Remaining in a 21 CFR Part 11 Compliant State

Remaining compliant with 21 CFR Part 11 requires many individual activities and the involvement of many individuals and groups.

by
Leonard A. Grunbaum
President and Chief Operating Officer
META Solutions, Inc.

This article provides practical advice for remaining in compliance with 21 CFR Part 11, the Electronic Records; Electronic Signatures Final Rule.[1] It is directed at those who are responsible for maintaining this compliance. And just how do we do this? Descartes, in his *Discours de la Methode*, provided a clue when he wrote, "Each problem that I solved became a rule which served afterwards to solve other problems." For our purpose, this translates to: remember how we got here and make sure we keep the momentum going.

We will first consider what it means to be in compliance with 21 CFR Part 11 (how we got here). Then we will examine what should be done to remain in compliance (keep the momentum going).

Compliance with 21 CFR Part 11: *What It Means and How We Got Here*[2]

Compliance with 21 CFR Part 11 means that policies and procedures exist to help ensure the development, deployment, maintenance, and use of validated[3] computerized systems,[4] and the establishment and maintenance of one's accountability for activity regarding electronic records and signatures. Many articles have been written, and many training sessions have been presented, regarding the road to compliance with 21 CFR Part 11. In its simplest form, compliance is attained as illustrated in *Figure 1*, the 21 CFR Part 11 Compliance Model.

Step 1 – Develop Systems Inventory

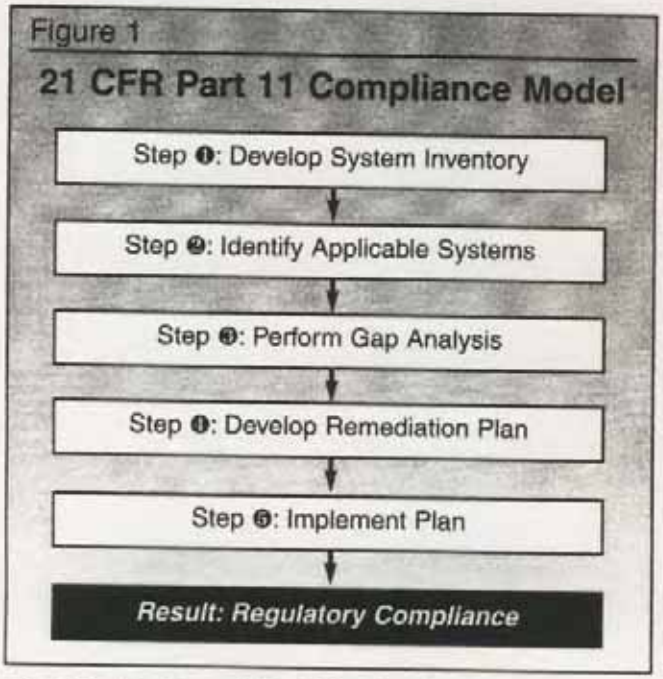
You have developed an inventory of your hardware and software, and a network architecture document appropriate for your circumstances. This is the basis for your compliance; you know what you have and where it's located. If you didn't have this information, you would be hard pressed to describe how you control it.

Step 2 – Identify Applicable Systems

You have identified all the computerized systems in your inventory that fall under the requirement to comply with 21 CFR Part 11. These are the systems that meet the following criteria:

- The process or the applicable data are covered under an existing FDA regulation
- A computerized system is being used to create, modify, maintain, archive, retrieve, or transmit the data

Figure 1



Step 3 – Perform "Gap" Analysis

For each system that must comply with 21 CFR Part 11, you will have identified regulatory deficiencies, or "gaps." The "gap analysis" would have addressed the existence and adequacy of the following items at a minimum:

- 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, technical specifications, and appropriate tests of stress/limits boundary conditions
- Evidence of validation (e.g., validation plan, validation summary, installation/operational/performance qualifications)

At the corporate level, you have also identified gaps by evaluating the existence and adequacy of the following items at a minimum:

