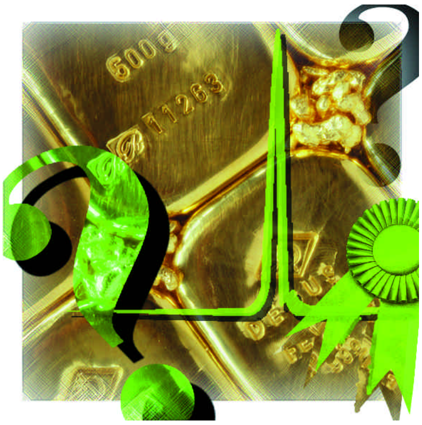

Just e-Sign on the Bottom Line?

R.D. McDowall, McDowall Consulting, Bromley, Kent, UK.

What is the impact of the Electronic Records and Electronic Signatures Rule on pharmaceutical and other chromatography laboratories?

Welcome to the third Millennium! I am assuming in writing this column that you have survived any occurrences of acute alcoholic poisoning during the festive period and any problems associated with the Year 2000 problem. So, what happens now on the quality front? What I want to discuss is the sequel to the Year 2000 problem: the Electronic Records and Electronic Signatures Rule for the pharmaceutical industry (1).

That Sinking Feeling...

What's all this about I hear you say? Let's look at an analogy to give you an idea. If you remember the story of the Titanic, imagine the Year 2000 problem is the ship. We have a story of set sail, cross ocean, hit iceberg, sink or swim and that's about it. You can have a few little variations such as a little love interest or the band continuing to play as the ship goes down or rearranging the deck chairs, but in the end, the ship goes down. Predictable outcome really — just like Year 2000.

I proudly introduce to you the sequel to the Titanic: The Iceberg. This sequel:

- is bigger than Year 2000
- 90% of the problem is hidden from view
- can go anywhere as interpretation evolves
- and how long it lasts before it melts cannot be predicted.

The iceberg is the Electronic Records and Electronic Signatures Rule from the Food and Drug Administration (FDA) for pharmaceutical laboratories amongst others (1).

We'll look at the following in this column:

- What is this rule?
- What is the impact on chromatography laboratories within the pharmaceutical industry or those supporting it?
- What will be the impact on other chromatography laboratories operating outside of this arena?

E-Sig: The Essentials

This rule has had a long history of development, originally being a pharmaceutical industry initiative in 1990 when the Pharmaceutical Manufacturing Association asked the US FDA to use electronic signatures rather than handwritten ones. The aim here was to take advantage of new technology and avoid the need for paper. A dialogue followed with a discussion paper being issued for comment in 1994 (2).

In March 1997, the final rule was published in the Federal Register and was effective from 20 August 1997. It affects both legacy (existing) systems and new ones and covers not only electronic signatures but also electronic records. The legislation is substantive (i.e., someone can end up in jail if things go badly wrong or your company can go out of business; but you won't let things get out of hand will you?).

The major issue from the FDA perspective is that electronic records and electronic signatures must be

- trustworthy
- reliable
- subject to FDA inspection.

Much of the driving force for the legislation is to prevent fraud. This is the major difference between a European and an FDA regulatory inspection (innocent until proven guilty versus guilty until proven innocent, respectively).

Note that the contents outlined in the preamble and the final rule itself represent MINIMUM requirements for implementation. Similar to all regulations and guidelines for computerized systems operating in the pharmaceutical industry over the past 10 years, the requirements only go in one direction: more stringent interpretation.

Definitions

Table 1 provides definitions for terms used in this column. What does this mean in practice?

Open and Closed Systems

First, let's deal with open and closed systems. Note here that we are talking about "systems" not "applications." Do not limit your vision to just the application. You must consider all aspects of the system: application, operating system, network, hardware and all associated services.

The main difference between an open and closed system is access. If you have a chromatography data system (CDS) that is run within your department, it is a closed system. It is still a closed system if the Information Technology (IT) department runs the server and maintains the network, and it remains a closed system if you outsource the IT support to a third-party provider, provided that no other company's work interferes with yours. When you start working across the Internet then the CDS becomes an open system and more controls are required. For the purposes of this column I have assumed that the CDS or any other application is a closed system and we will not consider open systems any further.

