http://www.pharmtech.com/data-integrity-analytical-laboratory

Data Integrity in the Analytical Laboratory

Data integrity in the analytical laboratory is an area of increasing focus for regulators such as FDA.

May 02, 2014

By Paul Smith

Pharmaceutical Technology

Volume 38, Issue 5

BARIS SIMSEK/E+/GETTY IMAGES

Most companies have experienced being audited and, where necessary, "defending" the work carried out in their analytical laboratories during audits. Historically, laboratories have tended to provide information about the validation of their methods and procedures, the qualification and suitability of their analytical equipment, and information about training of their laboratory staff as justification for the validity of the analytical results.

Nonetheless, the focus on data integrity by FDA, the United Kingdom Medicines and Healthcare Products Regulatory Agency (MHRA), and other regulatory bodies during audits may mean that historical approaches to laboratory audit preparation and audit "defense" is simply not enough. In a data integrity-focussed audit, the emphasis has moved away from providing information based on technical justification and scientific rationale towards providing evidence that the analytical results are not fraudulent. This is almost a "guilty until proven innocent" approach and can be very different to historical audits. For any laboratories that are not prepared for this change, the audit will at best be "uncomfortable" and at worst may present a potential high risk to the organization.

FDA warning letters (1-3) and the recent announcement of MHRA (4) have highlighted the increasing focus on data integrity in the laboratory. Data integrity is a subject that many laboratories currently have significant concerns about (5). To add to those concerns, even the term "data integrity" can have widely differing meanings or interpretation, and there are currently few definitive reference sources available on the subject.

What is ALCOA?

The acronym ALCOA has been widely associated with data integrity by FDA and was first used by Stan Woollen when he worked for the agency to help him remember compliance terms relevant to data quality (6). The good automated manufacturing practice (GAMP) guide "A Risk-Based Approach to GxP Complaint Laboratory Computerized Systems" (7) includes an appendix (Appendix 3) on data integrity. The terms used in the appendix are sometimes referred to as "ALCOA +" because they incorporate additional terms based on the European Medicines Agency's concept paper on electronic data in clinical trials (8). The terms associated with ALCOA + are described as **A**ttributable, **L**egible, **C**ontemporaneous, **O**riginal, **A**ccurate, complete, consistent, enduring, and available (see **Table I**).

Table I: Terms associated with ALCOA +

"*ALCOA*" abbreviation		**Description / Explanation**	**Comments**
A	Attributable	Who performed an action and when? If a record is changed, who did it and why? Link to the source data.	**Who did it?** **Source data**

L	Legible	Data must be recorded permanently in a durable medium and be readable.	**Can you read it? Permanently recorded**
C	Contemporaneous	The data should be recorded at the time the work is performed and date / time stamps should follow in order.	**Was it done in "real time"?**
O	Original	Is the information the original record or a certified true copy?	**Is it original or true copy?**
A	Accurate	No errors or editing performed without documented amendments.	**Is it accurate?**
Complete		All data including repeat or reanalysis performed on the sample.	**21 *CFR* 211.194**
Consistent		Consistent application of data time stamps in the expected sequence.	**Date time stamps**
Enduring		Recorded on controlled worksheets, laboratory notebooks or electronic media.	**Medium used to record data**
Available		Available / accessible for review / audit for the life time of the record.	**For the life time of the record**

Comparisons are often made between secure electronic data and data that are available in paper format. The comparison results in similar conclusions that electronic data are more secure, more difficult to manipulate or change, and any changes are easier to detect (assuming that the software is technically compliant to *21 Code of Federal Regulations (CFR) Part 11* (9) and technical controls are appropriately implemented). On the other hand, changes to paper data, such as a printed chromatogram, are simpler to make, but much harder to detect. FDA has previously advised that defining paper records as "raw data" (the so-called typewriter rule) does not satisfy the predicate rules, that the industry has misinterpreted the 2003 21 *CFR Part 11* Scope and Applications Guidance (10) and that "the printed paper copy of the chromatogram would not be considered a true copy" (11). Although this comment was made about chromatographic data, the principles have much wider implications.

The available evidence and the regulatory data integrity focus implies that paper is "bad" and that laboratories should implement fully electronic systems that move away from paper or even hybrid systems as soon as possible. However, with many laboratories concerned about data integrity and unsure what to do, this implementation strategy could be a potentially dangerous over-simplification. It could result in an over-concentration of resource "only" on ensuring security of electronic systems when there may be other significant risks.

FDA observations around computer security, sharing passwords, and/or not activating audit trails are not new, and certainly, if a laboratory finds itself in this situation, it should act immediately. For most laboratories, however, implementing a fully electronic approach may represent a significant change from what they actually do now. To put into perspective the scale of the change that might be required, many laboratories currently still define printed copies as their raw data despite FDA's clarification in its guidance on records and reports (11). Additionally, many laboratories perform chromatography calculations manually or using software such as Microsoft Excel, rather than the chromatography data system (CDS). Manual calculations present one of the highest data integrity risks, even where traceability to the "source" data used is unambiguous. In extreme cases, FDA have identified instances where sample weighing practices could mean laboratories have calculated and entered the sample weight after the injections so that the result would pass specifications (12). Therefore, laboratories need to take a strategic approach to implementing data-integrity improvements.

