Data Integrity in Pharmaceutical Quality Control Laboratories: What You Need to Know

Whitepaper

Author

Loren Smith,
Agilent Technologies, Inc.
Santa Clara, CA USA

Data integrity problems in pharmaceutical quality control laboratories are driving more regulatory action than ever before. What has changed to drive all this activity? While plenty of information is available, much of it seems to confuse rather than clarify. This article will dispel common myths by looking at facts, based on a study of available resources and direct interactions with U.S. Food and Drug Administration (FDA) staff and their consultants. It will discuss the following:

- How to put the current enforcement environment into historical context.
- How to apply critical thinking skills to various myths regarding data integrity.
- How to evaluate current laboratory software and associated processes against new expectations.
- How vendors are redesigning laboratory software to help respond to new realities.

Agilent Technologies

Definition and History of Data Integrity and FDA Compliance

In an article in Scientific Computing (September 2013), Bob McDowall defined data integrity as "generating, transforming, maintaining, assuring the accuracy, completeness, and consistency of data over its entire life cycle in compliance with the applicable regulations."

A common myth is that the applicable regulations are new. But 21 CFR Part 11, Electronic Records; Electronic Signatures was first released in 1997. In 2003, after the pharmaceutical industry spent years struggling with the regulation, the FDA released its Scope and Application guidance, clarifying some of the requirements in Part 11. This guidance also included a discussion of the FDA's selective enforcement strategy based on what the administration was finding during its inspections. In 2010, the FDA announced its focus on data integrity inspections. At that time, however, few people within the FDA were qualified to understand the data integrity aspects of computerized systems. So, the FDA started a significant training exercise in data integrity, data integrity inspections, and regulations for personnel that included chemistry experts, manufacturing experts, and people with other GxP expertise. They also hired experts in fraud investigation, including people from the U.S. Federal Bureau of Investigation. Thus, beginning in 2013, data integrity has been a primary inspection point, and there has been a visible increase in data integrity enforcement across all geographies. In addition, starting in 2014, as a result of those inspections, the FDA has often included the names of hardware and software products in their warning letters and related public information documents in a less than subtle message to the hardware and software makers that the administration expects them to assist customers with data integrity and compliance concerns.

Mythbusting

Another myth commonly heard is that if a pharmaceutical company is using a particular software system, the FDA will shut them down. The concern was expressed this way: "Systems throughout manufacturing organizations and laboratories may have potential weaknesses that could be considered a data integrity risk. If that weakness has not been exploited, does the FDA have grounds for delivering an observation in a 483 warning letter?"

The clear answer is no. Capability does not equal violation. Consider this analogy: The speed limit throughout much of the United States is 65 miles per hour, but my car's ability to exceed that limit does not justify a citation. Similarly, in a pharmaceutical company, if potential data integrity weaknesses have not been exploited for data manipulation or deletion of data (or other fraudulent activities), then there is no basis for the agency to issue a citation or warning letter. One should expect a detailed conversation with the inspector, as the focus will turn to procedural controls to ensure that the known weaknesses are not exploited.

Procedural Versus Technical Controls

Let's consider the statement: "This software is Part 11 compliant." There are a few problems with this statement. First of all it is a logical impossibility. There are components of Part 11 that are not meant to be satisfied by technical controls within a computerized system. For example, CFR Part 11.10(j) requires policies for the use of electronic signatures. This is a requirement that a chromatography data system is not going to satisfy. It is an element of the regulation, but it is not something that is expected to be a technical control. The software, in fact, does not comply with regulations. The software itself is inert; software contains the technical controls to support compliance with the applicable regulations. In addition to technical controls, procedural controls must also be in place. A discussion about procedural controls versus technical controls is often seen in FDA warning letters, particularly when gaps in a system's ability to support technical controls required by various regulations have been exploited.

A standard operating procedure (SOP), used as a procedural control, can substitute for a technical control as long as:

- People are trained on that SOP
- The SOP is followed
- Adherence to the SOP is confirmed by quality oversight and/or compliance auditing

Often, however, even if SOPs exist, they are not followed, and adherence isn't properly verified. Consequently, the FDA will demand system remediation to prevent a recurrence of the behavior.

Audit trails within computerized systems are an example of technical controls. The software must be able to generate audit trails that contain all the components the regulations require, and then those controls must be enabled.