- Organization chart and job descriptions to document the appropriateness of the organization structure
- Policies and procedures (i.e., Standard Operating Procedures [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 the Quality Assurance (QA) unit

Step 4 – Develop Remediation Plan

At the conclusion of your gap analysis, you have developed a plan to address the deficiencies (remediation plan). The plan probably had the following general characteristics:

- The systems were stratified in order of risk to the company
- Each issue would have been associated with a specific corrective action (e.g., SOPs to be developed, validation activities to be performed, and vendor audits to be conducted)
- Roles and responsibilities, resource requirements, milestones, and target dates were identified
- The plan was reviewed and approved by appropriate representatives of company management, information technology, and QA

Step 5 – Implement Plan

And, finally, you have implemented, or you will be in the process of implementing, appropriate procedures and controls. These are referred to in 21 CFR Part 11 § 11.10, as stated:

> *"...procedures and controls that are designed to 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."*

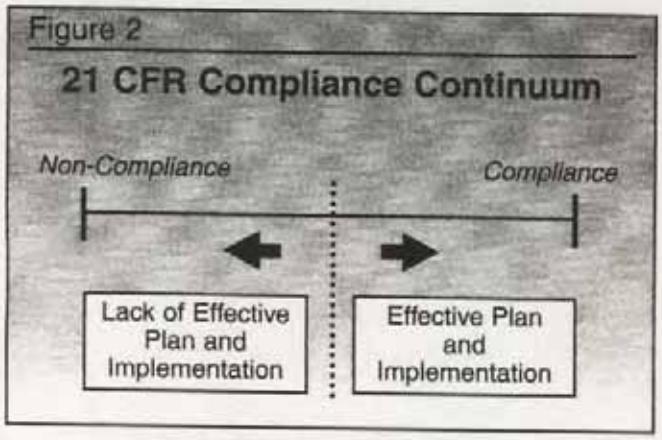
Please refer to the author's article "Complying with Federal Regulations: Controlling the Electronic Transfer of Clinical Trial Data: Practical Advice," in the April 2000 issue of the *Journal of cGMP Compliance*, for a detailed discussion of the requisite procedures and controls.

Result: Regulatory Compliance

To the extent that you have effectively developed and implemented the remediation plan described above, you have minimized the risk of non-

compliance with 21 CFR Part 11 (the "glass is half empty" view), or maximized the likelihood of compliance (the "glass is half full" view). This concept is illustrated in *Figure 2*. While there may be 21 CFR Part 11-related issues that an FDA inspector could uncover (regulatory compliance is never a hundred percent certainty after all), these will tend to be isolated, relatively insignificant, and not reflective of the overall compliance status.

Figure 2



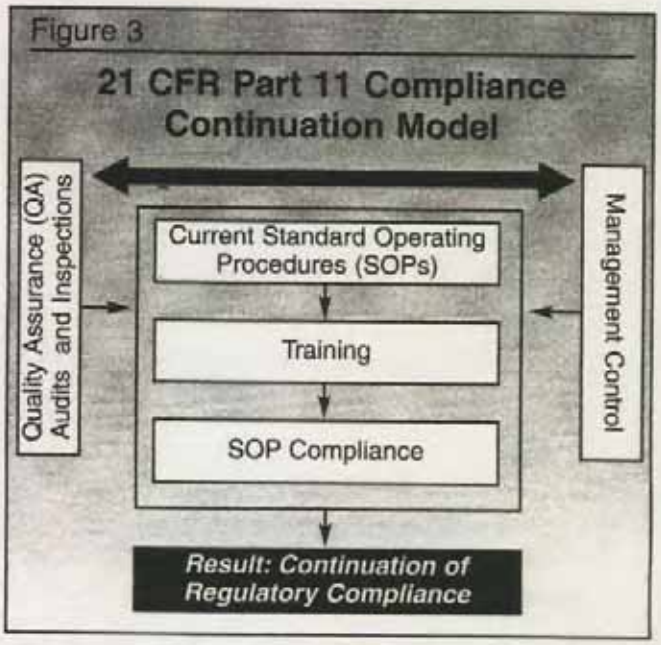
Remaining in Compliance with 21 CFR Part 11: *Keeping The Momentum Going*

