



FDA 21 CFR PART 11

Toby Davis

TESSELLA SUPPORT SERVICES PLC

Issue V1.R1.M0

November 2002



INTRODUCTION

Organisations want cost savings, improvements to process control, and the opportunity to integrate data from across the enterprise. These improvements in flexibility and productivity can be delivered by using electronic records instead of paper-based systems – knowledge can be shared and searched more easily, and the existing investment which has gone into generating this knowledge can provide more effective returns.

Where paper documents with physical signatures have traditionally been used to assert the validity of data and processes, electronic equivalents pose particular problems. Without careful design, planning and safeguards, electronic records are more open to tampering, falsification, and repudiation. These concerns have prevented the large-scale take-up of electronic records, leaving organisations unable to take advantage of the benefits this could have offered. To address this problem the U.S. Food and Drug Administration (FDA) issued Rule 21CFR Part 11, giving the regulatory framework required for submission of electronic records in lieu of traditional paper submissions. This describes the conditions that an electronic records system must satisfy in order for electronic records to be admissible in submissions to the FDA.

Issued in 1997, the framework was postponed while organisations dealt with Year 2000 compliance issues. In the meantime, electronic records technology has matured to a point where the move to electronic systems is become a required step in order to keep pace with competitors' process improvements. This year the FDA has issued further draft guidelines on compliance with the regulations, prompting more interest in their use, and reaffirming the position technology has occupied in providing established solutions to many of the issues involved in 21 CFR Part 11.

This technical supplement provides a background to the issues raised by 21 CFR Part 11, and describes the core requirements which need to be considered when adopting or developing an electronic records system to ensure that it meets the FDA's requirements. It discusses the elements of the system, and the safeguards that must be put in place.

ELECTRONIC DATA

In a typical laboratory environment today, data comes from a variety of electronic

sources (automated data acquisitions, LIMS, etc.). Frequently, these are printed out and pasted into a lab book as a paper record. Additional data coming from other sources is handwritten alongside. This provides a permanent record of all the information connected with the work which will satisfy regulatory authorities, but is slow, duplicative and cannot be easily shared. The data needs to be stored in a productive way which allows it to be used as much as possible, by all the people who could benefit from access to it.

Effective use of this data demands that the laboratory store information in a place where everyone can access it at the same time, while still allowing the addition of new data. The paper lab book may still be a useful tool, but the raw data, at the very least, should be kept on-line in electronic formats. A LIMS (or several LIMS across different labs and different specialisations within the organisation) will help manage the low-level data. Electronic Lab Notebooks (ELN) help gather all data into an efficient, searchable resource, including higher levels of data such as the scientist's comments and description of their work. A consistent strategy across the enterprise will be needed to gain the best advantage from the work carried out in the labs.

Whatever approach is taken to the gathering, the management of the raw data needs to be carefully governed. Without confidence in the integrity and reliability of the basic information, the next, more productive, step of knowledge management will not have a solid foundation.

Raw results come under the same level of regulation as a signed record in a lab book. The FDA applies this principle to electronic formats as well as to paper records of the data. If the data is open to error or manipulation before it is stored, there cannot be confidence in the end record. If an individual signs the record as being accurate, it is still their responsibility to ensure that the data is accurate, but processes should be in place to make it difficult to enter incorrect data in error.

LIMS will manage the low-level data from laboratory systems, and will likely allow collation and searching. To include the level of data usually held on paper in a laboratory, however, a broader management system is required which includes more than machine data – the additional comments and work diary of a scientist. This might be implemented as an enhanced LIMS or as a separate piece of software sitting above the LIMS layer. Including the knowledge associated

with a piece of data allows an organisation to use the full potential of the information – whether it is the fact that a particular compound under test is a derivative of a particular family, or a comment that altering buffers might yield clearer results than in this test.

ELECTRONIC RECORDS

The move from managing raw data to managing an organisation's knowledge is core to making an electronic records system provide the sort of return on investment which is expected. Similar principles apply for the management of the raw data as for the types of document or record that will be required in a submission to the FDA, but the difficulties are much clearer and more immediate for the higher levels of document. We will discuss the issues in relation to these documents, bearing in mind that the regulations will also apply to the raw data.