You'll need to consider the definition of system very carefully as this includes the IT department's support services and network maintenance. One impact of the final rule is that the work of the IT department comes within it; much to the surprise of many IT departments. This means that the inspection of such departments will be realized in a very short time.

Electronic Records

From the definition given in Table 1, your CDS has been generating electronic records; however many laboratories still define their raw data as paper. If you are working in the pharmaceutical industry or for a contract research organization (CRO) that works on its behalf, this is no longer the situation. Chromatography data systems produce electronic records and you must follow these regulations.

Remember that you'll need to consider more than just the raw data files, so don't forget to include the method files, run sequence files and integration parameters used for the data analysis. Not mentioned so far, but a critical component of the regulations, is the need for a comprehensive audit trail; this is also an electronic record that is subject to the same controls.

An electronic record must consist of two components: a human-readable section and a machine-(computer) readable section. The content of the human-readable section will include information about the creation and any further processing of the data. There must be controls to ensure the integrity of any data held within any electronic record, such as cyclic redundancy checks.

Controls for Closed Systems

Several controls are needed for the closed computerized systems operating in the chromatography laboratory. These are

- validation
- training
- security
- checks
- archiving
- written policies
- copying
- documentation controls.

Just looking at this list shows that there must be a comprehensive approach to implementing electronic records and signatures. We'll discuss the areas in more detail now.

Validation of systems: Validation of the systems must be undertaken to ensure that they are accurate, reliable, operate consistently and have the ability to determine either invalid or altered records. Approaches to the initial and ongoing validation were covered in the recent articles on chromatography data systems, and I'll not repeat the overview information that is contained in these articles (3, 4).

Table 1: Definitions of Terms.

Biometrics means a method 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.

Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

Electronic record means any combination of text, graphics, data, audio, pictorial or other information representation in digital form that is created, modified, maintained, archived, retrieved or distributed by a computer system.

Electronic signature means 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.

Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

Open system means 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.

However, the extent of these regulations means that the level of testing must be increased to meet the requirements of the final rule. For example, the audit trail should be tested to demonstrate compliance with the system and how electronic signatures are used within the system.

Training of all staff involved with the system: First, there must be a policy for users making them accountable for their use of electronic signatures in any computerized system used by them. This must be accompanied by training, and knowledge of their understanding may be required or demonstrated during an inspection.

Second, the identity of all users must be verified by organizations before they start using electronic signatures.

Many organizations routinely undertake this step either during recruitment or during the induction when a new member takes up a position. However, if not done already, it needs to be completed before an individual uses their electronic signature.

Finally, all involved with the system need to be qualified with a mixture of education, training and experience. This is no different to normal requirements for any quality system inside or outside the pharmaceutical industry. However, remember that FDA talks in terms of systems and this extends to the IT department if they support the server or the CDS in any way.

System security: To ensure the system generates accurate and trustworthy data there must be mechanisms in place to restrict access to authorized individuals. Solutions to this will usually be based on the access control mechanism of the CDS software package. You'll tailor access to an individual's abilities and job tasks; for instance, there'll only be two or three people with system administration rights, whilst not all analysts will have supervisory functions to change methods or approve data. A formal approach to this security issue is required so that all access rights are documented.

Audit trail: A key requirement to ensuring the trustworthiness of electronic records and signatures is an effective audit trail. This must be a computer generated, not a paper record, and is an internal part of the CDS or whatever application you are using. If you have used a laboratory information management system (LIMS), you will be aware that all of the commercial systems for use in the pharmaceutical industry have an audit trail in which changes are logged behind the scenes and appear only where the user must enter the reason for a change. The same will now apply to all computerized systems used under 21 CFR 11.

However, there are specific requirements for the audit trail: it must be independent of the operator and cover the lifetime of any electronic record from creation, through modification to deletion. When an audited change is made, the audit trail must record

- who made the change
- when the change was made: local time in hours and minutes, and the date
- the original data without overwriting them
- the new entry
- the reason for the change.