Common data-integrity issues

Where should the laboratory start preparing for data integrity? Some of the common issues that repeatedly come up in FDA warning letters are:

- **Common passwords.** Where analysts share passwords, it is not possible to identify who creates or changes records, thus the A in ALCOA is not clear.

- **User privileges.** The system configuration for the software does not adequately define or segregate user levels and users have access to inappropriate software privileges such as modification of methods and integration.
- **Computer system control.** Laboratories have failed to implement adequate controls over data, and unauthorized access to modify, delete, or not save electronic files is not prevented; the file, therefore, may not be original, accurate, or complete.
- **Processing methods.** Integration parameters are not controlled and there is no procedure to define integration. Regulators are concerned over re-integration of chromatograms.
- **Incomplete data.** The record is not complete in this case. The definition of complete data is open to interpretation--see references 13 and 14 for a detailed analysis of FDA 483 observations on complete data (*21 CFR 211.194* and sub parts).
- **Audit trails.** In this case, the laboratory has turned off the audit-trail functionality within the system. It is, therefore, not clear who has modified a file or why.

Process flow mapping in data integrity

To balance the focus on electronic data that data integrity tends to drive, a useful approach is to map the workflow within the laboratory, to identify and list all of the steps performed for each analytical technique (from sample receipt to approval of results) and each laboratory operation. For each step, the mapping should identify:

- What actions are performed
- How those actions are performed
- How they are recorded
- Any decisions made
- The extent to which the process is manual or automated
- The possible risks associated with the step (e.g., how could fraud be prevented or detected).

In some instances, this type of mapping may have already been performed (e.g., Lean Sigma, Six Sigma). Even if this is the case, it should be reviewed. One of the purposes of data-integrity auditing is to actively look for evidence of fraud, and previous mapping exercises may not support the change in focus.

Identification by infrared

Using infrared identification as an example of an analytical technique, the steps, decisions, and actions performed when an analyst completes material identification by infrared spectroscopy have to be identified. For infrared, the high-level process steps associated with performing material identification are shown in **Figure 1** and appear relatively simple.

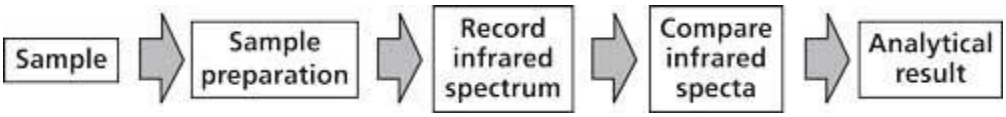

Figure 1: High-level flow chart for material identification by infrared spectroscopy.

Nevertheless, when these steps are examined in detail, it soon becomes apparent that many of the steps have data integrity and/or scientific compliance risks associated with them. **Figure 2** shows an expanded representation of the flow chart shown in **Figure 1**. Fundamentally, the way the sample is prepared for examination by infrared has a significant influence on the quality of the spectrum obtained.