A record is, at its most simple, a snapshot of a specific set of data formatted in some manner. The means of presentation is important because it can vastly alter the way the data is interpreted. As a trivial (and unlikely) example, if the system presents a page to the user with headings "Sample A" and "Sample B" displayed above graphs of the data for two samples, it makes a lot of difference whether the graph marked "Sample A" is actually for Sample A or for Sample B. If the presentation means is later changed (for example, correcting the bug so that the right graph is under the right heading) a user will now see something different, based on the same data. Presentation cannot be divorced from content in the definition of a record, because we need to be sure that we know what information was available at a given time. There is little point keeping records if, when challenged by an auditor, we cannot say for sure that the record shown now is still showing the same meaning (from the same data) as what we signed a month ago. Equally there is a limit to how useful it is to present data without context – a page showing a list of numbers only is devoid of meaning (aside from the user knowing which options they selected to get to this list).

We need, then, an electronic record that does not change: it is permanently linked to a specific set of data, and a specific presentation means. Audit trails in underlying databases provide basic assurance that the information has not been changed. Once we have this it becomes meaningful to attach metadata to it, and to move on to managing the organisation's knowledge instead of just its data.

There may however be a real requirement for records to be modified over time. Corrections to text or data are the most obvious case, while annotations during review might be a common process. Changes, as for paper systems, will need to be made in such a way that the original data is not destroyed. In a paper lab book, a user might ‘strike through’ text rather than obliterating it, so that although they have corrected the detail, their original entry remains available. In the same way, when the data is stored electronically, it must be possible to retrieve a copy of the data as it was prior to the change. We will refer to the different versions as different electronic documents, forming part of the same record¹. By maintaining a history of the different documents we can see the record changing over time, and at any stage see how it was displayed to users at a given time.

In particular, review of a document presents interesting problems to a records system. We shall see later how issues of identity become clearly important; establishing means of signing documents in a secure, non-repudiatable way and of ensuring documents cannot change after being signed will be paramount.

ELECTRONIC SIGNATURES

To maintain confidence in the electronic system, the FDA mandates the use of electronic signatures that are bound permanently to records in the same way a handwritten signature is permanently linked to a paper record. The signatory is asserting, by signing a record, that it is true and accurate, and the system asserts by displaying the signature at a later date that what is being shown is the same record (in the same context) as seen by the signatory when their signature was applied. We need to have confidence in both (and to be able to demonstrate to the FDA that our confidence is warranted).

How this is implemented is the responsibility of the records system. Typically the system might create a digest (an electronic signature based on a mathematical operation on the record’s content and the user’s signature) of the record using the user’s signature, and attach that to the record. When viewed at a later date, the displayed content of the record should still match the stored digest – if it does not, the record is not the same as when stored and cannot be used as a valid record. As the digest is based on the content of this individual record, it protects against falsification in a number of ways. The signature cannot be copied to another document as it would not match the content of the second document. With the user’s signature forming part of the process, another user’s signature

cannot be substituted instead, as that would also fail to match the digest.²

A signature is of little use if it is easy to falsify, or if more than one person could apply the same signature. To be valid in lieu of paper records, an electronic signature must carry the same weight as a handwritten signature. To ensure that a similar (or better) level of confidence exists in the validity and authenticity of electronic signatures, the FDA defines a high standard for the constitution of electronic signatures. These standards apply the same basic principles apply that we expect from handwritten signatures:

- The contents of the signed document should not be able to change after signing (and still remain a validly signed document).
- It must be clear what the signature means in context.
- Signatures must belong to individual persons, not re-used.
- Signatures must be difficult to forge.

It should be possible to demonstrate that these are satisfied by the system. The first has been discussed in our example above; the others are discussed below.

