http://www.spectroscopyonline.com/spectroscopy/Articles/Can-You-Demonstrate-the-Integrity-of-Your-Data/ArticleStandard/Article/detail/859588?contextCategoryId=38141

Can You Demonstrate the Integrity of Your Data?

Nov 1, 2014

By: R.D. McDowall

Spectroscopy pp. 22-27

Recently, regulators in both the United States and United Kingdom issued guidance concerning laboratory data integrity that followed serious noncompliances found during inspections. In this column, we explore what this guidance means for spectroscopy systems used for analysis in regulated laboratories and derive some common-sense guidance that you can follow.

Ensuring the integrity of data is a prime requirement of any analytical laboratory so that the results generated and the decisions taken using that information can be relied upon. This is certainly so in laboratories working toward good practice regulations such as good laboratory practice (GLP) and good manufacturing practice (GMP).

Data integrity is defined by the Food and Drug Administration (FDA) as "The degree to which a collection of data is complete, consistent and accurate" (1). This is similar to the GMP requirement for complete data from quality control testing under the United States (US) GMP regulations (2), which I discussed in the April 2013 installment of this column (3). Going further, the Institute of Electronic and Electrical Engineers (IEEE) defines integrity as "The degree to which a system or component prevents unauthorized access to, or modification of, computer programs or data" (4). From the IEEE definition, we can focus on a computerized system that needs to have controls to only allow authorized users access to the system and technical controls to prevent unauthorized changes to the data entered or generated by the laboratory system. Not bad when you consider that the IEEE is not a regulated health care organization, but the requirements outlined in their definition equate to those in the US GMP (2).

Following the Able Laboratories fraud case (5) the FDA also revised its *Compliance Policy Guide* (CPG) 7346.832 for preapproval inspections (PAI) (6), which has three objectives, the third of which is the data integrity audit. Under this objective an FDA inspector has to "audit the raw data, hardcopy or electronic, to authenticate the data submitted in the CMC [chemistry, manufacturing, and controls**]** section of the application. And to verify that all relevant data ([for example,] stability, biobatch data) were submitted in the CMC section such that CDER [Center for Drug Evaluation and Research] product reviewers can rely on the submitted data as complete and accurate."

This focus on data integrity especially around computerized systems has found many noncompliances in a variety of quality control (QC) laboratories. I summarized some of the data integrity issues that were found in recent FDA inspections involving chromatography data systems in a recent article in *LCGC Europe* (7). The main areas of noncompliance were citations against four main areas of the Code of Federal Regulations (CFR):

- Quality management system and management responsibility
- Automatic and electronic equipment (§211.68)
- Laboratory controls (§211.160–§211. 165)
- Laboratory controls (§211.194 a–e) (7)

Interestingly, this focus on data integrity has not gone unnoticed on the other side of the Atlantic Ocean.

UK Regulatory Agency Focuses on Data Integrity

Table I: MHRA expectation for data integrity focused internal audits (SEE TABLE BELOW)

The first recent regulatory change in data integrity we will discuss came from the United Kingdom (UK). In December 2013, via a posting on their website, the UK's Medicines and Healthcare products Regulatory Agency (MHRA) stated that beginning in 2014, inspections would check that regulated users were ensuring data integrity through self-inspections or internal audits (8). The requirement for internal audits is covered in chapter 9 of the *EU GMP Guide* (9). The full text of the MHRA posting is presented in Table I. I split the text into four sections, and my comments are in the right column next to each section.

Now, let's recross the Atlantic Ocean to see what has happened with our friends at the FDA.

FDA Level 2 Guidance for Data Integrity

FDA guidance comes in two flavors: Level 1 and Level 2. Level 1 guidance is published in the "Guidance for Industry" documents that go through a draft stage for industry comments and then (eventually) are released as final versions. Level 2 guidance is posted directly on the FDA website, and there is no period for industry comment. In my "Focus on Quality" column on complete data (3), I mentioned the FDA Level 2 guidance, item 3 which discussed paper versus electronic records where the FDA stated that electronic records were the raw data and can never be paper printouts from a computerized system (10).