The audit trail must be retained with, and as long as, the original electronic records and must be capable of review or copying by FDA inspectors. Thus, to meet this requirement, the system or you must be able to organize both the data and the associated audit trail information into separate directories or projects and be able to archive both at the same time.

It all seems reasonably straightforward, doesn't it? However, let's think this through in a little more detail. Assume you have 10 chromatographs attached to your CDS; what are the sorts of problems and issues that could arise with an audit trail? Let's assume that each chromatograph is used on average four days per week to inject 50 samples in duplicate. Not a large number of injections you'll agree. So assuming 10 instruments, four days use per week, 100 injections per run, we have 4000 injections per week. Therefore, each time you inject a sample you'll be creating an electronic record and there'll be a corresponding entry in the audit trail. This will be performed automatically, but you'll have 4000 records per week and assuming 50 weeks per year, you'll have 200 000 data file creation entries in the audit trail per year alone. If you have a larger system then you'll have proportionally more data entries in the audit trail.

Then of course, you'll be interpreting the data won't you? Automatically applying the method to the data files will generate more information in the audit trail and usually you, and possibly your supervisor, will fiddle with baseline placement for those chromatograms you want to interpret and not repeat — further entries in the audit trail.

Just to add the final straw, there are also the audit trail entries for modifying the method and run sequence files. Remember at least one audit trail entry for each time you create, modify or delete anything to the record. Naturally, all your work will be of the same type so you don't need to worry about separating different audit trail entries, do you?

So before you start, think about how you want to organize your data. If you are purchasing a new system, consider the functionality of the audit trail. Can it be separated to monitor specific directories or projects, so when you archive the data files, methods etc., the specific project audit trail is archived at the same time?

Let's consider the audit trail a little further. Does the system have the ability to query the audit trail and find out exceptions from the detail of normal actions so that quality assurance can monitor the data in the same way that an FDA inspector may do? There's little point in having entries in the audit trail unless you can search and highlight areas around specific work packages.

Checks: Several checks are required for compliance with the electronic signature and electronic record regulations. These include:

- Sequence checks to enforce, where necessary, the correct sequence of events in the system. For example, you should not be able to produce a report until you have acquired, interpreted and calculated the results. Therefore, operations, where appropriate, must be completed in the correct sequence and must not impact the quality of the information produced by the laboratory.
- Authority checks to ensure that individuals are authorized to perform their allotted tasks within the system (e.g., setting up a method, acquiring data or approving results with their electronic signatures). It is especially critical to ensure that users signing records cannot repudiate a signed record as not genuine.
- Device (meaning either input or output device) checks to determine the validity of data input or outputs. This can come in a variety of forms: some of the data entries for the CDS can be downloaded from a spreadsheet or LIMS, acquired through the analogue-to-digital unit or input manually. Approaches to meeting this requirement may vary from validation, calibration and use of verified data entry where appropriate.

However, remember that any computer system must have trained staff to operate it. Despite all the checks in the world, the users can and do get it wrong. Effective training will only mitigate the severity and the frequency of mistakes.

Archival of records: Unless you have an inexhaustible supply of disk space, you'll need to archive your electronic records off the system at some time. The procedure must be effective and you'll need to know where a specific data file is located. The data will need to be retained for the length of time required, which may be over 20 years. There are issues here concerning the data format and whether you will be able to read the data or the media on which the data are recorded etc. This was addressed recently in the last part of the CDS series (5).

Of course, once archived, you'll need to be able to retrieve the data. The regulation calls for "accurate and ready retrieval." So, the data when retrieved must be able to be reanalysed with the same results. To do this you may need to have the original software or the software will need to ensure that historical data can be imported and reprocessed to obtain the same results. Ready retrieval is relatively self-explanatory but you'll need to know where it is archived, and the procedure for getting it back must be tested and known to work. Data archive software for chromatographic data is emerging and will become increasingly important for this part of 21 CFR 11.