- The context of the signature (e.g. approval, review) should be made clear at the time of signing in terms of a description on the presented record (the equivalent of an “Approved by:” dotted line at the bottom of a paper document). The signatory must know what they are doing by applying a signature to a document (so that they cannot later deny their intent), and a reader should be in no doubt what was meant.
- Each individual should have a distinct signature, which is not re-used between individuals. (The term ‘individual’ is used carefully to ensure that it is clear that the single person, not the position they hold, is who is associated with the signature.) Signing a document on behalf of someone else (if this is allowed by the organisation’s processes) would be conducted in the same way as on paper – the actual signatory would apply their own signature, but comment that it is on behalf of the other individual. They would not be able to use the other individual’s signature, in the same way as they would not be able to write another’s signature on a paper record.
- The difficulty of forgery is specified, in part, to prevent repudiation. At no point should a signatory be able to deny that the signature is theirs, or claim incorrectly that the document was different when they signed it . Paper forgeries are susceptible to discovery by well-established means

(the depth of impressions, the order of strokes, etc.) but electronic signatures, once forged, are much more difficult to disprove. To avoid this the FDA prefers that they are made as difficult to forge as possible in the first instance.

Spelling out the definition of a reliable signature is necessary to ensure that all the related aspects are considered by all parties, and addressed. By breaking down the value of a handwritten signature into its component parts, we can ensure that all have equivalents in the electronic system.

ACCESS CONTROL

To safeguard against impersonation, the FDA stipulates minimum requirements for identification. If biometric information is not used (identifying a user on the basis of physical characteristics such as fingerprints or retinal scans), users should have passwords that meet certain security criteria.

- The system should enforce minimum complexity requirements on passwords (to prevent easy guessing)³.
- Passwords should age, so that if they are compromised they cannot be misused for long.

There are additional guidelines on the type of administrative systems that should be put into place to minimise the chances of impersonation.

A consequence in 21 CFR Part 11 of this requirement to know unequivocally the identity of the current user is that users need to prove their identity each time they execute an action (creating a record, approving a document, etc.), instead of assuming that the current user is the same person who successfully authenticated earlier. This may constitute the single largest change in working practices for lab staff, in particular in environments when machines are shared. Simply logging on to a computer in the morning and remaining logged on throughout the day does not provide sufficient assurance about identity. Part 11 requires that staff re-assert their identity when executing actions.

The access controls the FDA requires may seem more strict than when using paper lab books, but it does equate to a similar level of security – staff do not lock up their lab books, but we can assume that it is difficult to forge handwriting and to replace a genuine page with a forged one. This is easier on electronic

systems, so additional constraints must be implemented in place of those we take for granted with paper.

These guidelines in general form good practice that most organisations would wish to apply to help secure their proprietary data in any case. If access to read electronic records is restricted on the basis of authentication as a specific authorised user, commercial and corporate data are made that much more secure. The support mechanisms required for successful implementation of an electronic system are likely to already be in place, and the investment which has gone into them can provide a ready foundation for the new system.

RECORDS RETENTION

The required lifetime of a record will depend on what type of document it is, what development it relates to, and so on. Existing FDA regulations will specify retention periods for specific documents, with the same retention period applicable to electronic records as for the traditional paper equivalent. (Remember that 21 CFR Part 11 specifies regulations for using electronic records in the same way as paper records, so all requirements for paper will apply to the electronic versions.) If a record is to last from initial development of a product to the expiry of patent, the retention period may well exceed thirty years. During all of this time the record will need to remain readable and be presented in the same format – paper records may fade with time but they still present the same information in the same format to the reader (assuming that colour-coding does not become indistinct with age). Processing that was possible on the original at the time of creation should still be possible on the archived record, so storing the electronic equivalent of a photocopy of the original records (for example, rendering it to a static graphical image) is not ideal if the original could be searched or sorted in more sophisticated ways.

This is a common concern in data archiving: where data is produced by a specific application on a specific platform for specific hardware, one of the links in the chain may be obsolete in thirty years' time. Should a company maintain a museum of obsolete hardware in order that they can download a copy of the original data file to a lab machine and open it with the original obsolete software? Should they invest in emulator software to mimic an obsolete lab machine long after the original no longer functions? Should they migrate records periodically to newer systems?

The FDA's draft guidelines issued in 2002 provide scenarios of how long-term record retention could work, focussing on museums and migration. Each has its problems (acknowledged by the FDA), though these are areas undergoing active research and have proven solutions. (See Tessella's technical supplement on Electronic Archiving for a detailed discussion of the issues involved.)

These issues will also apply to the validation of electronic signatures, but the primary concern for development and design will be the retention and preservation of the records themselves – an area which may require more planning than the retention of the signing data due to the wider variety of document types and technologies.