In August 2014, this area guidance was updated with the addition of three new items, of which we focus on items 5 and 7 because they are relevant to laboratories and concern data integrity. The two points deal with user identities for computerized systems and the use of test samples as system suitability testing (SST) samples (10). This Level 2 guidance takes the form of a question and answer session, as explained more below.

Question 5: Shared Login Accounts

The question posed by the agency is "Why is FDA concerned with the use of shared login accounts for computer systems?" This noncompliance has occurred in a number of warning letters. The answer given by the FDA is:

Appropriate controls must be exercised to assure that changes to computerized master production or control records or other records, or input of laboratory data into computerized records, are only made by authorized personnel and there must be documentation controls that ensure that actions are attributable to a specific individual (§211.68(b), §211.188(b)(11), §211.194(a)(7) and (8).

This section of the answer is merely stating what needs to happen when you use a laboratory computerized system. Access must be limited to authorized individuals as required by §211.68(b) and that the tester and the reviewer need to be uniquely identified to comply with §211.194(a)(7) and (8) for signing test results as either the tester or reviewer, respectively.

When login credentials are shared and a specific individual cannot be identified through the login, this would not conform to the [Current Good Manufacturing Practices] cGMP requirements in 21 *CFR* 211. FDA requires systems controls, including documentation control, to be designed to meet cGMPs (§211.100).

Failing to attribute an action or activity to a specific individual is a major cause of noncompliance, especially when a computer is involved, as Ohm Laboratories (11) and Concord Laboratories (12) amongst other worthy companies have found out when they received FDA warning letters. One possible cause of sharing user accounts is to save money on software licenses; this can be a false economy as the cost of noncompliance (that is, fixing the issues as well as getting back into compliance) far outweighs the cost of the licenses in the first place.

Question 7: Using Actual Samples for Performing System Suitability

This is a more interesting question and arises from many noncompliances involving chromatography data systems when inspectors have looked underneath the hood and found some interesting analytical business practices. Actual samples were used to check to see if the batch was going to be within specification, but were either ignored or deleted when it came to reporting the batch analysis. In essence, this was falsification of data and also failed the complete data requirement of GMP (2).

You may think this is aimed solely at CDS users and, therefore, spectroscopists can sit back and relax. Not so. The fact that spectroscopy is not mentioned does not mean that the same practices do not happen, it's just that CDS are used more widely and have more users than spectroscopy. Don't feel left out — your turn will come! In one warning letter, one company that failed to protect their Fourier transform infrared (FT-IR) spectroscopy system had no restrictions to access data and it was not backed up (13).

The question posed by the FDA is as follows: In warning letters to firms, why has FDA objected to the practice of using actual samples to perform system suitability testing (sometimes also referred to as "trial," "test," or "prep" runs)? This was their response: "FDA wants to discourage the practice of 'testing into compliance.' In some situations, the use of actual samples to perform system suitability testing can be a means of testing into compliance. (See the guidance for industry Investigating Out-of-Specification Results.)"

The practice of injecting the actual samples before committing the whole run was to see if the results were within specification or not. If the result was good, the whole run was analyzed but the original test injection was forgotten, deleted, or filed in a different directory than the actual samples. The major issue here is that this practice fails the complete data (2,3) as the "test" is not evaluated or reported.

According to the United States Pharmacopeia (USP), system suitability tests should include replicate injections of a standard preparation or other standard solutions to determine if requirements for precision are met (16). System suitability tests, including the identity of the preparation being injected and the rational for its selection, should be performed according to the firm's established written procedures and the approved application or applicable compendial monograph (§211.160).

Thus, if an actual sample is being used for system suitability, it should be a properly characterized secondary standard and written procedures should be established and followed (§211.160 and 211.165) (2). All data should be included in the data set that is retained and subject to review unless there is documented scientific justification for its exclusion.

