C, § 11.300, controls are required to ensure the security and integrity of identification codes and passwords. The controls should be designed to ensure that:

- Each identification code/password combination is unique (section [a])
- Identification code/password combinations do not become obsolete (section [b])
- Lost, stolen, missing, or otherwise compromised objects containing identification codes/passwords (e.g., identification cards) are properly disposed of (section [c])
- Adequate measures are employed to prevent unauthorized used of passwords and/or identification codes, and to detect and report such use immediately (section [d])
- Initial and periodic testing of all objects containing identification codes/passwords (e.g., identification cards) to ensure continued proper functionality (section [e])

What is the Current FDA Thinking?

You are probably asking yourself "What was the Agency thinking?" The more appropriate question, however, is "What is the Agency's current thinking regarding enforcement of the regulation?" In a recently issued Compliance Policy Guide,[13] the Agency provided insight into the current thinking regarding enforcement of the regulation. The following points are of special interest as you weigh potential risk factors while attempting to comply with the regulation:

- While 21 CFR Part 11 does not grandfather legacy systems, the Agency will expect that companies will be proactive in developing plans to bring their legacy systems into compliance. This means that such plans should be available for inspection should the Agency pay you a visit.
- There is no overall threshold that will automatically result in regulatory actions on the part of the Agency. Decisions regarding the pursuit of such actions will be made on a case-by-case evaluation. The policy guide indicates that the evaluation "may" include the items described below. I suggest that you read this as the degree of Agency concern will be greater to the extent that:
  - There are numerous deviations from 21 CFR Part 11, and the deviations are such that data integrity can be compromised, records are not available for audit, electronic signatures can be disavowed or compromised, etc.
  - The deviations can be shown to have a direct effect on product quality and data integrity, such as the potential for performing unauthorized data changes or pro-

cessing activities coupled with no audit trail capability to document the activities that take place
- The company does not have an effective plan for remediating 21 CFR Part 11 deficiencies in a timely manner
- The company has a history of 21 CFR Part 11 violations or of ineffective or unreliable record keeping

So, How do I Comply?

Here is a four-step approach to help you comply with 21 CFR Part 11:

Step ❶ – Know the Rules

There are three documents you must read to be able to understand the rules of the game, and they are all available on the FDA web site (www.fda.gov). These documents are:

- 21 CFR Part 11 Electronic Records, Electronic Signatures; Final Rule[14]

  This is the regulation (i.e., the rulebook) itself. You need to understand the provisions before you can determine how best to comply with them. Note: The 30-plus page Preamble provides significant insight into the FDA interpretation of the final rule, which is approximately two pages in length.

- Guidance for Industry: Computerized Systems Used in Clinical Trials[15]

  This document addresses "...long-standing regulations covering clinical trial records, [including] requirements of the Electronic Records/Electronic Signatures

Figure 2

Sample 21 CFR Part 11 Checklist

CFR Part 11	Yes	No	N/A	Comment/Impact of "No" Answer
Subpart B – Electronic Records				
Section 11.10 Controls for closed systems				
1. Has the system been validated to ensure:				
a. Accuracy?				
b. Reliability?				
c. Consistent intended performance?				
d. The ability to discern invalid or altered records?				
2. Does the system have the ability to generate accurate and complete copies of records suitable for inspection, review, and copying by the Agency in both:				
a. Human-readable form?				
b. Electronic form?				
3. Are records protected to enable their accurate and ready retrieval throughout the records retention period?				
4. Is system access limited to authorized individuals?				
5. Are secure, computer-generated, time-stamped audit trails used to independently record the date and time of operator entries and actions that:				
a. Create electronic records?				
b. Modify electronic records?				
c. Delete electronic records?				

rule..." It provides a good overview of the regulation.

- Enforcement Policy: 21 CFR Part 11; Electronic Records; Electronic Signatures (Compliance Policy Guide Section 160.850)[16]

  This document "...represents the Agency's current thinking on how to comply with the regulations for electronic records and electronic signatures."

Step ❷ – Know Thyself

At the System Level

You need to develop an inventory of all clinical systems in your company and, for each, determine if 21 CFR Part 11 is applicable. If the following questions are answered "yes," the regulation is applicable to the respective system:

- Is the process or the applicable data covered under an existing FDA regulation?
- Is a computer system involved in the process?
- Is the computer system being used to create, modify, maintain, archive, retrieve, or transmit data?

An analysis should be performed for each applicable system to identify potential regulatory issues. An effective tool to use in this instance is a formal checklist incorporating the regulations' provisions as criteria to be measured. *Figure 2* illustrates what such a checklist would consist of for a portion of section 11.10.

Each provision would be listed down the left side of the checklist in the form of a question, and each question requires a "yes" or "no" answer, except for issues that are obviously not applicable (e.g., controls for "open systems" are not applicable if the system is "closed"). Each "no" answer should be evaluated as to its significance as described above.