Audit trail records automatically (21 CFR Part 11.10(e)) show that the system is working and it's doing its job properly, and can be consulted in an audit or an inspection without any extra work by the humans.

Certificates of Software Validation or Capability: Do They Provide Value?

Many software vendors provide a Certificate of Software Validation, or they may issue a certificate along the lines of 21 CFR Part 11 Readiness Claims. Such a certificate has limited value, because the FDA expects the software to be validated for its intended use by the users in the environment where it will be used. While vendors should engage customers to build and design systems according to customer needs, and spend considerable time testing that software before they deliver it, the development and testing work does not (and cannot) substitute for the customer declaring their intended use and then validating their system according to that intended use.

Another related point is that the FDA does not have legal jurisdiction over a vendor's informatics software organization. So (unless the software is registered as a Medical Device with the FDA) any documentation that the vendor might provide cannot be recognized by the FDA because of that lack of enforcement authority.

Vendors may be able to provide detailed information about a product's abilities relative to Part 11, but that information is based on the vendor's interpretation of the regulations. This interpretation may or may not agree with various pharmaceutical manufacturers, or the FDA itself. The vendor's interpretation cannot substitute for an audit to determine the software's functional ability to satisfy regulatory concerns.

Your Responsibilities: Audit, Assess, and Validate

Data integrity compliance responsibilities include vendor audits, a computer system assessment, and software validation.

When auditing vendors, there is a fourfold dilemma, or a set of problems that are focused on by the auditors themselves. (See Mourrain, J., Therapeutic Innovation and Regulatory Science, Volume 40 (#2), pp. 177-183.)

The first dilemma is disparity. Regulations are few. The Part 11 regulation, for example, is a grand total of three pages, not counting the information in the preamble of the 1997 Federal Register entry. Guidelines are many, and interpretations of the guidelines are even more plentiful. The disparity of interpretation is the problem in many auditing situations. For example, a customer during an audit might see a regulation a certain way, whereas the vendor may look at the regulation differently.

Partiality is also an issue with auditors. Audit reports are partial, meaning incomplete. Certain auditors feel they need to have a large number of audit findings. As a result, they will have separate findings for every problem in every SOP, and they will list all of them separately, creating the potential misconception that the audit report is good based simply on volume. Other auditors may take examples and put them into a few large observations to support their case for a major finding in an audit. It is possible that neither of these types of reports will tell the whole story of what was learned during the audit.

Another auditor issue is variability. Auditors, to no one's surprise, are human. Some auditors will obsess over certain subjects such as disaster recovery, while others are consumed with Part 11.

Legibility (not in the handwriting sense) is next. Auditors may be able to communicate the issues that they find during an audit. However, they are often challenged to communicate the "So what?" That is, the computerized system impact on patients, to the product, and to data integrity.

What is the solution to these audit dilemmas? The solution is a model, rather than a checklist, the components of which include:

- Procedures
- Training of personnel
- Software development activities
- Testing activities
- Quality management systems
- Infrastructure

The latter is often irrelevant unless the vendor takes custody of the GxP records in, for example, a cloud-based application.

In a model approach, scoring can make what is a fairly subjective process into an objective measurement system that supports a defensible individual vendor audit, as well as comparative evaluations between multiple software or service vendors. The point of all this activity is that the vendor audit can contribute to a risk-based validation strategy (a la FDA's General Principles of Software Validation, Section 6.3). The better job a vendor is doing, the less work required (at least theoretically) during software validation.

Assessing the Software's (and the Vendor's) Compliance Support

Assessing a software's ability to support compliance requires attention to all the regional regulations where a regulated company does business or may intend to do business. Some regulated companies, if they are solely doing business within the United States, or solely within Europe, may choose to pay attention only to Part 11, or only Annex 11 requirements. Part 11 and Annex 11 share commonalities. However, any software evaluation for compliance should be based on evidence rather than hearsay (that shiny Part 11 Certificate).

Agilent, like many other vendors, receives numerous customer checklists, and provides straightforward responses with product answers. However, it is important that the evaluation of the responses be based on evidence, rather than being strictly limited to what the vendor has said that the system will do. Areas for review should include data integrity issues, access controls, audit trails, device checks, etc., as per applicable regulations. This review is valuable during a software assessment process because observed gaps indicate where procedural controls or customization may be required. Feedback to the vendor regarding any gaps observed is therefore important so that the procedural controls or custom solutions do not become permanent.