My personal view is that if you are going to evaluate if a spectrometry system is ready for analysis you need to use an independently prepared system evaluation standard specifically for this purpose. This is the spectroscopic equivalent of a system suitability test or point of use test that ensures that a spectroscopic system is ready to undertake an analysis — it is a holistic test that demonstrates that all components of the system are functioning correctly and give the expected results. The evaluation standard should be prepared from a known reference standard that is either an in-house or traceable standard and is only used to evaluate if the system can be used for a qualitative or quantitative analysis. The standard can be solid, semisolid, or liquid depending on the sample type for analysis. However, what is important to remember is "complete data" (2), the results of the system evaluation need to be reported along with the samples analyzed.

10 Compliance Commandments for Laboratory Computerized Systems

Although the focus of this column has been data integrity, I developed 10 compliance commandments for laboratory computerized systems based on the analysis of a number of warning letters in which fraud and falsification were discovered by regulatory agencies. It would be remiss of me if I did not use this opportunity to present the way that spectroscopic systems should be used and the controls that need to be in place to ensure that the data integrity of the electronic records generated and the results interpreted by spectroscopists are trustworthy and reliable. Therefore, based on this review of warning letters and noncompliances, I drew up the 10 compliance requirements that are presented in Table II. Because these are relatively self-explanatory, I will not discuss them any further in the text.

Table II: The 10 compliance requirements for computerized laboratory systems (SEE TABLE BELOW)

Summary

Data integrity is a crucial cornerstone for producing reliable and trustworthy reportable results. This column installment analyzed some FDA warning letters involving data falsification and drew up 10 compliance commandments for laboratory computerized systems to help ensure data integrity.

References

(1) US Food and Drug Administration, *Glossary of Computer Systems Software Development Terminology* (FDA, Rockville, Maryland, 1995).

(2) Current Good Manufacturing Practice for Finished Pharmaceutical Products, 21 *CFR* clause 211 (U.S. Government Printing Office, Washington, DC, 2008).

(3) *IEEE Standard Glossary of Software Engineering Terminology*, 610 (2002).

(4) R.D. McDowall, *Spectroscopy* **28**(4), 18–25 (2013).

(5) Able Laboratories, FDA Form 483 Observations, July 2005.

(6) Compliance Program Guide (CPG) 7346.832 Pre-Approval Inspections, published May 2010, effective May 2012.

(7) R.D. McDowall, *LCGC Europe* **27**(9), 486–492 (2014).

(8) MHRA Self Inspections for data integrity, http://www.mhra.gov.uk/Howweregulate/Medicines/Inspectionandstandards/GoodManufacturingPractice/News/CON3554906/.

(9) European Commission Health and Consumers Directorate-General, *EudraLex: The Rules Governing Medicinal Products in the European Union. Volume 4, Good Manufacturing Practice Medicinal Products for Human and Veterinary Use* (Brussels, Belgium, 2001) chapter 9.

(10) US Food and Drug Administration, *Level 2 GMP Guidance*, http://www.fda.gov/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/ucm124787.htm (FDA, Rockville, Maryland).

(11) Ohm Laboratories, FDA Warning letter, December 2009.

(12) Concord Laboratories, FDA Warning Letter, July 2006.

(13) Posh Chemicals, FDA Warning Letter, August 2014.

(14) US Food and Drug Administration, *Guidance for Industry, Part 11 Scope and Application* (FDA, Rockville, Maryland, 2003)

(15) EU GMP Chapter 4, Documentation, 2011

(16) United States Pharmacopeia General Chapter <621> "Chromatography" (United States Pharmacopeial Convention, Rockville, Maryland).