CASE STUDY

How not to do it

A fictitious company, Acme Pharmaceuticals, has a new database that prevents direct user access to data, confining them to controlled access through forms together with restrictions on who can modify each category of data. It contains audit trail data giving names and times for who has read each database row and who has written to each. Users' passwords are complex enough that they feel confident no lab worker will crack another worker's account even by dedicated effort. Deletion of records requires users to have certain restricted levels of authority, available only to lab managers and above.

When Acme provides the FDA with their submission for their new drug, they are unable to demonstrate that the systems in place satisfied the requirements for electronic submission of data. However good the drug may or may not be, the FDA cannot have confidence in the authenticity and validity of the submitted data because Acme's systems had significant flaws making their electronic records less reliable than paper ones.

Where have they made mistakes in their implementation? There may be additional problems implicit in this description of their system, but we will concentrate on four key areas:

- ❑ Firstly, the audit trails alone do not provide sufficient guarantees. Knowing simply who has changed a record does not tell us what it was changed from or to. Knowing that someone has retrieved data from a table also does not tell us what specific fields they retrieved, or how that data was presented to them – not a specific requirement in itself, but it becomes relevant when we come to signing content (see below). There is also a worry about how easy the audit trails themselves are to modify, delete or even invent, though the FDA could request further details to clarify this.
- ❑ Secondly, even a good system may be used in a bad way. How do the staff at Acme use computers? Does the first person to arrive each day switch the computer on, log on, and leave it for the rest of the day as a shared resource? Having complex passwords is little use if it is easy to use someone else's identity without needing a password in the first place. 21 CFR Part 11 does address this problem by insisting that users re-authenticate at each action they carry out, but it is not clear that Acme have implemented this. (In practice this might be the subject of a request for further evidence.) Again there will be scope for concern over access to the underlying administrative data – are these complex passwords held in plain, readable format in the database, or are they hidden from even the administrators?
- ❑ Thirdly, and perhaps most worryingly, is that deletion of records can occur at all in this system. The audit trails will record the fact that data has been deleted, but does not tell us what has been deleted. It should be possible to archive records at the end of their lifetime, or to withdraw from circulation a document that has been found to contain errors, but it should remain retrievable and should have an associated reason and authorisation for its withdrawal. Complete destruction of records is as serious for electronic documents as for signed paper documents.
- ❑ Lastly, there is no explicit signing of content mentioned in the description. Simply being able to show from an audit trail that a lab manager has read a record does not constitute her signing it – and her apparent decision to not delete it would not constitute a meaningful approval action either, even if deletions were allowed by the FDA. A related issue, hinted at earlier, is that even with signing, we have seen no evidence that the presentation means is stable. There is no history of what forms were in use at the time they viewed the data – would the same data viewed today by the FDA be given the same order and the same descriptive text, and use the same calculations as when the lab manager saw it originally?

Lessons to be learned

If Acme had maintained paper records for their submission, they would not have treated them in the same way. Staff would not share the same lab book, and signatures would be required on the lab book instead of just an archivist's record of who had read it and who had used a pen on it. Removal of pages or obliteration of parts of pages would not have been permitted at all.

The basic lesson Acme is learning is that the electronic system replaces specific paper systems *to do the same as them* and more. The added benefits of the electronic system are conditional on getting the basics right – applying the same levels of rigour, and the same compliance with the applicable good practices, as they are used to for paper operation. There will be some benefits to be found in making day-to-day data entry and operation quicker and simpler than a paper system, but this is not the core area where an organisation would expect to see return on investment. That will come from the added benefits of sharing knowledge effectively, which will rest on the same rigorous foundation and approach as need to be applied to make a paper system work successfully.

To some extent the problems we have seen are a product of the artificially scant description of Acme's systems and processes. In practice they should expect to have to provide the FDA with detailed descriptions of their systems and the nature of the safeguards employed. It may be necessary to present evidence of an independent validation of the system's compliance with 21 CFR Part 11, or for FDA representatives to carry out such a validation. The scope of the exercise will need to go far beyond the single-paragraph summary given here, and Acme should expect that and ensure that their system is documented and tested in sufficient detail to support this part of their submission. The delays in waiting for additional information requests from the FDA, and providing the required documentation (if it exists) are likely to be costly in terms of getting a product to market.

