Can You Meet the Technical Requirements of Annex 11?

Jul 1, 2012

By: R.D. McDowall

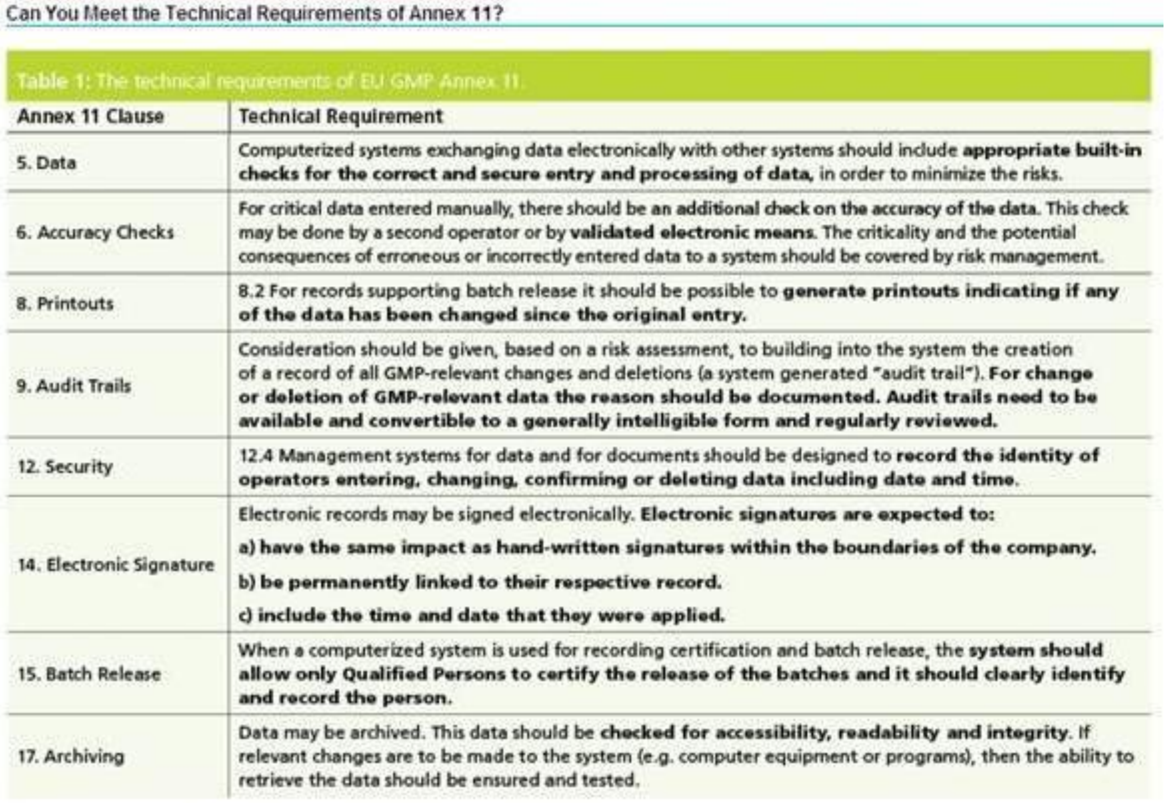
LCGC Europe
Volume 25, Issue 7, pp. 384-388

In January 2011 the updated version of EU GMP Annex 11 on computerized systems was published that became effective on 30 June 2011 (1). In April 2011 this column (2) reviewed Annex 11 and also Chapter 4 on documentation to see if this was Europe's answer to 21 CFR 11 on electronic records and electronic signatures (3). In this "Questions of Quality" column I want to review the technical requirements of the new version of Annex 11 to see how the software commonly used in regulated laboratories meets these requirements and where they don't. To begin, I had better explain what I mean by a technical requirement of software.