Simply stated, remaining in compliance with 21 CFR Part 11 requires that you continue to conduct those activities that got you here in the first place. As I said, this is simply stated. Doing it, however, is a bit more complex. What follows is my recipe for keeping the momentum going and remaining in compliance with the regulation. It is not a "technical" recipe. There are no magical technical solutions here. Rather, it is a "management" recipe. Management must establish controls to help ensure (1) that regulatory processes are followed and (2) that management is informed when they are not. This is illustrated in *Figure 3*, a 21 CFR Part 11 Compliance Model. You will note the following: the activities are of a management nature; There are two additional processes, management control and QA audits and inspections; and these latter elements are linked.

Management Control

Remaining compliant with 21 CFR Part 11 requires many individual activities and the involvement of many individuals and groups. While the requisite procedures and controls will have been established to allow for regulatory compliance in the first place, company management is now responsible for maintaining the momentum. This means that company management must create an environment wherein the individuals and groups continue to perform the appropriate activities in an appropriate manner: "Herding cats" is a layperson's term for this concept. The question then becomes, "what procedures and controls can company management employ to ensure that this is done?"

Figure 3



While the procedures and controls referred to in 21 CFR Part 11 § 11.10 are primarily technical in nature (e.g., validation, computer security, backup and recovery), the requisite management controls are not. Technical activities still must be reflected in SOPs, just as are activities governing study conduct, statistical analysis of data, drug shipment and accountability, etc., all of which are "technical" to one group of individuals or another. So the objectives and techniques of management control remain the same:

- SOPs for regulated processes must be developed, approved, and remain current
- Individuals responsible for conforming to these SOPs must be trained in a timely manner
- Staffing levels must be appropriate, and there must be an adequate degree of supervision
- SOPs must be complied with
- Only qualified individuals must perform or have responsibility for regulated processes
- Individuals must be accountable for adhering to regulations as they relate to their specific

area of responsibility (e.g., department, study, function)
- Deviations from approved policy must be brought to management's attention in a timely manner and resolved in an acceptable way

These controls are preventive in nature; their effective implementation will tend to prevent regulatory non-compliance. They will also tend to require an adequate investment in resources regarding salaries, training, levels of supervision, and management, etc.: "Short cuts" are not advised. Is prevention a hundred percent certainty? Of course not. So we also need to discuss detective controls.

Quality Assurance Audits and Inspections

This section describes the detective controls that a company should consider to remain in compliance with 21 CFR Part 11. These controls relate to audits and inspections by the QA unit.

An effective QA unit is the last line of defense in that it should be able to detect regulatory non-compliance in a timely manner, and allow company management to address potential impacts before they become major risks to the company. The QA unit, separate and independent from the direction and conduct of the day-to-day business processes, represents a management control to help assure that policies and procedures are being performed properly, and that regulatory compliance is being maintained. As stated in 21 CFR Part 58 § 58.35:

> *"A testing facility shall have a quality assurance unit which shall be responsible for monitoring each study to assure management that the facilities, equipment, personnel, methods, practices, records, and controls are in conformance with the regulations..."*

With respect to 21 CFR Part 11, this means that the QA unit staff (either internal staff or contractors) must:

- Understand the requirements of 21 CFR Part 11, and the processes being performed that involve and relate to electronic records and electronic signatures
- Perform the requisite audits of processes and inspections of data to be able to assess regulatory compliance
- Report instances of regulatory non-compliance to company management in a timely manner

Understanding the Requirements and Related Processes

Individuals responsible for auditing for compliance to 21 CFR Part 11 should have the education, training, and experience in the regulation and applicable technology (e.g., development methodologies, programming methodologies, security tools and techniques, backup and recovery tools and techniques) to adequately perform such audits. An auditor can obtain an understanding of the regulation by attending training sessions provided by industry organizations, or contracting with a qualified consultant to do on-site regulatory training, and reading pertinent industry articles. An understanding of the technology is another matter.

