Selecting a Computerised System Compliant to 21 CFR 11 Requirements.

R.D. McDowall
McDowall Consulting

As the vast majority of the computerised systems operating in the pharmaceutical industry are not compliant with the technical controls required by 21 CFR 11: Electronic records and electronic signatures final rule1 and the Compliance Policy Guide2. Getting these systems into compliance is a major concern for all organisations under FDA regulation.

There are two main approaches to achieving this aim:

1. Working with the supplier to implement a new version of the system that is compliant with the regulations
2. Evaluating alternative systems that are compliant and the corresponding suppliers

The first approach is the easiest to consider as you'll be working with a system and supplier that you know (and love?). Ideally the supplier will have a large presence in the pharmaceutical industry and will be sensitive to the need to comply with the regulations. There will be a time lag between now and when a compliant version is available but you'll be able to use the system if you have undertaken the system assessments and incorporated procedural controls as required by the Compliance Policy Guide2.

However, there will be instances where this first approach will not be applicable, such as:

- The supplier of the existing has gone out of business
- A supplier has no intention of implementing technical controls as the sales of the product within the pharmaceutical sector are too low
- You are unhappy with the supplier
- Want to look at alternative approaches
- Replacement of a legacy system

This paper is concerned with the discussion of system replacement and the need to comply with the requirements of 21 CFR 11. I'll be presenting generic principles to broaden the applicability of the approach. I'll be looking first if you should take redesign the process or simply replace the system, then we'll look at some of the requirements that need to be specified in more detail to meet the requirements of the Final Rule and some tips about system selection.

Replace System or Redesign Process?

The first thing to do when confronted with a decision to replace a system is to look for a system with similar functions; replace like with like.

I strongly suggest that you need to stand back and think first as you have an opportunity. The opportunity is about looking at what the system does and where its is sited and the systems it interacts with.

This opportunity gives you the ability to consider some options:

- What is the process and can it be improved?
- How effective and efficient is the current system in automating the process?
- What are the strengths and weaknesses of the current system?
- Can you work better electronically with a new system?
- What are the current support costs versus a replacement system?

There may be some computerised systems, such as process equipment, that you may think will not need the approach that I'm describing. However, by stepping back you may consider that a move to SCADA (Supervisory Control and Data Acquisition system) or DCS (Distributed Control System) may bring about a better overall control of your manufacturing process than just looking at a single piece of equipment. However, such an approach can only be justified by an effective cost benefits analysis.

For systems, other than the process equipment described above, in pharmaceutical research and development or manufacturing, look at the workflow that is being automated by the

system. Map it and review the steps in the process. Many legacy systems may be linked to others using manual data transfer that has to be checked for transcription errors every time. Alternatively, additional steps are not required because of organisational changes or changing work practices outside of the system.

Regardless of the reason for purchasing a new system, do not rush into purchasing one that simply replaces what you have already. Look at this as an opportunity for looking at alternatives that you would not normally have time to consider: the same objective can be achieved in a number of ways and still be compliant with the regulations.

Step Jump in Validation Requirements for Systems

The requirements of 21 CFR 11 and its enforcement means, in my view, that systems will require a step jump in overall validation. Let me explain what I mean. Over the past 18 years since the first CPG on computer validation[3] was published computer validation regulations and guidelines have gradually increased their stringency. Therefore, what was state of the art a few years ago will be average now and out of date soon due to a process that I will term regulatory creep.

With the need to comply with increased 21 CFR 11 requirements in areas such as security, access control, audit trails, electronic records integrity and electronic signatures we will experience a step jump in the overall validation requirements for systems. This will mean these functions must be adequately specified, evaluated and tested. However, this does not necessarily mean that costs for validation will rise appreciably. As many of the new requirements will be common across all systems, once an organisation has put the time and effort into defining 21 CFR 11 requirements once they can be applied to other systems. However to avoid the incorporation of boilerplate text into specifications, the requirements should be reviewed regularly in light of internal experience and external information from FDA warning letters and 483 observations.

System Documentation

In all of this, remember that the system documentation also comes under the remit of 21 CFR 11. Requirement 11.10(k) looks for controls of system documentation: pagination, distribution lists, authorisation, change control etc. Furthermore, §11.10(k)(2) states:

Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

So as the replacement system is designed, built, tested and qualified the documentation must be produced at the same time. Not as is the case with many systems developed in the past where the documentation has been delivered either late or not at all.

Requirements Specification

You'll have to define the system requirements, as this is a generic discussion, I'll ignore the system detail and just focus on the need to specify the requirements to meet 21 CFR 11. In this discussion, I'll be assuming that we are defining a closed system. Owing to space limitations we'll discuss just security and access controls as a way of illustrating the requirements for the regulations.

Requirements Traceability

In developing your system requirements, the current best practice is to number them, so that they can be traced through later specification and testing documentation. This approach has two main benefits, one business and one regulatory. The business benefit is that the system will be better specified and will have a greater chance of meeting user requirements; a major feat these days. The other will be the meeting of regulatory requirements. With an increased validation approach under 21 CFR 11, an organisation will be able to show how they have correctly specified their requirements to meet the various sections of the regulations and how they have tested them or not to demonstrate compliance with the final rule.

Security and Access Controls

The main requirements for security and access controls for systems under 21 CFR 11 are found in the following sections of the Final Rule:

- Limiting system access to authorised individuals (§11.10c)
- Authority checks to ensure that only authorised individuals can use the system etc.(§11.10g)

How can these be interpreted into system requirements that we can use practically? The answer can be clarified in the only guidance document issued by the FDA since publication of 21 CFR 11, Computerised Systems in Clinical Trials3. Here the requirements for security and access controls are expanded further into two sections on physical and logical security, which are listed verbatim below.