Another common software compliance support myth is, "I bought the vendor's IQ/OQ package, therefore my system is validated." However, buying the vendor's validation package (traditionally limited to a basic software IQ and a core, generic OQ) is insufficient to validate the system for its intended use. Validation responsibility cannot be abdicated to vendors, but they are (or should be) a reliable source of information and assistance for your validation effort.

A corresponding validation myth that is, "Any system change requires full revalidation." The reality is that whenever software is changed, the software change must be evaluated to determine the impact of the change on the entire software system, and the risk of that change to patient safety, product quality, or data integrity. Often, companies will limit their change validation to the change only, or they will go to the other extreme and they will needlessly repeat the entire validation. The right answer is somewhere in between.

In Conclusion: Agilent's Response

Agilent's goal is to avoid shipping software that introduces or maintains regulatory exposure for customers, by incorporating FDA priorities into our system designs. The FDA is clearly pushing for more technical controls, prioritizing technical controls over procedural controls, and prioritizing prevention controls over detection controls. That's why 21 CFR Part 11.10(a) talks about systems needing to have "the ability to detect invalid or altered records." That is the only part of the regulation that actually talks about detecting records that may have been manipulated through nefarious means. The rest of the controls are preventive. So yes, detection controls are important, but prevention controls are better. Prioritizing online records over hard copy printouts has also been emphasized. The FDA cannot always trust the paper that's being handed to them.

Another example of system design is the use of an online audit trail review. Many systems may generate audit trail reports in printed form, but the new version of the Agilent OpenLAB Chromatography Data System has a built-in tool that allows a user to electronically review electronic audit trails entries. These audit trail entries are organized by type, an online review can be performed, and electronic signatures incorporated.

These examples serve to demonstrate how Agilent is applying critical thinking to redesigning laboratory software to help respond to new regulatory compliance realities.

Frequently asked questions

Question: Will new data systems eliminate all need for procedural controls?

Answer: No; the needs for procedural controls will decrease based on additional technical controls, however certain procedural controls such as system administration or user administration will always be required. Another procedural control involves having policies and procedures regarding the legal application of electronic signatures. Ideally the number of procedural controls would decrease to the point that the system is covering the human variability important to the data integrity and the procedures around the systems will remain.

Question: When software is updated my, how much revalidation is required?

Answer: The FDA guidance: General Principles of Software Validation focusses on two points related to revalidation. First, changes to the system must be evaluated for their relative impact to the particular company's intended use for the system. For example, instrument support functionality changes may not be related to a user's particular instrument configuration or may reflect unused features. From the vendor's release documentation, it should be possible to determine what features and functionality have been updated, and what defects in the software have been corrected. Any changes should be compared against the intended use to determine any revalidation impact.

Second, whenever software is changed, the user should evaluate the change themselves, including some degree of regression testing to confirm that the change in the software or the updated software has not broken something else in some way that may have had unintended consequences. It is not uncommon, for example, when updating software for home computers or phones to find that features that worked before the update may not work afterwards.

Question: How do you deal with automatic updates of Windows or antivirus programs?

Answer: Another item the FDA has started discussing more in the last few years, in conjunction with the ISPE GAMP v5 Guidance, is the concept of risk and risk-based validation. One of the things to think about with operating system and antivirus updates is the relative risk of having e.g. a security problem or a virus vulnerability in a system. Sometimes the update risk may be greater than the original risk to the system itself (or vice versa). Some companies have the luxury of staff to deal with networks and server infrastructure qualification and can insulate operating systems from the software validation itself, having the responsibility to make sure that the systems are being kept current with security and antivirus updates. As a general practice companies should periodically run a small set of standard regression tests, triggered by operating system or antivirus updates or simply on a periodic basis, to make sure that changes do not have any adverse impact on the system.

Question: When a new PC is implemented, is it necessary to revalidate the software?

Answer: If the new PC has the same or greater capabilities than the original and is using the same version of the operating system and software, revalidation is not necessary since the functionality of the system is the same. However, repeating the installation qualification activities to confirm that the software has been properly installed or restored properly from the backup onto the new PC is required.

One detail that can make this process more efficient is to avoid overly detailed specification documents. Avoid specifying a particular model of PC, particular processor speed, or a particular memory or disk capacity. Use of the designation "or higher" will prevent having to continually update the documentation as technology advances.

Question: Regarding GMP lab data integrity: once data are required, can they be modified under any circumstances?