An effective auditor vis-á-vis compliance with 21 CFR Part 11 is a person who will have some practical experience with one or more aspects of computerized systems. Book learning is not sufficient. The auditor may have to evaluate any or all of the following issues, to list just the more common ones:

- System development practices (e.g., what methodologies are available and when they are applicable)
- Validation principles and practice
- Computer security and recoverability
- Good and practical programming, testing, and documentation practice
- Change control and configuration management
- Encryption tools and techniques
- Documentation of hardware maintenance
- Digital signatures/biometric signatures, etc.
- Disaster recovery planning

The practical nature of the auditor's experience is important to enable the auditor to understand complexity and context. With respect to complexity, the auditor should be able to perform activities such as, but not limited to:

- evaluating internal system workings to obtain an understanding of security processing
- audit trail updating, etc.
- evaluating testing documentation to confirm that testing is of sufficient nature and scope
- evaluating a backup facility to confirm that it will effectively support use in an emergency situation

With respect to context, the auditor should be able to determine when a particular procedure or control is not proper in the circumstance (e.g.,

when the formulas used in an Excel spreadsheet used to process regulated data are not properly documented, when customizations made to off-the-shelf software are not properly tested), and discuss the impact of deficiencies (i.e., which deficiencies impact data integrity and which do not).

Performing the Requisite Audits and Inspections

The QA unit should include audits of 21 CFR Part 11 activities in the master audit schedule. The form of the audit/inspection (e.g., SOP compliance audit, "in process" inspection, an audit of data/records) is dependent on the given audit objective. The key point to consider is that all of the elements of 21 CFR Part 11 should fall within the audit scope in some respect. By whatever means, the following questions at a minimum should be addressed as part of the overall audit scope of the QA unit:

- Are the organizational chart and job descriptions current?
- Is the system inventory current?
- Are the SOPs that relate to 21 CFR Part 11 current?
- Is the applicable staff trained on the SOPs? Are the training records complete and accurate?
- Has the applicable staff received regulatory training? Are the training records complete and accurate?
- Are all regulated computerized systems validated? Is the validation documentation current (i.e., all changes appropriately considered)?
- Is each computerized system in compliance with 21 CFR Part 11 (appropriateness of audit trails, authorization checks, electronic signature controls, etc.)?
- Are all programs and files protected against unauthorized access (internal and external)?
- Have any unauthorized access been attempted? Have they all been resolved in a satisfactory manner?
- Are computing resources protected against viruses?
- Is a current disaster recovery plan in place? Has it been tested?
- Are all files appropriately backed up? Is the backup data useable?
- Have recoverability procedures been successfully used/tested?
- Are maintenance records (hardware and software) current?
- Have established standards (e.g., programming, testing, documentation) been followed?

It should be noted, however, that the effectiveness of detection is directly related to how soon a problem is detected, so it is important to perform audits and inspections with a frequency that is commensurate with the potential regulatory risks. For example, if SOPs are to be reviewed annually to ensure that they remain current, this process should be audited annually. The reason is that it is relatively easy to let SOPs become out-of-date. This is easily identified in an FDA inspection, and working with out-of-date SOPs can become a serious regulatory issue.