PART OF THE PROCESS

Making a laboratory or production environment work effectively, and to demonstrable quality levels, requires more than simply a [new] piece of software. To get to the stage where an organisation is considering implementing an electronic records system, they are likely to have already put significant effort into their supporting processes, which have been in place since their original

paper structure. These processes must be working effectively and answer the real needs of the staff (and the organisation as a whole). This existing investment in process can be taken forward with the introduction of electronic systems, forming a good foundation for taking advantage of the new system's benefits.

The match between the electronic system and the organisation's processes is two-way. It is likely that changes will be required to the supporting processes, to ensure both that the new system is used properly, and to receive the highest return on the investment. It should also be the case that the electronic system be tailored to how the organisation works. A new records structure may make parts of the existing process obsolete – there is no point running at 'half-speed' just to maintain compatibility with existing practices – but the best return will be achieved by designing a system that works the way the organisation wants to be working.

This should not automatically mean that off-the-shelf solutions are a poor choice. Depending on the individual product there will be different elements of customisation available that will enable the product to be adapted to best suit its new environment. The crucial point is to not tie an organisation that has worked successfully in the past to a different way of working just because a piece of software demands it. The requirements for the new software (whether custom-built or off-the-shelf) should be specified to make a real contribution to the organisation, bearing all the costs in mind. The improvements in corporate ability to share and exploit existing knowledge may need to be offset against the costs of both the retraining time and the potential inconvenience to the way the company works. Making the organisation less productive because staff have to move to a less suitable mode of practice defeats the purpose of changing the system.

Software compliance with 21 CFR Part 11 is achievable. Another factor, though, is to use a system in a manner and environment that supports 21 CFR Part 11 and other applicable standards in the required way. The controls on user administration, for example, are a crucial part of the overall security of the records management structure. However carefully the software has been designed, if users tape their passwords to the side of their screen the security is worthless. The software alone cannot mitigate against this and processes must be in place to support its use.

It is worth repeating that Rule 21 CFR Part 11 does not replace existing

regulations applicable to making submissions to the FDA. If an organisation is planning to comply with FDA regulations and make a submission, part or all of the required records can be supplied in electronic format if you *also* comply with this ruling. Rule 21 CFR Part 11 is a supplement to the existing regulations and guidelines.

WHERE TO GO FROM HERE

As discussed, the benefits of an electronic records system are only likely to fulfil expectations if it forms part of the wider organisational culture and process. It is important to consider the benefits expected within the existing operational structure, and to look for an opportunity to improve that structure by answering specific needs. The investment in working processes has been built up over considerable time and should form a key part of the way forward.

In looking to replace some or all of the paper process with electronic systems, an organisation should look for compatibility with the processes that they replace, with the surrounding support structures and processes, and with their existing technology investment (LIMS etc.). Making people work differently to use the new system, or making others work differently because of knock-on effects of the system, will not deliver the improvements expected unless the changes are themselves a planned benefit.

Planning the introduction or development of software requires careful specification in order to ensure the completed system gives the benefits required in that environment. Software can implement 21 CFR Part 11 specifications but still not provide either an effective business gain or a complete organisational compliance with 21 CFR Part 11 (or other FDA rules). The principles in 21 CFR Part 11 embody best practice, but require as much planning and consideration as any process involved in regulatory submission.

Tessella have gained significant experience working with large organisations to implement software solutions compliant with a variety of regulations, including FDA Rule 21 CFR Part 11 and 510(k) certification for medical systems. Tessella has been ISO 9001 and TickIT accredited since 1993, with a firm commitment to developing software and processes to a high-quality standard.

We would be pleased to discuss any requirements you may have for 21 CFR Part

11 compliance for new or existing software, either as a laboratory equipment provider or as an organisation wishing to make electronic submissions to the FDA.