A technical requirement is where compliance with a regulation is met through a feature or function in the software that has been designed, engineered and tested by the vendor of the product. In doing this, a vendor should seek the opinion of customers who although they work to the same regulation will tend to have different individual interpretations of how the software should comply with the regulations. The role of the vendor would be to sift through these interpretations, which will occasionally differ, to specify the software so that there is a generic approach to compliance. Where companies have different views then a vendor may use software configuration to enable individual laboratories to implement their own interpretation of a regulation. Here some features can be turned on and others off, allowing different laboratories to implement their own interpretations of a regulation but at the same time allowing a vendor to sell a standard product. So in this column we are looking at how software should meet the technical requirements contained in the new version of Annex 11.

What Are Annex 11 Technical Requirements?

The obvious starting point is to sift through the principle and 17 clauses of Annex 11 and identify what are the technical requirements so that we can then discuss each one individually. Table 1 presents my interpretation of Annex 11 to identify the technical requirements. In this table the technical requirement of each clause is highlighted in bold. As I just mentioned, this is my interpretation of the technical controls, there are clauses of Annex 11 that at first glance may appear to be technical controls (for example, clause 7 on backup) but are mainly procedural in my view.



Can You Meet the Technical Requirements of Annex 11?

Table 1: The technical requirements of EU GMP Annex 11.

Annex 11 Clause	Technical Requirement
5. Data	Computerized systems exchanging data electronically with other systems should include **appropriate built-in checks for the correct and secure entry and processing of data,** in order to minimize the risks.
6. Accuracy Checks	For critical data entered manually, there should be an **additional check on the accuracy of the data.** This check may be done by a second operator or by **validated electronic means.** The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.
8. Printouts	8.2 For records supporting batch release it should be possible to **generate printouts indicating if any of the data has been changed since the original entry.**
9. Audit Trails	Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). **For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.**
12. Security	12.4 Management systems for data and for documents should be designed to **record the identity of operators entering, changing, confirming or deleting data including date and time.**
14. Electronic Signature	Electronic records may be signed electronically. **Electronic signatures are expected to:** **a) have the same impact as hand-written signatures within the boundaries of the company.** **b) be permanently linked to their respective record.** **c) include the time and date that they were applied.**
15. Batch Release	When a computerized system is used for recording certification and batch release, the **system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person.**
17. Archiving	Data may be archived. This data should be **checked for accessibility, readability and integrity.** If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.

Table 1: The technical requirements of EU GMP Annex 11.

Of the requirements in Table 1, I am not going to discuss clause 15 release of a batch by a Qualified Person (QP) as this typically occurs outside of the laboratory and not many analytical scientists are QPs. Also, the requirement for archiving is subject for discussion in one or two "Questions of Quality" columns and therefore we will not discuss this any further. Therefore, this leaves the following sections to consider:

- Clause 5. Data
- Clause 6. Accuracy Checks
- Clause 8. Printouts
- Clause 9. Audit Trails
- Clause 12. Security (however, due to some similarities with clause 9, I will discuss these technical requirements under the section on audit trail)
- Clause 14. Electronic Signature

Looking through the list you will see that many of the topics are concerned with data integrity which is complementary to the discussion in my last "Questions of Quality" column *Fat Finger, Falsification or Fraud?* (4), so we will consider the discussions about data integrity we looked at there as well as what we shall cover in this column. We will therefore start in a boringly logical order with the lowest numbered clause and proceed in increasing numerical order.

Automated Data Transfer Checks between Systems

Looking on the bright side, if all the computerized systems in your laboratory are standalone, then you don't have to consider this section as you are condemned to life imprisonment with eternal transcription error checking instead of hard labour. Actually, considering what I have just written, there is probably not much difference between the two apart from the former being physical and the latter mental hard labour.

However, if you have seen the light and are linking your computerized systems together, e.g. a Chromatography Data System (CDS) with a Laboratory Information Management System (LIMS) then you will want to make sure that what was sent from the CDS was the same as received in the LIMS and vice-versa. This is not a regulatory requirement, it is simply good analytical science. However, as we can see in Table 1, Annex 11 pokes its nose in by requiring *"appropriate built-in checks for the correct and secure entry and processing of data"*. Therefore, there needs to be software functions to ensure that there is no corruption or truncation of data between the sending and receiving computerized systems. Ideally, there would be an interface option available from one or other of the software vendors, typically the LIMS vendor. This should be a standard software module that transfers the data between the two systems or it could be configurable application to accommodate the requirements for any CDS. However, it should not be a one-off module of code written specifically for your situation as this will be more difficult to support over time.