Copying of records: There is the requirement to make copies of the electronic records that are both "accurate and complete" and are suitable for review inspection and copying by both the internal quality assurance staff as well as the inspectorate. These records must have both human- and machine-readable elements so that the review is helped. We'll look at electronic records in more detail in a later column.

Documentation controls: This is a little jewel, hidden at the bottom of the section on closed-system controls, that comes with a sting in the tail like a scorpion [§11.10(k)]. The first part is straightforward [§11.10(k)(1)]: document controls are required on the access and distribution of documentation for the system, which is a normal requirement for controlled documentation.

Here comes the sting in the tail [§11.10(k)(2)]: "revision and change controls to maintain an audit trail that documents time sequenced development and modification of systems documentation." Cast your mind back to the life cycle of a CDS (6). This process starts for a new system with the requirements and then moves to selection. Of those involved in CDS projects recently, how many of you produced documentation in the correct sequence of events?

This requirement must be understood carefully. The documentation to support validation must be produced in the correct sequence. The validation plan needs to be written near the start of the project, not as an afterthought just before you go live, as validation covers the whole of the life cycle. Do not write the testing protocols first, followed by the user requirements specification and then the validation plan, as one organization did, which resulted in a warning letter (7).

When the system becomes operational, the problems of this section do not go away. One of the key areas of regulatory concern is change control: the documentation here also needs to follow the regulation. So, the change needs to be proposed, evaluated, approved, implemented, tested and validated in the correct time sequence, and the documentation accompanying each stage must also reflect the same time sequence. Remember the audit trail concept applies to the system documentation as well as the system itself.

Electronic Signatures

Instead of handwritten signatures, 21 CFR 11 (1), an electronic signature allows an authorized user to approve actions, results and reports. There are a number of issues here but we will look at an overview. The signatures can be either electronic signatures for closed systems or digital signatures for open systems. Is there a difference? Yes, let's look further.

- Electronic signatures as a minimum consist of a combination of a unique user identification plus a password. Their genuine owners only must use these electronic signatures, and any attempt at falsification must require collaboration by at least two individuals. Therefore, there are issues here about the ways that user IDs and passwords are administered. As unique user IDs are usually defined at a site or corporate level, then a user password must not be handed out by a system administrator but determined by the user themselves to be compliant with the regulation. In addition to passwords, an identity taken or security card can also be used either in combination with a password or in place of it. However, tokens or devices used either on their own or in combination with other means must also be tested when first used and periodically.
  Of course, practices such as shared passwords and multiple log-ons must not be used. There must also be a procedure for periodically checking that these still work, and there must also be procedures for their recall or revision in case they are compromised, with temporary replacements issued.
- Digital signatures usually involve biometrics to identify a user. Biometrics is the discipline that uses biological features of an individual to identify that person. Biometrics can be defined as a measurable, physical characteristic or personal behavioural trait used to recognize the identity or verify the claimed identity of an individual. Currently biometrics can use, amongst others, fingerprints, face or voice recognition.

It is vitally important that all users are instructed that use of their electronic signature is legally the same as a traditional handwritten signature. Part of that training as well as the implementation of any system is that users cannot repudiate or deny that they signed or approved any electronic signature; also, controls should be in place to prevent impersonation of others.

Linking Electronic Signatures with Electronic Records

We've discussed both electronic records and electronic signatures separately; we'll now look at how they must be linked together.

Signing sessions: When a user first starts to sign electronic records using their electronic signature, they must use both components initially. If the signing session is continuous then the user only needs to enter one component at later points. If the signing session is broken for any reason, then both components must be entered again. Regardless of the continuity of the signing, the identity and role of the user signing the records must be displayed on the screen (e.g., creating a method, calculation of results, authorization of results etc.).

Electronic records: When electronic records are signed, the name of the signer, time and date of signing and the meaning of the signature must be transferred to the electronic record. This information must be included in both the human- and computer-readable sections of the electronic records and this information then comes under the requirements for the electronic records described above. It is important that when electronic records and electronic signatures are linked the signature portion can't be deleted or removed. The electronic signature section must be able to be copied with the appropriate electronic record.