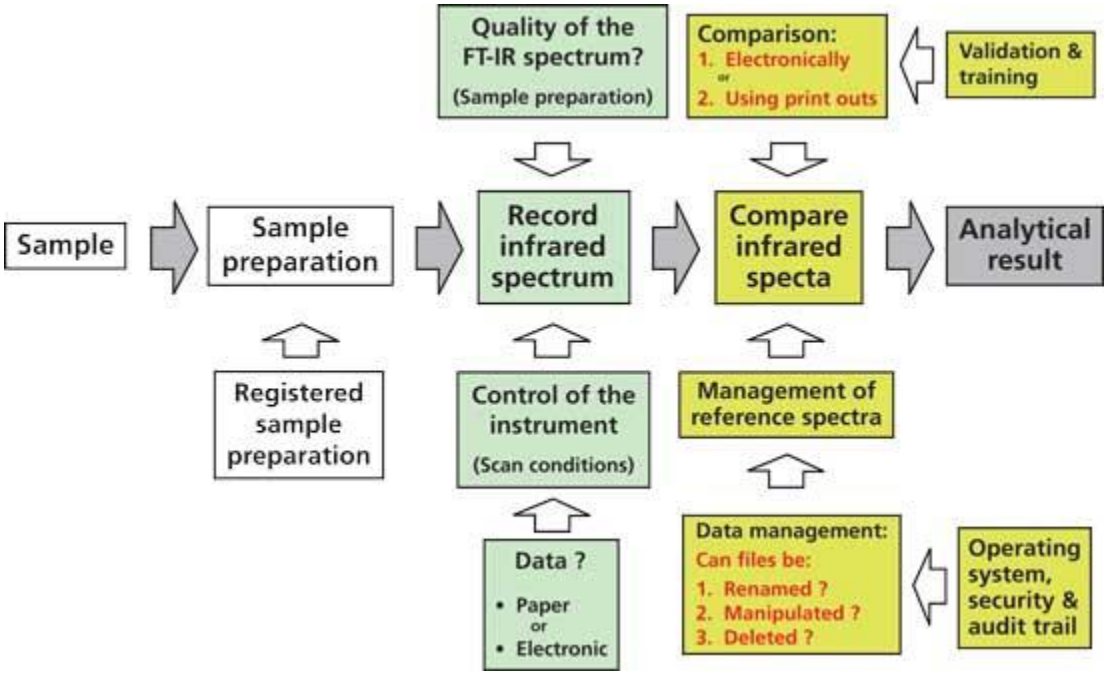

Figure 2: Expanded flow chart for identification by infrared. FT-IR is Fourier transform infrared spectroscopy.

Historically, laboratories may have "rejected" a spectrum before comparison with the reference based on sample preparation (provided this was documented in the analysts infrared training). However, in the data-integrity world, this approach would now be interpreted as the spectroscopic equivalent to a laboratory performing "test injections" on an HPLC system (1-2, 12) and will, therefore, be difficult to defend. Hence, although warning letters have been issued because the laboratory was renaming infrared spectra, there are also warning letters associated with poor use of the technique (see reference 15 and warning letter review).

For the software used to control the instrument and record the spectra, the system administrator may be required to show the auditor the "live" system and answer detailed questions about how audit trails are implemented, provide information on the security features of the software, and explain the system configuration options. Consequently, the choice of system administrator is no longer just a technical decision—they must be confident under the pressure of a data-integrity audit.

The laboratory must be able to defend the conditions it uses to record spectra relative to pharmacopoeia requirements and explain how any differences found between spectra are managed. Subjective tests need careful monitoring. If this is an electronic comparison, the software algorithm performing the comparison must be validated, while a manual comparison of spectra must be included in a documented training process.

Finally, are the electronic files secure or is the laboratory defining the print out as raw data? How can the audit trail be applied to detect changes to the spectra, and are the electronic files being examined when quality decisions are being made?

Even for something as apparently simple as identification by infrared spectroscopy, when the process is mapped, a number of additional potential compliance risks can be identified, which might not be the case if the focus is only on the management of electronic data. Process mapping can, therefore, help identify "scientific validity" concerns from a data-integrity perspective, as well as highlight areas of high data-integrity risks.

References

1. FDA, FDA Warning Letter WL:320-13-21, July 2013, accessed Apr. 9, 2014.
2. FDA, FDA Warning Letter WL:320-14-005, Mar. 2014, accessed Apr. 9, 2014.
3. FDA, FDA Warning Letter WL:320-13-26, Sept. 2013, accessed Apr. 9, 2014.

4. MHRA, "MHRA expectation regarding self-inspection and data integrity," accessed Apr. 9, 2014.
5. Agilent compliance seminar, *"La conformità del laboratorio"* (Milan, Italy, Apr. 2014).
6. S.W. Woollen, *"Data Quality and the Origin of ALCOA,"* in Newsletter of the Southern Regional Chapter Society of Quality Assurance, Summer 2010, accessed Apr. 9, 2014.
7. ISPE GAMP Good Practice Guide, "A Risk-Based Approach to GxP Compliant Laboratory Computerized Systems," Second Edition, ISBN 978-1-936379-48-4, ISPE Publication, 2012.
8. EMA, GCP Inspectors Working Group publication, *Reflection paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials*, (London, June 2010).
9. *Code of Federal Regulations*, Title 21, Food and Drugs (Government Printing Office, Washington DC,) Part 11, accessed Apr. 11, 2014.
10. FDA, *Guidance for Industry, Part 11; Electronic Records, Electronic Signatures, Scope and Application*, (Rockville, MD, Aug. 2003).
11. FDA, *Guidance and Answers on Current Good Manufacturing Practices, Level 2 Guidance--Records and Reports, Question 3*, accessed Apr. 9, 2014.
12. FDA, FDA Warning Letter WL:320-13-22, July 2013, accessed Apr. 9, 2014.
13. R. D. McDowall, LC-GC *Eur. 26* (6) 338-343 (2013).
14. R. D. McDowall, LC-GC *Eur. 26* (7) 389-392 (2013).
15. P.A. Smith and J. Sellers, *Pharm. Technol. Eur*. 23 (9) 85-89 (2011).

About the Author

Paul Smith is EMEAI laboratory compliance productivity specialist at Agilent Technologies UK Ltd, 610 Wharefedale Road, IQ Winnersh, Wokingham, Berkshire RG41 5TP, United Kingdom, paul_smith@agilent.com.