Don't forget that the interface between the two systems needs to be specified in a user requirements specification and tested in your validation of one or both systems.

Accuracy Checks for Critical Data

Annex 11 requires that if critical data are manually entered into a computerized system, then a second check needs to be made. This check can either be manual or automated. The key driver of this regulation is GIGO: garbage in, garbage out. Put rubbish data in to a computerized system you will get rubbish results out at the other end. It is therefore good common sense to put checks into the system to ensure that the data are correct before you go any further – in a worst case scenario it is cheaper to do this than have a product recall of nonconforming product.

First you need to define what critical data are. Consider some of the following situations:

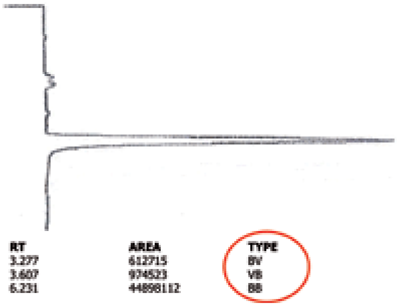
- Is the weight of an analytical reference material used to prepare a stock solution that is entered manually into a LIMS considered critical data?
- Are sample weights or factors entered manually into the sequence file of a CDS considered critical data?

The answer to this and other questions would be "yes" in my view. However, you need to define and document what are critical data for all systems in your laboratory as part of the specifications for the system to comply with Annex 11. Therefore you have choices to make: Do I check everything manually or attempt to automate the process? In my last "Questions of Quality" column (4) I discussed some of the ways of ensuring that manually entered data could be verified against predefined criteria, such as data format checks to ensure the correct number of numbers either side of the decimal point and also within the range of data anticipated. However, these verification checks cannot eliminate transcription errors just reduce them. So unless you are using automated data acquisition and data transfer, I don't think that you can eliminate manual checks of manually entered data, you'll just reduce the incidents of gross error with data field verification, but the second person check, although reduced, will still be needed. This is more reason to automate data transfer between systems rather than rely on the four eyes principle.

More Paper Printouts?

Annex 11 has the requirement that printouts can be printed on request, even for fully electronic systems, but as we can see from clause 8.2 there is the requirement for printouts involving batch release that it should be possible to *"generate printouts indicating if any of the data has been changed since the original entry"*. So, if we are analysing samples for batch release including stability samples then this section applies to laboratory systems.

For this technical requirement, let us consider a CDS. The printout from the CDS has to identify if data have changed since the original acquisition, interpretation or data entry. At the integration level we are very well served with a CDS as this has been built into commercial integrators and data systems since the mid-1970s. When peaks are automatically integrated, the integration is identified with capital letters e.g. BB for baseline to baseline resolution as shown in Figure 1, however, if you manually reposition where the baseline is drawn on the training edge the integration becomes, say, Bb where the training baseline has been repositioned manually. This is available from all CDS now and can be printed on demand.



RT	AREA	TYPE
3.277	612715	BV
3.607	974523	VB
6.231	44898112	BB

Figure 1: Chromatogram illustrating that integration is automatic.

But this is as far as it goes in most systems.

Printouts for changes to everything in a batch analysis you may have to hunt for, depending on the CDS you have, because you will need to identify changes to the sequence file entries, instrument method and processing method. It is not always straightforward or easy to obtain a single printout about the changes made during the analysis of a set of samples analysed for batch release. So what are you going to do about it? Perhaps you might want to check out how you can meet this requirement before an inspector calls.

To help, the European Medicines Agency has published a question and answer section on the web (5) and here question 10 provides some help:

Question: What alternative controls are accepted in case a system is not capable to generate printouts indicating if any of the data has been changed since the original entry?

Answer: As long as this functionality is not supported by the supplier, it may be acceptable to describe in a procedure that additionally a printout of the related audit trail report must be generated and linked manually to the record supporting batch release.