Answer: Acquired data, the data coming directly from the instrument captured by the PC should be considered sacred; raw data should not be modified for any reason. However, a second kind of data, generated during post acquisition data analysis and data processing, e.g. reintegration, changing baselines, deleting peaks that aren't necessarily relevant to the analysis, or other calculations, are considered normal parts of data processing and may be modified under controlled circumstances as captured in audit trails.

Question: Software sometimes has complicated calculations or algorithms in it, for example, for the integration of chromatograph, is it necessary for the software user to validate the results?

Answer: Yes, calculated results must be validated. Not all of Microsoft Excel's calculations, but any specific calculations programmed into a configurable report, e.g., CDS reporting capabilities using report templates and automatic calculations. If calculations are used to determine whether or not a particular result is within specifications, the calculation will need to be validated with data both within and out of specification to ensure that the calculations are working properly. This validation also evaluates the vendor's ability to build good software and perform accurate calculations.

Question: Once a vendor is audited, is there a recommended time within which that vendor should be re-audited?

Answer: There are several factors to consider when determining the frequency of vendor audits, many related to the relative risk of the system to patient's safety, drug product quality, and data integrity. One factor is the vendor's performance and response from previous audits. If they performed well, re-auditing those vendors every three years could be justified, but not longer. For other vendors that are mission critical or perhaps those that didn't perform well in prior audits, re-auditing every 12 months is justified to increase scrutiny.

Question: What should the auditing approach be for software such as the CDS that is no longer supported by the vendor but is still being used within the validated state?

Answer: Vendors will occasionally go out of business, or more commonly, discontinue support of a particular version of their software. If a user continues to use the software, it would be at an increased level of risk because if a problem arises, the vendor may not exist to actually address the defect or willing to correct defects in obsolete versions of software they no longer support. The risk is, however, somewhat instrument and software dependent, particularly for older instruments and software. As long as those systems are being managed and used properly, there may not be a reason to update them. Agilent regularly considers whether or not upgrades provide enough value, enough new functionality, or enough defect fixes to be able to justify the cost, the time, and the pain involved in replacing or revalidating the system.

Question: What is regression testing?

Answer: Regression testing is a way to confirm that features working prior to any change are still working. Regression testing should involve either the most commonly used functions in the system and/or the most high-risk functions determined during risk-analysis to determine whether or not a particular software update has changed something not directly addressed in the vendor's documentation. That is to confirm that the system itself has not regressed or that a change has not introduced some kind of an unintended failure.

Question: How can I ensure and prove that SOPs are followed?

Answer: Through audits. Audits are the only way to follow up to make sure that people are doing what they have been trained to do.

Question: Do pharma companies typically do onsite audits at Agilent to review SOPs, et cetera or are these audits typically paper audits?

Answer: Approximately 90 percent of the informatics software product audit requests that Agilent receives are paper audits, and the remaining 10 percent will actually come and do onsite audits. However a paper audit is not evidence based. It is based on declarative statements, or whatever Agilent chooses to say, so there is nothing in the way of verification of anything that is said in a paper audit. Paper audits are typically performed by "box checkers"—people doing the paper audit so that they can say that they did it. Some customers will use a paper audit as a preamble to an onsite audit to get a rough idea of Agilent's position before they come onsite.

Question: Some say that [purchasing] the IQ-OQ package [as a complete validation solution] is a myth.

Answer: The IQ-OQ package itself is real, not a myth. However, the IQ-OQ package is necessary but insufficient because it does not satisfy all the FDA's requirements for validating a computerized system. For example, the IQ-OQ package does not include validation planning documentation or validation summary reporting. The IQ-OQ package also does not include requirement specification, user requirements, a functional specification, or traceability from the IQ and OQ test themselves to the user's requirement either user requirements or functional specification.

Question: What about systems with no audit trail or an incomplete audit trail? What's the work-around for such systems?

Answer: There are many old systems that still get used in regulated labs, and the systems work perfectly fine to do what they do. But the work-around for this is a heavy dose of procedural controls that would include handwritten records. Depending on the criticality and the risk of the particular process that's involved, or that the system is addressing, the procedural requirements may need to go as far as a second person verification of information or actual concurrent witnessing of the work being performed. The purpose of the audit trail is to be able to tell the story or reconstruct the history of an electronic record, not just the creation of that record but also the changes or the deletion of records. If the system has limited or incomplete audit trail ability, then the record must be supplemented in some other way, often taking the form of paper records. For example, a use notebook next to an instrument. Technical controls make everybody's life much simpler.