Physical Security

1. In addition to internal safeguards built into the system, external safeguards should be in place to ensure that access to the computerized system and to the data is restricted to authorized personnel.
2. Staff should be thoroughly aware of system security measures and the importance of limiting access to authorized personnel.
3. SOPs should be in place for handling and storing the system to prevent unauthorized access.

Logical Security

1. Access to the data at the clinical site should be restricted and monitored through the system's software with its required log-on, security procedures, and audit trail. The data should not be altered, browsed, queried, or reported via external software applications that do not enter through the protective system software.
2. There should be a cumulative record that indicates, for any point in time, the names of authorized personnel, their titles, and a description of their access privileges. The record should be in the study documentation accessible at the site.
3. If a sponsor supplies computerized systems exclusively for clinical trials, the systems should remain dedicated to the purpose for which they were intended and validated.
4. If a computerized system being used for the clinical study is part of a system normally used for other purposes, efforts should be made to ensure that the study software is logically and physically isolated as necessary to preclude unintended interaction with non-study software. If any of the software programs are changed the system should be evaluated to determine the effect of the changes on logical security.
5. Controls should be in place to prevent, detect, and mitigate effects of computer viruses on study data and software.

This gives us more insight into FDA thinking on interpretation of the two main sections above. Do not close your mind to the fact that this discusses clinical trials computerised systems if you work under GLP or GMP and not GCP. Use this document to interpret these requirements for your own organisation, systems and regulatory situation.

We are now in a better position to look at the requirements for your replacement system under the security and access control section. Specifically, for each major function within the system you'll need to define who has access to it and the level of the access (read only, create, modify, delete etc) for more information see McDowall[4]

One advantage of working with many commercial software applications is that there is usually an access control facility where the user types can be defined together with their access privileges to each of the functions of the application.

Evaluating and Selecting a System

The system requirements document will be used as a basis for defining evaluation tests to assess prospective systems. To conserve resources, these evaluation tests can be used as the basis of the qualification tests before the system is released for operational use, thus reducing the overall validation effort. We'll look first at security and access control evaluation and then move onto some other areas for evaluation that are crucial for 21 CFR 11 compliance.

Where many system evaluations before 21 CFR 11 became effective, would only concentrate on application functionality, there is an increased emphasis on other data integrity and security features that now must also be evaluated.

Security and Access Control

In the system requirements document you will have defined the number of user levels, such as user, supervisor and system administrator. Each user type will have a matrix of the access privileges for the major functions required by the system. Either tests can be constructed for execution or a demonstration of the required functionality can be requested during the system evaluation. In either case, a record of the ability of the system to meet these requirements is necessary to demonstrate that the system was able to fulfil these functions. In addition, you may want to see if a user can be upgraded or downgraded from one user level to another easily, as this may affect the operational use of the system.

Other Areas to Evaluate before Selection

In addition to security and access control, there are other areas where evaluation must be considered before system selection. Some of these areas are:

- Electronic Records: §11.10b requires accurate and complete copies of electronic records. Therefore, based on previous experience of some laboratory systems it is important to show that what appears on the screen is accurately reflected on a paper printout.

- Ability to discern invalid or altered records is highlighted

Table 1: Continuum of User Privileges (from McDowall Reference 4)

Access Privilege	Access Rights
Zero-Level	No access rights or access denied
Execute Only	User can execute functions accessed but nothing else
Read Only	User can only read the data accessed but cannot write or append anything
Write Only	User can overwrite data
Read-Write	User can read or write as required
Append Only	User cannot change any data but can add additional information
Administrator	Full access rights to create, read, write, copy and delete data

specifically as a validation requirement in §11.10b. Therefore before purchase of a new system, how the records are stored and how their integrity is maintained needs to be evaluated. Some records can have a cyclic redundancy check (CRC) to do this: what happens if you can open the file in a text editor?

- Audit Trail: The audit trail is a key foundation of 21 CFR 11 as outlined in §11.10e. However here's where the predicate rule comes in as there is a difference between GMP on one hand and GCP and GLP on the other. The difference is that GLP and GCP both require an entry for the reason for changing the record. In other respects (who made the change, date and time of the change and the original record not deleted) the requirements are the same across all three areas.

There are other issues to consider from a practical perspective, as the audit trail has to capture the creation of a record, there will be numerous routine entries. Can you sort through these to find the one that is relevant to your specific query? As the audit trail must be archived with the electronic records to which it is linked, can the audit trail be retrieved and begin operation again at a later stage - possibly after several version changes of the application?

Summary

Replacing a computerised system for one that is compliant with 21 CFR 11 is an opportunity to take time to reflect if the current way of working is optimal and ideal. Can improvements be made in effectiveness of the overall process? Process redesign should be considered. Then the system must be specified, there are several requirements that are mandatory under 21 CFR 11 such as security and access control, audit trail and electronic records integrity and these should be included in the system requirements document. Evaluation of any prospective system needs to include these items as well as the actual functionality of the application. ■

References

1. 21 CFR Part 11, Electronic Records; Electronic Signatures; Final Rule. Federal Register Vol. 62, No. 54, 13430-13466, March 20, 1997.
2. Compliance Policy Guide 7153.17 for enforcement of 21 CFR 11: Electronic Records and Electronic Signatures, Federal Register 64 (1999) 41442-41443.
3. FDA Guidance for Industry, Computerized Systems used in Clinical Trials, CDER, 1999
4. R.D.McDowall, Computer (In)security, Scientific Data Management 3 (6) 8-13, 1999

Bob McDowall is a consultant specializing, amongst others, with computerized system validation and electronic records and electronic signatures. Dr. McDowall has published many articles on these, and other subjects. He received his undergraduate degree in Bio Chemistry from Newcastle University and received his PhD in Toxicology from London Hospital Medical College