So from the inspector's perspective you can hunt to find this information. However, from your perspective should you not be asking your CDS and LIMS vendors to provide this functionality as standard?

Most Audit Trails Don't Comply with Annex 11

I was thinking of titling this section "what the regulator gives with one hand they take away with the other" but it was a bit too long to fit on the page. Here's what I mean: section 9 on audit trail allows a company to determine if they need to have an audit trail or not (giving with one hand) based on a risk assessment. **But**, clause 12.4 states that if your system holds data or documents it *"should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time"* (taking away with the other hand). Although you do not need to have an audit trail to fulfil the requirements of 12.4, if the system holds data then there needs to be a mechanism to identify users who enter, change or delete data. For the majority of systems we use in the laboratory, an audit trail is really the only sensible solution to meet requirements in clauses 9 and 12.4 of Annex 11, especially if you want the benefits of working electronically.

In addition, if time and date are changed there needs to be a record of this and is an added justification for ensuring that all laboratory computerized systems are linked to the network and time stamps are independently maintained by the IT department. Time and date are critical elements for ensuring data integrity in computerized systems used in the laboratory, therefore there needs to be a means of ensuring their accuracy and also preventing unauthorized people from playing about with the computer clock. The simplest way is to link systems to the network and do this automatically. Summer and winter time changes can also be automated in this way.

Let us now focus on clause 9 for audit trails. I reiterate that if working electronically an audit trail is mandatory in my view to ensure data integrity and to identify who has done what to the data. Although clause 9 does not mention creation or entry of data, clause 12.4 does and therefore the audit trail has to encompass data creation as well as changes and deletion of already entered data. Personally, I would restrict the ability to delete data to one or two individuals or nobody so that the deletion aspect of this clause can be dealt with quickly.

What is new, although perfectly logical, is the requirement to add a reason for change when data are changed or deleted. This brings GMP into line with Good Laboratory Practice (GLP) that does require a reason for change when altering data. Your CDS should be capable of having, at a minimum, a free text entry to allow a user to enter a reason for the change when such a change has been made. A better design for an audit trail would be to have context sensitive user predefined entries that a chromatographer can select when making a change – a faster and easier way of entering data and avoiding all those mistyped and misspelled entries.

The final sentence of this clause has two requirements for us to consider:

- *Audit trails need to be available and convertible to a generally intelligible form and:* The audit trail is present in the system (obviously) but it needs to be readable and understandable. This may not be the case with some CDS audit trails as some can be piles of unintelligible rubbish. Therefore, when you are considering a new CDS for a regulated laboratory, this is one area that you must pay close attention to. Therefore ask the following questions: is there a single audit trail for the whole system or are entries split into smaller units? How are the entries made: can you see who made the change, when it was made, the old and new values and reason for change? Can you search the audit trail easily with user selected criteria to obtain a summary of audit trail entries associated with a specific analysis run?
- *regularly reviewed.* This is the major weakness with virtually all CDS on the market in that **if** you can read the entries and **if** you can search the entries effectively you **cannot** demonstrate electronically that you have reviewed the entries.

Now here's the issue "regularly reviewed". This brings the EU into line with what the FDA have been requiring laboratories to review audit trails: those who have not been complying have featured in a number of warning letters and 483 observations. The simple reason is that there is no point having an audit trail if it is not reviewed. However, what is meant by "regular"? This depends on the use of the CDS. If it is used for batch release, then regular means prior to signing off the batch results from the CDS.

Ask yourself a question. Do you really want to trawl through masses of audit trail data to find out about data changes or are you lazy? Join the club.

What is required is a review of the audit trail by exception: so the system needs to inform you if there have been any changes to the data since initial entry or acquisition for that analytical run thus allowing you to focus your attention where it is needed. If there are no changes – job done! Or is it? How are you going to demonstrate that you have reviewed the audit trail even if there are no changes to data? Hmmm, my CDS does not do this. Therefore, who are you going to call? Let me give you a clue, it is not Ghostbusters but your CDS vendor to ask them how they will implement features to enable you to comply with the law.