OTHER READING

Tessella, Technical Supplement “Electronic Lab Notebooks”

Tessella, Technical Supplement “Archiving Electronic Records”

Tessella, Technical Supplement “Laboratory Information Management Systems (LIMS)”

U.S. Food and Drug Authority, “Electronic Records; Electronic Signatures; Final Rule” – Food and Drug Administration, 21 CFR Part 11

http://www.fda.gov/ora/compliance_ref/part11/

<http://www.21cfrpart11.com/>

FOOTNOTES

¹ The FDA considers the terms “electronic record” and “electronic document” to be generally synonymous; we will distinguish the terms here to illustrate the issues involved in change histories and review cycles, but the issues remain the same.

² An alternative technology is to add a handwritten signature using a stylus and an input pad, appending the image of the signature to the end of a document. Although this is similar to signing a paper document, it is likely to be easier to falsify than a digital signature based on a public/private key architecture, as discussed later.

When using a handwritten signature in this way, it would still be advisable to create a digest of the signed document, as an additional safeguard against future tampering.

³ This is not a requirement under 21 CFR Part 11, but with regard to non-biometric identification in the context of 21 CFR Part 11, the FDA caution against the use of “easy” passwords. Providing minimum complexity requirements is the simplest way of ensuring that this advice is incorporated to the system.

Tessella Support Services plc
Creating Software for Science and Engineering

Tessella's services range from feasibility studies, through system design, development, implementation and ongoing support. Our expertise includes:

Data Analysis Software
Data Capture
Simulation Software
Advanced Graphics
Systems Support
Database Applications

Other Technical Supplements available include:

- | | |
|---|--|
| <input type="checkbox"/> Archiving of Electronic Info | <input type="checkbox"/> Object Oriented Programming |
| <input type="checkbox"/> Active Server Pages | <input type="checkbox"/> Pocket PC |
| <input type="checkbox"/> Automated GUI Testing | <input type="checkbox"/> Portable GUI Development |
| <input type="checkbox"/> Bayesian Statistics | <input type="checkbox"/> Printer Technology Guide |
| <input type="checkbox"/> Beowulf Clusters | <input type="checkbox"/> Real Time Systems |
| <input type="checkbox"/> C++ | <input type="checkbox"/> Regression Testing |
| <input type="checkbox"/> Client-Server Technology | <input type="checkbox"/> Security and the Internet |
| <input type="checkbox"/> COM | <input type="checkbox"/> Simulation |
| <input type="checkbox"/> Computational Fluid Dynamics | <input type="checkbox"/> Soft Computing |
| <input type="checkbox"/> Computer Image Processing | <input type="checkbox"/> Software Design Methodologies |
| <input type="checkbox"/> Decision Support Systems | <input type="checkbox"/> Software Development Cycle |
| <input type="checkbox"/> Electronic Data Capture | <input type="checkbox"/> Software Documentation |
| <input type="checkbox"/> Electronic Lab Notebooks | <input type="checkbox"/> Software Portability |
| <input type="checkbox"/> Excel | <input type="checkbox"/> Software Re-engineering |
| <input type="checkbox"/> Extending the Life of Software | <input type="checkbox"/> Software Specification |
| <input type="checkbox"/> Federal Drug Administration | <input type="checkbox"/> SQL |
| <input type="checkbox"/> FORTRAN 90 | <input type="checkbox"/> UNIX Inter-Process Comms |
| <input type="checkbox"/> Grid Computing | <input type="checkbox"/> UNIX Systems Performance |
| <input type="checkbox"/> High Throughput Screening | <input type="checkbox"/> UNIX Workstations |
| <input type="checkbox"/> Instrumentation | <input type="checkbox"/> Visual Basic 6 |
| <input type="checkbox"/> Integrated Lab Systems | <input type="checkbox"/> WAP |
| <input type="checkbox"/> J2EE | <input type="checkbox"/> Web Services |
| <input type="checkbox"/> Java | <input type="checkbox"/> Windows 2000 Services |
| <input type="checkbox"/> Lims | <input type="checkbox"/> XML |
| <input type="checkbox"/> Linux | <input type="checkbox"/> X Windows |
| <input type="checkbox"/> Microsoft Net | |



INVESTOR IN PEOPLE

Tessella Support Services plc

3 Vineyard Chambers, Abingdon, Oxon, OX14 3PX, England

Tel: (+44) (0) 1235 555511 Fax: (+44) (0) 1235 553301

E-mail: info@tessella.com Web Address: <http://www.tessella.com>