R.D. McDowall

R.D. McDowall is the Principal of McDowall Consulting and the director of R.D. McDowall Limited, and the editor of the "Questions of Quality" column for *LCGC Europe*, *Spectroscopy*'s sister magazine. Direct correspondence to: spectroscopyedit@advanstar.com

Table I MHRA Expectation for Data-Integrity Focused Internal Audits

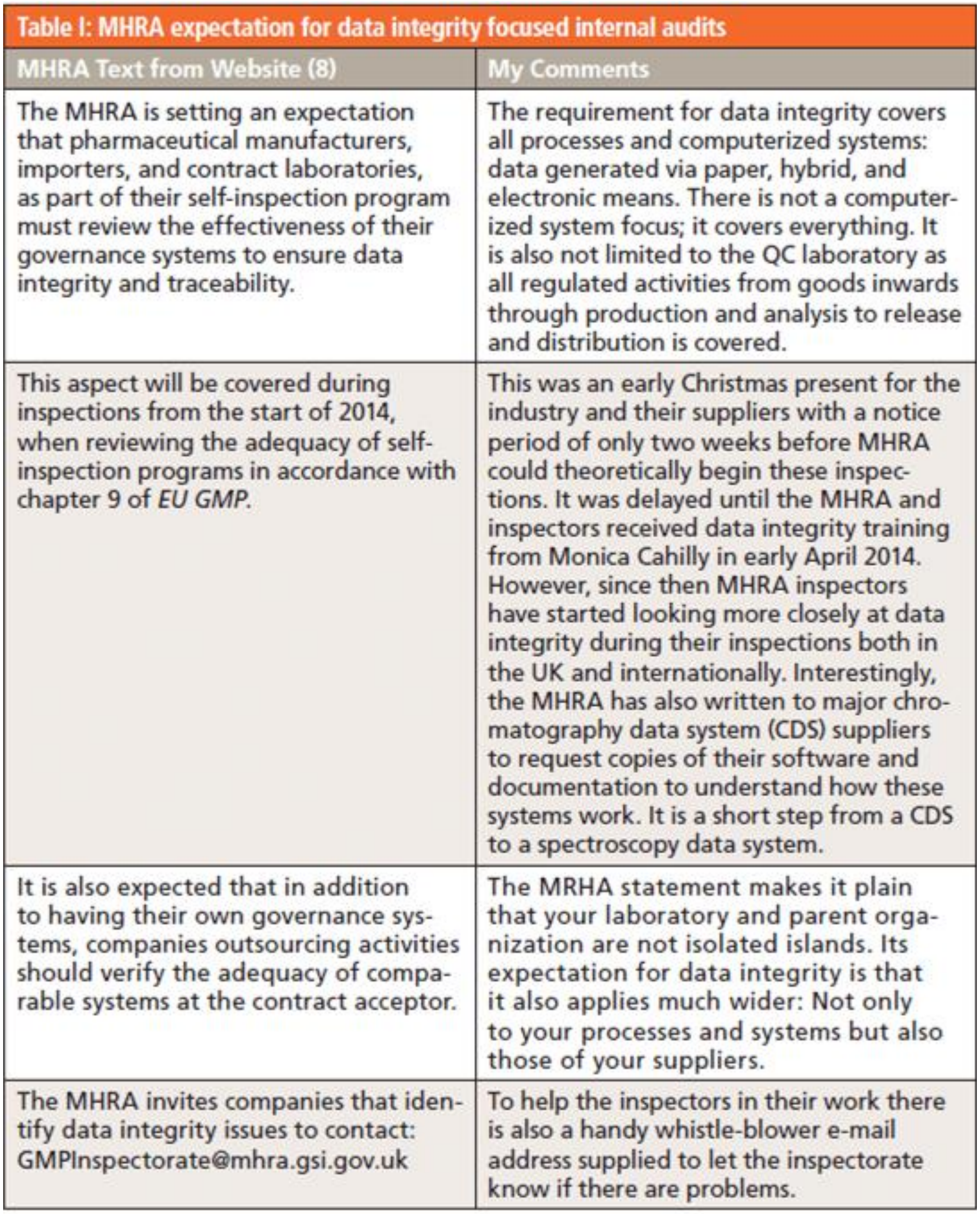


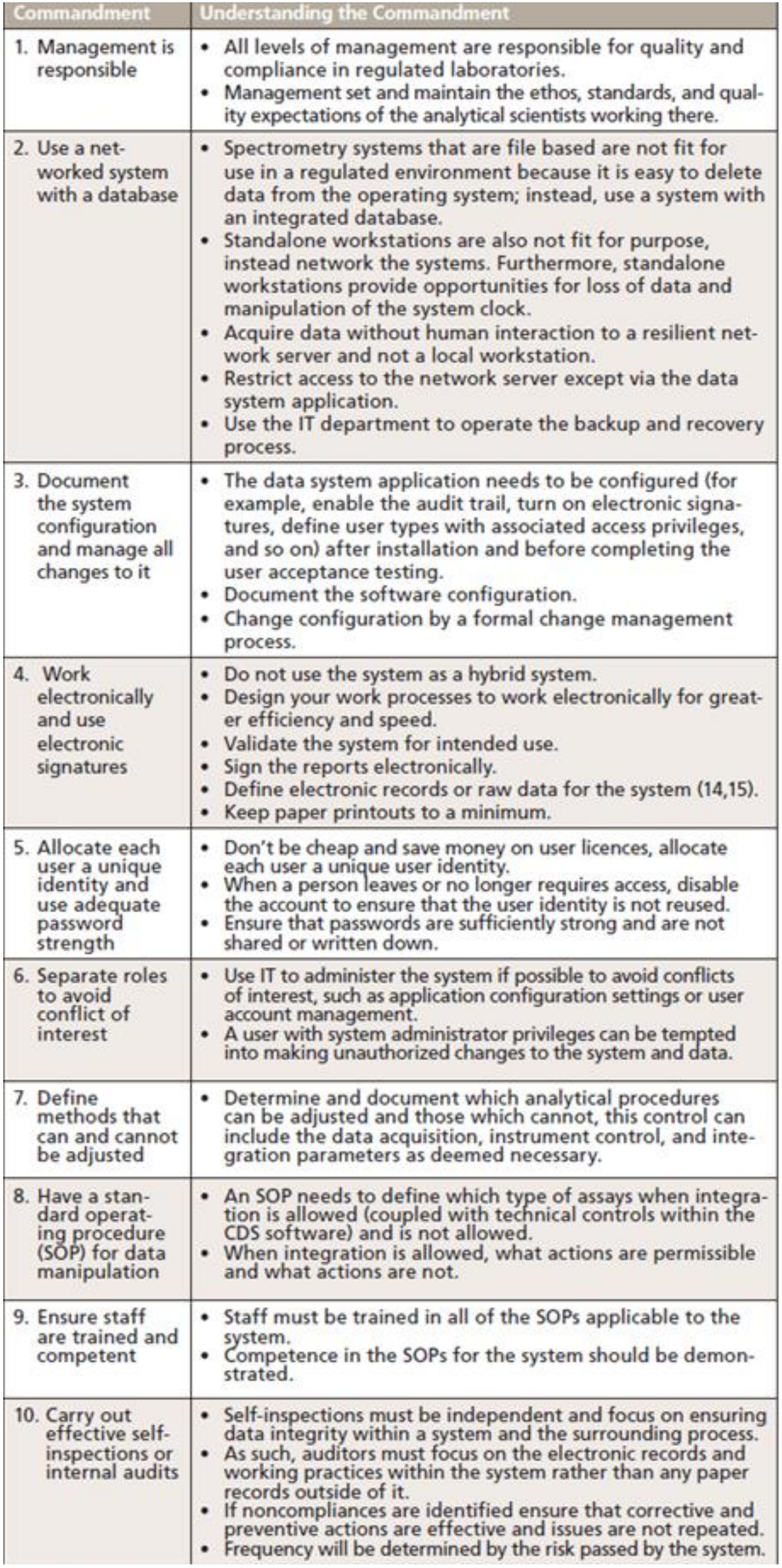
Table I: MHRA expectation for data integrity focused internal audits