Question: Will new data systems eliminate all need for procedural controls?

Answer: No. Procedural controls will always be required. For example, the procedures for granting users access to a data system or the procedures for changing, modifying, or removing a person's access to a data system would be examples of procedures that are required by the regulation that the data system is not necessarily going to be able to address. Currently, the data system can create those accounts and change user privileges. But the procedure for how that is done is normally going to require some type of record keeping that includes management reviews and approvals of system access or changes to system access. So, procedural controls are not going to go away completely.

Question: Is it an essential element to execute a disaster recovery process on a manufacturing kit during qualification, and do you see any risk with respect to software removal?

Answer: Disaster recovery testing is expected by the regulations. European regulations are slightly more explicit on the subject. A disaster recovery test can often fail due to incorrect assumptions. Disaster recovery testing is particularly useful for mission-critical systems.

Question: Are there examples of audit trail review that are less cumbersome than what Agilent is building into its software?

Answer: Some systems that have electronic audit trails don't have the means to indicate that those audit trails have been reviewed, resulting in having to divide the audit trail review into smaller chunks and primarily having those audit trails be very, very relevant to the data that is being reviewed. For example, for pharmaceutical batch release, a QA review must be performed for all the relevant records that go into manufacturing that product and all the systems that support its manufacture. If the QA review looks at audit trail entries that are relevant to those records, even if it happens to be on paper the audit trail review is more relevant to the record review itself. So the review is less cumbersome simply as a result of dividing the problem into smaller chunks that are more relevant to the actual record.

Question: Can you talk about addressing the challenges of peak integrations in auto mode instead of manual?

Answer: Automatic peak integrations are normally addressed in a procedure that determines the parameters for the allowed automatic peak integrations and potential reintegrations. Generally, the flexibility of the integration or reintegration activity is addressed in an SOP and part of the system or process validation for that particular analytical method.

Question: At some point, there must be an administrator for every system who will have access to modify or delete records, how do you recommend dealing with this potential data integrity problem?

Answer: The best practice for selecting a system administrator is making sure that the administrator on a particular system does not have a vested interest in the data on that system. What this means in larger organization is that often someone in the IT department is in charge of administering the system. Separation of duties is a subject that IBM has discussed in the past, and it is also significant in the financial world. If a person has no motivation to do anything with the data on that system, then it's unlikely that there will be a problem. The FDA has said that if there is any evidence of intentional fraud that they would pursue it as a criminal activity, and that is something that they do look for.

Question: When samples are processed, is an audit trail comment enough or is an approval process also necessary?

Answer: It depends on what a company's policies and procedures expect. If there are sufficient controls in the system and people are sufficiently trained, so that when sample reprocessing occurs, it's occurring under the proper conditions with the proper controls and procedures in place, then the audit trail comment may be enough. However, if the procedure doesn't address the reprocessing of samples, or if it's considered anomalous or unusual, then it may be important to have an explicit documented approval process.

Question: Is it ever acceptable to delete data in the eyes of the FDA?

Answer: The FDA has answered this question explicitly and implicitly in two different areas. First, they talk about data retention requirements for pharmaceutical products, and the requirement is to maintain pharmaceutical manufacturing records for seven years after the expiration of the last manufactured lot of a particular pharmaceutical product. So, if after seven years production of a drug product is halted, and the product has an expiry that's 12 or 18 months out, then seven years after that expiration date, it is acceptable to delete data. Second, CFR Part 11 specifies that audit trails need to deal with three things: they need to deal with creation of regulated records, modification of regulated records, and the deletion of records. However, pre-Part 11 in the mid-90s, the FDA found that many companies, in their analytical laboratories, were deciding that the final analytical report was the regulated record, and companies were deleting the raw data.

Question: Is a vendor postal audit enough to satisfy GMP requirements?

Answer: Time and resources will play a role in deciding how to approach audits. One approach is to organize software suppliers based on a risk assessment—risks to patient safety, product quality, and data integrity for a particular system, based on the results of prior audits. If vendors have gone through audits and produced positive results in the past, then that can be factored into the risk assessment for that particular vendor. In that way, a determination based on risk can define the audit cycle for many suppliers.

www.agilent.com/chem/OpenLAB

Published in the USA, June 20, 2016
5991-6827EN

Agilent Technologies