We shall return to the audit trail while we review Annex 11 electronic signatures in the next section as there is a further impact on some CDS products used in the laboratory and how electronic signatures can be implemented in many applications.

Electronically Signing Electronic Records the Annex 11 Way

Detailed interpretation of sub clause 14a can derive the same electronic signature requirements as required under 21 CFR 11 except for the horrible administrative over head of writing a formal letter to the FDA and requiring people to verify during an inspection that their electronic signature is the equivalent to their handwritten one. There is also no need to classify a computerized system as either open or closed, nor the need to specify the types of electronic signature that can be used (electronic, biometric or digital). Annex 11 does all of this in 40 words compared with 745 (excluding definitions) in Part 11. A neat and effective way to write a regulation and perhaps if the FDA get round to revising Part 11, they can learn from this simple approach. The reason is that the primary authors of Annex 11 are the inspectors themselves and not lawyers.

However, looking at the way Annex 11 is written there are issues concerning electronic signatures that directly impact on the design of software used in GMP regulated laboratories. Clause 14 requires that electronically signed electronic records or a report of an analysis must be available outside of the computerized system that generates it but within the boundaries of your company. This is not an unreasonable requirement as the users of the information generated by an analytical laboratory typically reside outside of the laboratory in development, regulatory or manufacturing. After the laboratory data have been interpreted by an analyst, a report will be prepared with an electronic signature attached to the report.

The electronic signature must therefore be applied to a representation of the records to which it pertains and not stuffed as an afterthought by a vendor's software engineer into the audit trail where it is difficult to see that the record has been signed. In short, the record and the signature must be together, as clause 14 makes perfectly clear. Furthermore, the linkage between the signature and the record interpretation must be permanent as required by Annex 11. How this is to be achieved is left to the software vendor to interpret and the laboratory to see if it complies with their interpretation of the regulation. However if the signature is not attached to the record, then the system does not comply.

Furthermore, the signature and record must be secured to prevent tampering, otherwise how can it be considered permanent? Thus if an attempt was made to replace a signature or to change the results on a signed report, the attempt would be recognized and the report invalidated or corrupted to indicate tampering.

However, many CDS have the signature in the audit trail which is a pointless exercise from the perspective of the laboratory. What needs to happen is that the electronic signature is attached to the appropriate report/record and an entry of the activity goes into the audit trail that the report/record has been signed. When the signed report is seen outside of the system you know it has been signed as the electronic signatures of the analyst and the reviewer are seen on the report

Summary

In this column I have looked at the technical requirements of EU GMP Annex 11. Most computerized systems in the laboratory comply with these regulations but there are exceptions to this that process owners need to be aware of before an inspection or audit. The main problem areas are printouts showing data have changed since entry or acquisition, review of audit trails and attachment of electronic signatures to the associated electronic records so that the signature is effective outside of the system but within the boundaries of the company.

"Questions of Quality" editor **Bob McDowall** is Principal at McDowall Consulting, Bromley, Kent, UK. He is also a member of *LCGC Europe's* Editorial Advisory Board. Direct correspondence about this column should be addressed to "Questions of Quality", *LCGC Europe*, 4A Bridgegate Pavilion, Chester Business Park, Wrexham Road, Chester, CH4 9QH, UK, or e-mail the editor Alasdair Matheson at amatheson@advanstar.com

References

(1) EU GMP Annex 11 Computerized Systems (2011).

(2) R.D. McDowall, *LCGC Europe*, **24**(4) 208–216 (2011).

(3) 21 CFR 11 Electronic Records; Electronic Signatures final rule 1997.

(4) R.D. McDowall, *LCGC Europe*, **25**(4) 194–200 (2012).

(5) Supplementary requirements: Annex 11 Computerized Systems, available on the web at: http://www.ema.europa.eu/ema/index.jsp?curl=pages/regulation/q_and_a/q_and_a_detail_000027.jsp&murl=menus/regulations/regulations.jsp&mid=WC0b01ac05800296ca