At the Corporate Level

At the corporate level, you should determine if policies and procedures are conducive to developing and deploying systems that are compliant to 21 CFR Part 11. That is, controls are needed to help ensure that validated systems are developed, deployed, and maintained, and that one's accountability for activity regarding electronic records is established and maintained. Applicable elements of controls encompass, but are not necessarily limited to:

- A current inventory of all hardware and software, including the network architecture, to document what you have and where it's located
- A current organizational chart and job descriptions to document the appropriateness of the organization's structure
- Policies and procedures (i.e., SOPs) that provide for system validation, development and deploying systems according to a formal methodology, physical and logical security, backup and recovery, system operations, staff training, change control, contingency planning, and use of purchased systems
- Effective audits and inspections of computer systems and related processes by Quality Assurance
- For each computer system that falls under the scope of the regulation:
  - Documentation of what the system is supposed to do (e.g., functional requirements)
  - Documentation of how the system works (e.g., technical specifications)
  - Documentation of the applicability of the specific electronic records/signature provisions and how the specific requirements of the regulation are being addressed in the system
  - Formal test plans and documented test results, with traceability to functional requirements and technical specifications, and appropriate tests of stress/limits boundary conditions
  - Evidence of validation (e.g., validation plan, validation summary, installation/operational/performance qualifications)

The Agency must have the ability to inspect your records and systems to confirm that reliance can be placed on the information provided for review.

Step ❽ – Develop a Remediation Plan

You will need to develop a plan to address the issues identified for each applicable system, per Step 2. The plan should have the following characteristics:

- The systems should be stratified in order of risk to the company. For example, a mission-critical legacy system with significant deviations should have a higher priority than a non-mission critical system with few current issues
- For each system, the specific issues should be identified along with the specific correction
- Roles and responsibilities, resource requirements, milestones, and target dates should be provided
- The plan should be reviewed and approved by appropriate representatives of Management, Information Technology, and Quality Assurance

This plan should be available to the Agency should they arrive at your company for an inspection.

Step ❾ – Implement the Plan

The activities provided in the plan should be addressed in the order of significance. The person(s) responsible for the completion of the plan should provide status information to Management on a regular basis. Changes in business conditions or project priorities should be reflected in the plan and a new plan developed if appropriate. At the completion of the effort, a summary report should be generated which reflects the work performed, deviations from the project plan, and overall conclusions regarding compliance with Part 11.

Summary

When you get behind the regulatory language, 21 CFR Part 11 provides the requirements for well-controlled use of computer systems. The clinical trials context heightens the need for these controls over the technology; poor controls could result in great harm to people and large problems for companies. But this is the game we're involved in, so we must always look for practical ways to compete and do well. ❑

About the Author

Len Grunbaum is the President and Chief Operating Officer of META Solutions, Inc. He is responsible for all operational aspects of the company, and the management of all aspects of the Validation Consulting Services to the pharmaceutical industry. Len has a Bachelor of Arts degree and a Masters of Business Administration degree from Long Island University. He was a Director of the EDP Auditors Association and is a member of the Drug Information Association (DIA). Len is the author of Do It Right The First Time: A Handbook for Controlling Technology Through Good Validation Practices, *published in the February issue of the* Journal of Validation Technology. *He has also presented validation and audit-related training sessions to clients and professional groups. Len can be reached by phone at 732-845-4904, by fax at 732-845-4834, and by e-mail at len_g@metasol.com.*

References

1. *Federal Register*, 64(146), Friday, July 30, 1999/Notices, p. 41442.
2. Code of Federal Regulations, Title 21, Food and Drugs, Part 11, "Electronic Signatures: Final Rule," *FDA Federal Register*, 62(54), pp. 13429-13466 (20 March 1997) p. 13464.
3. FDA, Guidance for Industry: Computerized Systems Used in Clinical Trials, April 1999, p. 2.
4. Code of Federal Regulations, Title 21, Food and Drugs, Part 11, "Electronic Signatures: Final Rule," *FDA Federal Register*, 62(54), pp. 13429-13466 (20 March 1997) p. 13465.
5. Ibid.
6. Ibid.
7. Ibid, p. 13466.
8. Ibid, p. 13465.
9. Ibid.
10. Ibid.
11. Ibid.
12. Ibid.
13. Federal Register, 64(146), Friday July 30, 1999/Notices, pp. 4142-41443.
14. Code of Federal Regulations, Title 21, Food and Drugs, Part 11, "Electronic Signatures: Final Rule," *FDA Federal Register*, 62(54), pp. 13429-13466 (20 March 1997).
15. FDA, Guidance for Industry: Computerized Systems Used in Clinical Trials, April 1999.
16. *Federal Register*, 64(146), Friday, July 30, 1999/Notices, p. 41442.