Published on *IVT Network* (http://www.ivtnetwork.com)

Conducting Data Integrity Self Inspections by Quality Assurance

Image not found file:///var/www/ivtnetwork.com/current/sites/default/files/imagecache/author_thumb/LinkedIn-format-better-contrast%5B1%5D.jpg

By **Siegfried Schmitt**

Nov 21, 2017 8:00 am PST

Introduction

The subject of data integrity (DI) has received much attention in recent years, not least because of the increased number of regulatory inspection reports citing data integrity violations. This has caused the regulators to issue new or updated guidance on the requirements and expectations with regards to achieving and demonstrating compliance in respect to data integrity [for instance, the FDA's Guidance entitled "Data Integrity and Compliance With CGMP"]. Amongst the activities a regulated pharmaceutical company has to perform for assuring compliance is for the Quality Assurance (QA) function to perform self inspections (also referred to as internal audits or internal inspections) [e.g. EudraLex Vol 4 Part I Chapter 9 Self Inspection]. It is obvious that these self inspection programs need to include DI in their scope. This paper describes possible approaches, procedural considerations and frequently asked questions in the context of these self inspections, specifically performed by the QA function.

The Pharmaceutical Quality System (PQS)

Essentially, activities performed to assure compliance with the applicable regulations, including quality assurance, must be defined and described within the PQS. PQS is the term used in the ICH Q10 guidance [www.ich.org], whereas many companies may use the term Quality Management System (QMS). The PQS needs to detail first and foremost the role and the responsibilities, i.e. the purpose of the Quality Assurance function. This is particularly important as the regulations do not provide an easy to understand description [S. Schmitt, "The Role of the Quality Unit," Pharmaceutical Technology 41 (9) 2017]. QA establishes and owns the PQS and can be regarded as the legislative authority within the pharmaceutical company. In comparison, the other departments, including Quality Control (QC) can be considered the executive.

Thus, QA has to assure that a PQS is in place and that it is suitable for the specific circumstances of the pharmaceutical operations. Furthermore, QA needs to verify through suitable means, such as quality metrics or self inspections, that the PQS is being followed, i.e. adhered to.

DI Self Inspections

As with all audit programs, this requires to have a process description in place, which is generally in the form of a Standard Operating Procedure (SOP), including any associated instructions and forms. Companies should have an established SOP in place and now need to review it with regards to DI. Here now some specific examples that describe what QA should look for and how they could perform the self inspection.

Backward Traceability Example

QA should randomly pick a Certificate of Analysis (CoA) as the starting point. Working backwards, the auditors should be able to trace back to the raw data. This is best demonstrated by a practical example:

Record	pH 6.8 with specifications 6.5 to 7.0 for sample A123Z

Supporting Record or Data	The analytical record for this sample contains this information: - Date and time of the measurement - Name of the analyst - ID of the instrument - The pH value of 6.78 - The reviewer’s signature - The specification range 6.5 to 7.0
Self-inspection activity	Verification that: - this was a working day - there is documented evidence that the analyst and the reviewer were working that day - the analyst was trained to perform the analysis - the reviewer was authorised to review - the instrument logbook shows the instrument was available that day and time - the instrument was within calibration - the instrument printout confirms date, time, value, instrument ID - the instrument printout is initialled by the analyst across the printout and the laboratory record page - the colour of the printer ink is the same as other printouts from that day - the sample logbook in the laboratory details the sample ID - the sample logbook in the plant details the sample ID - the sample collection time is before the sample analysis time - the signatures and initials on the records conform to the master signatures list

As this relatively simple example shows, finding the supportive evidence often requires the assistance of other departments, such as engineering, IT, or human resources. Also, information may be available in different formats (e.g. paper, electronic or digital (e.g. video)) and this information may be located on different systems and in various locations. Therefore, such an exercise requires time and effort, and obviously can only be performed on a case by case basis, but not as a routine undertaking. This example is for just one reported value from the CoA, so tracing back all reported values to the raw data can be quite an extensive activity, taking several days to complete.

General Aspects

The QA auditors may also want to observe the behaviour of those audited: do they behave in a reasonable manner or do they stall the self inspection? Do they provide the required documentation and information in a timely manner? Do they answer questions or is their behaviour evasive? Are the documents provided complete? Is staff who performed the activity answering or is one person answering on others' behalf?

Can the data (e.g. from the laboratory instrument) be verified from the backup data on a secure drive? If data was wilfully modified or deleted, could that be proven by analysing information stored on other systems (paper and/or electronic)? How difficult would be such a manipulation, e.g. would it require several persons to collude or the falsification of more than one document? Is there any incentive for data falsification/adulteration?

Audit Trail Reviews

Of interest to QA is first and foremost whether the system should have an audit trail, a fact which must be described in the User Requirements Specification (URS). This and other application validation documents need to describe the technical specifications for the audit trail, such as format (e.g. human readable form), search functionality, what the audit trail is supposed to capture (e.g., the system configuration, the analytical method), etc. Thus, QA verifies first what the audit trail is supposed to do before investigating whether the audit trail meets the requirements. As QA auditors are not normally subject matter experts in a particular application, it is unreasonable to expect QA to understand the contents of the audit trail information, or the technical details associated with the audit trail configuration. Instead, QA can verify if the process for identifying the audit trail requirements and their implementation has been followed.

Alleged DI Breaches Reporting and Investigation Process

As companies must have a defined process for reporting alleged Data Integrity breaches, QA should verify that such reporting channels exist (e.g. anonymous mailbox, or confidential phone line). Furthermore, there has to be an investigation process that allows for an unbiased, independent and expeditious investigation. The QA audit will focus on whether the process has been duly followed and that the findings were reported as per the instructions.

It is quite possible that self inspections of this particular process may have to be repeated more frequently than just annually or bi-annually, e.g. after reorganisations, or staff complaints relating to such investigations.

Summary

Data Integrity has to be embedded in the self inspection processes, which in many companies is still in the implementation stages, rather than an established routine. Lack of experience with the process can lead to an overzealous or unfocussed approach, which could impact the effectiveness of the self inspection process. The Quality Assurance function should lead by example and revise their existing self inspection program and associated documentation as early as possible. From the above discussions it is clear that QA's remit is limited and that only the entirety of all self-inspection activities by each and every department involved in data integrity assurance will provide a full picture of the company's state of compliance with data integrity rules and regulations. Non-compliance is not an option.