The final rule requires signature and record linking to be sufficiently robust to prevent falsification by "ordinary" means. Essentially, FDA recognizes that there are sophisticated means to hack files but by using applications such as Notepad and appropriate system design, together with training and management supervision, this should not be an issue.

Impact of the Final Rule

Looking into my crystal ball, here's my view of some of the potential impacts of this regulation.

Impact on non-pharmaceutical laboratories: As the pharmaceutical industry constitutes a large proportion of sales, there will be changes in the systems that you use in the laboratory, even if you don't work in the pharmaceutical industry. Some of the requirements to meet this rule should be designed in such a way that they can be turned on or off when first installed, so that if you are not working in the pharmaceutical industry you'll not be affected by the additional functions unless you want them.

End of stand-alone laboratory PCs? Where do the regulations for electronic records and electronic signatures position stand-alone PC systems?

In short, their days are numbered. This is not because of any inherent inability to do a task such as a CDS or instrument controller. It is driven by the resources required to back up the electronic records and maintain them over the course of their lifetimes as well as mitigating the impact of their loss because of a disk failure.

Not convinced of this argument? Imagine you have two PCs that run stand-alone CDS software. You'll have to back up each system, usually daily, to minimize data loss and ensure data security. Each PC's configuration will usually be a single disk and this is the main point of failure in the system.

Multiply this by the number of stand-alone PCs you have in your laboratory and you'll get the feeling of the administrative burden this will become. Therefore, you'll see PC applications being designed with network links as a minimum and integrated with the network over time. The obvious home for your chromatography data and any associated files is the network drives run by your IT department or department IT expert. These network drives should be fault tolerant so that a single disk failure will not impact data security or integrity. However, this can move you from the regulatory frying pan into the regulatory fire, as we'll now see.

Information technology in the trenches: Many organizations running multi-user data systems will use the central IT department to run the server and the network that the application runs on as well as to back up and recover the data stored. You lucky people! Does your IT department run to Good Manufacturing Practice (GMP) or Good Laboratory Practice (GLP): probably not. You should be investigating whether your IT department has the procedures to support this role of supporting your data and the system. Are the records kept, are procedures available and are they followed? For example, what are the procedures for monitoring security breaches? We'll look closer at the role of the IT department in a later column.

Major problems can occur with change control where changes can be made without the laboratory's involvement, which throw the system's compliance out. More problematic are organizations that have developed Standard or Common Office Environments (SOE and COE, respectively) that are driven from a desire to cut the cost of ownership of IT systems. Changes in these environments can be made from a central IT group with no appreciation of their impact on the validation status of many applications. Great care is needed in this area.

Hybrid systems: What are hybrid systems, I hear you say? We've talked so far about systems that are only electronic and have no paper output. A hybrid system has both paper and electronic output. The problem with hybrid systems is that you have to match the paper sign-off of the printout with respect to the electronic records. A hybrid system should be avoided as there may be issues of collating the paper and electronic records together.

However, nearly all computerized systems, to some extent, come with the option to print out data and screens. Unfortunately there are 3000 years of human behaviour with cellulose-based products that the FDA regulators are trying to cope with. Remember, when in doubt print it out and look at it. I do this myself.

Legacy systems: The majority, if not all, of current systems operating within chromatography laboratories in the pharmaceutical industry do not comply with the regulations. Therefore, as we'll see below in the enforcement notice, FDA will be looking to see what progress you've made in making the system compliant. Do not stick your head in the sand and rely on your current definition of CDS raw data as paper.