Reporting Regulatory Non-Compliance

As with the results of any audit, issues raised regarding policies and procedures related to 21 CFR Part 11 must be reported to company management in a timely manner. Management needs to know the status of regulatory compliance, specifically:

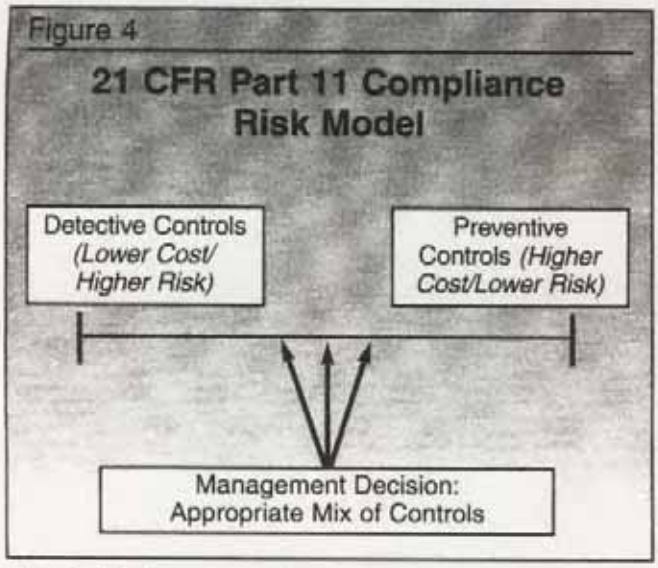
- What the specific issues are
- What remediation steps are planned
- When remediation will be instituted/completed
- If the company is at significant risk for regulatory action, should FDA perform an inspection

This feedback mechanism allows company management to enhance existing controls, strengthen enforcement of existing controls, and/or institute additional controls as warranted. This will also allow company management see trends vis-á-vis compliance to 21 CFR Part 11, such as an increasing frequency of regulatory issues in one area, with one individual or group and/or with selected processes. As new/enhanced controls are implemented, QA will assimilate them into the master audit schedule, audit them as appropriate, and thereby provide continuous feedback to company management.

Summary

Remaining in compliance with 21 CFR Part 11 is a management issue, not a technical issue. Regulatory compliance is always a management issue regardless of which regulation. It is management's responsibility to manage the business. Every process is technical in some respect. The controls can be categorized as preventive or detective. The ben-

Figure 4



efit of effective preventive controls is that they will tend to prevent regulatory non-compliance, but will be more costly than detective controls. The benefit of detective controls is that they will tend to be less costly than preventive controls, but they may not be as effective in helping you remain in compliance with 21 CFR Part 11. This concept is illustrated in *Figure 4*.

Company management must implement a combination of preventive and detective controls. The proper combination boils down to a management issue. ❑

About the Author

Leonard A. 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 B.A. and an M.B.A. from Long Island University. He was a Director of the Electronic Data Processing (EDP) Auditors Association. Len is the author of "Do It Right The First Time: A Handbook for Controlling Technology Through Good Validation Practices," published in the February 2000 issue of the Journal of Validation Technology. *Len can be reached by phone at 732-845-4904, by fax at 732-845-4834, or by e-mail at len_g@metasol.com.*

References

1. FDA. Code of Federal Regulations, Title 21, Food and Drugs, Part 11. "Electronic Records; Electronic Signatures: Final Rule." *Federal Register*, 62 (54). (March 20, 1997). pp. 13429-13466.
2. Grunbaum, L.A., "Complying with Federal Regulations: Controlling the Electronic Transfer of Clinical Trial Data: Practical Advice." *Journal of cGMP Compliance*. Vol. 4, No. 3 (April). 2000. pp. 73-79.
3. FDA. *Guidance for Industry: Computerized Systems Used in Clinical Trials*. (April). 1999. "...confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through the software can be consistently fulfilled." This is included in the "definitions" section of the document.
4. FDA. *Guidance for Industry: Computerized Systems Used in Clinical Trials*. (April). 1999. "...computer hardware, software, and associated documents (e.g., user manual) that create, modify, maintain, archive, retrieve, or transmit in digital form information related to the conduct of a clinical trial." This is included in the "definitions" section of the document.

Article Acronym Listing

CFRs:	Code of Federal Regulations
EDP:	Electronic Data Processing
QA:	Quality Assurance
SOP:	Standard Operating Procedure