MHRA Text from Website (8)	My Comments
The MHRA is setting an expectation that pharmaceutical manufacturers, importers, and contract laboratories, as part of their self-inspection program must review the effectiveness of their governance systems to ensure data integrity and traceability.	The requirement for data integrity covers all processes and computerized systems: data generated via paper, hybrid, and electronic means. There is not a computerized system focus; it covers everything. It is also not limited to the QC laboratory as all regulated activities from goods inwards through production and analysis to release and distribution is covered.
This aspect will be covered during inspections from the start of 2014, when reviewing the adequacy of self-inspection programs in accordance with chapter 9 of *EU GMP*.	This was an early Christmas present for the industry and their suppliers with a notice period of only two weeks before MHRA could theoretically begin these inspections. It was delayed until the MHRA and inspectors received data integrity training from Monica Cahilly in early April 2014. However, since then MHRA inspectors have started looking more closely at data integrity during their inspections both in the UK and internationally. Interestingly, the MHRA has also written to major chromatography data system (CDS) suppliers to request copies of their software and documentation to understand how these systems work. It is a short step from a CDS to a spectroscopy data system.
It is also expected that in addition to having their own governance systems, companies outsourcing activities should verify the adequacy of comparable systems at the contract acceptor.	The MRHA statement makes it plain that your laboratory and parent organization are not isolated islands. Its expectation for data integrity is that it also applies much wider: Not only to your processes and systems but also those of your suppliers.
The MHRA invites companies that identify data integrity issues to contact: GMPInspectorate@mhra.gsi.gov.uk	To help the inspectors in their work there is also a handy whistle-blower e-mail address supplied to let the inspectorate know if there are problems.

Table I: MHRA expectation for data integrity focused internal audits

Table II

The 10 Compliance Requirements for Computerized Systems



Commandment	Understanding the Commandment
1. Management is responsible	• All levels of management are responsible for quality and compliance in regulated laboratories. • Management set and maintain the ethos, standards, and quality expectations of the analytical scientists working there.
2. Use a networked system with a database	• Spectrometry systems that are file based are not fit for use in a regulated environment because it is easy to delete data from the operating system; instead, use a system with an integrated database. • Standalone workstations are also not fit for purpose, instead network the systems. Furthermore, standalone workstations provide opportunities for loss of data and manipulation of the system clock. • Acquire data without human interaction to a resilient network server and not a local workstation. • Restrict access to the network server except via the data system application. • Use the IT department to operate the backup and recovery process.
3. Document the system configuration and manage all changes to it	• The data system application needs to be configured (for example, enable the audit trail, turn on electronic signatures, define user types with associated access privileges, and so on) after installation and before completing the user acceptance testing. • Document the software configuration. • Change configuration by a formal change management process.
4. Work electronically and use electronic signatures	• Do not use the system as a hybrid system. • Design your work processes to work electronically for greater efficiency and speed. • Validate the system for intended use. • Sign the reports electronically. • Define electronic records or raw data for the system (14,15). • Keep paper printouts to a minimum.
5. Allocate each user a unique identity and use adequate password strength	• Don't be cheap and save money on user licences, allocate each user a unique user identity. • When a person leaves or no longer requires access, disable the account to ensure that the user identity is not reused. • Ensure that passwords are sufficiently strong and are not shared or written down.
6. Separate roles to avoid conflict of interest	• Use IT to administer the system if possible to avoid conflicts of interest, such as application configuration settings or user account management. • A user with system administrator privileges can be tempted into making unauthorized changes to the system and data.
7. Define methods that can and cannot be adjusted	• Determine and document which analytical procedures can be adjusted and those which cannot, this control can include the data acquisition, instrument control, and integration parameters as deemed necessary.
8. Have a standard operating procedure (SOP) for data manipulation	• An SOP needs to define which type of assays when integration is allowed (coupled with technical controls within the CDS software) and is not allowed. • When integration is allowed, what actions are permissible and what actions are not.
9. Ensure staff are trained and competent	• Staff must be trained in all of the SOPs applicable to the system. • Competence in the SOPs for the system should be demonstrated.
10. Carry out effective self-inspections or internal audits	• Self-inspections must be independent and focus on ensuring data integrity within a system and the surrounding process. • As such, auditors must focus on the electronic records and working practices within the system rather than any paper records outside of it. • If noncompliances are identified ensure that corrective and preventive actions are effective and issues are not repeated. • Frequency will be determined by the risk passed by the system.