Recent FDA Moves

Coming to a laboratory near you: Paul Motise, the key FDA person involved with the 21 CFR 11 final rule, moved recently last year to the Office of Enforcement signalling an increased effort on behalf of the agency to enforce the regulation. In addition, there are reports that 50–100 inspectors have been trained to evaluate systems in the industry. Therefore, we can look forward to an increased level of surveillance in this area. Happy days are here again…

Compliance policy guide: To complement your unrestrained joy, the FDA published a compliance policy guide in July 1999 for enforcing 21 CFR 11 (8). This will be done on a case-by-case basis and is dependent on a number of issues outlined below:

Nature and Extent of Part 11 Deviations

- Are the deviations numerous?
- Do the deviations make it difficult for the agency to audit or interpret data?
- Can you make copies for the agency to review?
- Are file formats easy to copy and read?
- Is data integrity compromised?
- Are employees accountable for actions made under their electronic signatures?

Effect on Product Quality and Data Integrity

- Absence of an audit trail when there are data discrepancies.
- Individuals deny responsibility for record entries.
- Lack of operational system checks are significant if operators have the ability to deviate from the sequence of events and this results in adulterated or misbranded product.

Adequacy and Timeliness of Planned Corrective Measures

- Do you have a reasonable schedule for modifying systems to make them compliant?
- Is there demonstrable evidence of progress against the plan?
- Do you have procedural controls in place? (FDA recognizes that technical controls will take longer.)

Compliance History — Especially Regarding Data Integrity

- In short, have you been good boys and girls? Part 11 deviations are more significant if the firm has a record of inadequate or unreliable record keeping.

Until companies become fully compliant with these regulations, FDA inspectors are being briefed to be more vigilant to detect inconsistent, unauthorized modifications, poor attributability and any other problems associated with failure to comply with the requirements of 21 CFR 11.

Linweld warning letter: FDA has already issued at least one warning letter concerning 21 CFR 11. This was to Linweld, a US distributor of medical gases (7), and the letter cites violations of both the GMP regulations (21 CFR 211) and electronic records; electronic signatures rule (21 CFR 11) as follows:

- No testing of the system after installation at the operating site.
- No worst case testing.
- Lacks testing provisions to show correct functioning of the software.
- Time sequence of system documentation: testing August 1993, validation plan September 1993 and user requirements March 1994.
- The system does not generate an audit trail and there is no way to determine whether values have been changed on batch records apart from the last value entered by an operator.
- Does not record out of specification value.
- No documentation or testing of the system's ability to discern invalid or altered records. This is significant because electronic records by their nature may be easily altered in a manner that is difficult or impossible to detect.
- No documentation to show whether the system has the ability to generate accurate and complete copies of records in electronic form. It is vital for FDA to be able to audit electronic production records, among other things, reviewing electronic copies of your electronic records.
- No safeguards to prevent unauthorized use of electronic signatures that are based on identification codes/passwords when an employee who has logged on to a terminal leaves the terminal without logging off. This is serious because another employee could impersonate or falsify electronic records.

There you have it, apart from these comments it was a very efficient computer system.

Summary

We've looked at some of the issues surrounding the electronic records and electronic signatures regulations (21 CFR 11) and how they affect chromatographers working in the pharmaceutical industry. Currently no systems in our laboratories fully comply with these regulations. The regulations impacting both electronic records and electronic signatures are discussed together with the impacts of these regulations. The latest news from FDA and the impact of one of the first warning letters on systems is discussed.

References

(1) Electronic Records, Electronic Signatures Final Rule, Federal Register, (available on www.fda.gov).
(2) Notice of Proposed Regulation, Federal Register (1994).
(3) R.D. McDowall, LC•GC Europe, 12(9), 568–576 (1999).
(4) R.D. McDowall, LC•GC Europe, 12(12), 774–781 (1999).
(5) R.D. McDowall, LC•GC Europe, 13(1), 30–35 (2000).
(6) R.D. McDowall, LC•GC Int., 12(4), 226–235 (1999).
(7) Linweld Warning Letter, FDA August 1999.
(8) Enforcement Policy 21 CFR Part 11: Electronic records; electronic signatures (Compliance Policy Guide 7153.17) Federal Register 64 (1999) 41442–41443.

Bob McDowall is Visiting Research Fellow in the department of Chemistry at the University of Surrey, and Principal of McDowall Consulting, Bromley, Kent, UK. He is also a member of the Editorial Advisory Board of LC•GC Europe.