Agaram
TECHNOLOGIES

Data Integrity Introduction, Challenges and Solution

White Paper
Part - 1

by
Galit Lisaey

Gal.IT Data Integrity Consulting

Oct - 2020

Introduction

The importance of maintaining the quality and reliability of the data (Data Integrity) submitted to the authorities, especially in the field of pharmaceuticals, has become a binding requirement. As part of the global transition to computerized, automated systems and software in the past thirty years, and in order to ensure that critical electronic data presented to the authorities as a basis for decision-making are accurate and reliable, some methodical official guideline documents have been published by the health authorities.

A compliance document of the US Food and Drug Authority (FDA) namely **21 CFR Part 11** was published in the late 1990s. It was followed by other documents such as EU Annex 11 by the European Authorities, as well as similar documents for the Canadian, Australian and other International Health Authorities.

The authorities consider violations of these principles severely, and a reference for that can be found in the FDA's warning letters.

"The lack of control over the integrity of your data raises questions about the authenticity and reliability of your analytical data and the quality of your drug products."

As part of the regular review, the purpose of the authorities is not only to identify problems and serve as gatekeepers, but also to help the companies to improve. In recent years, clarification documents have been published attempting to find the right ways to facilitate learning and understanding.

One way is to bind the requirements under the acronym ALCOA+, in which each letter represents a set of regulatory requirements. These requirements are obligatory; however, it is not always easy and obvious to do so. The purpose of this acronym is to allow international alignment, addressing discourse and harmonization in order to enable effective assimilation of the regulatory requirements.

“ALCOA+” stands for:

Attributable:

Do records include who acquired the data, the nature of the actions, and the time of action?

Legible:

Is the data always clear and easy to read and to use by everyone at any time?

Contemporaneous:

Was the data recorded in real-time?

Original:

Was the raw data well defined and kept free of modification?

Accurate:

Is the data error free, correct and have all changes been updated?

Plus (+):

Consistent, Available, Enduring, Complete

This article discusses the challenges and some of the suggested solutions related to the requirements package related to: “Attributable”.

One of the elaborated descriptions of ‘Attributable’ can be found in a document published by PIC/S. *“It should be possible to identify the individual or computerised system that performed the recorded task. The need to document who performed the task / function, is in part to demonstrate* *that the function was performed by trained and qualified personnel. This applies to changes made to records as well: corrections, deletions, changes, etc."*

Attributable

'Attributable' can be referred to as the "Data ID" - all relative information - and it relates also to topics concerning the metadata, which is a set of data describing other data. In other words, data about the data.

In order to make sure the data is attributable, one must be able to answer a few questions, for example:

Do records include who acquired the data, the nature of the actions, and the time of action?

This article we will focus on the challenge of user and password management from two different aspects.

- Managing metadata using paper or in case where legacy techniques are involved, does not ensure an appropriate identification record.
- Qualification training where it is not sure when to identified a specific user name for the trainee.

In both aspects the main question is "how can one be sure they know who conducted the work?" The solution in this case lies in the control based on risk assessment.

"Your assessment should include analyses of the risks to patients caused by the release of drugs affected by a lapse of data integrity and analyses of the risks posed by ongoing operations." (FDA, Warning letters - https://bit.ly/3i5aj1W)

Paperwork and Legacy instruments

In cases of Paperwork and Legacy instruments, the identifying the operation, the execution date and time, as well as other defined properties are part of the challenge. The same controlled solution can apply in both cases.

The control process must ensure that the information is comprehensive and accurate and appropriately translated into work procedures.

A variety of control processes can be implemented depending on the work environment.

For example:

Option 1: A full documented review of a paper form could be performed by two employees parallelly, so that one is the operator and the other one is the reviewer. This option may cause a “bottle neck” in the completion of multiple tasks.

Option 2: Work with a pre-defined reviewed control document, downloaded from a computerized system such as SDMS (Scientific Data Management System). The same system should enable the uploading of the updated documents as well. It is advisable to use a validated computerized system that is managed in accordance with the requirements to record the user ID, date, time and other required properties. This type of process is called a hybrid process. This way it is possible to document the activity time and other properties adapted to the working method.
The advantage in such a case is that the review of the data can be carried out within a time frame defined in the work procedures and is not required to be carried out during the procured conduct.

Furthermore, the SDMS system can monitor full activities in a local folder to ensure a thorough review. Even with modern devices, it is sometimes impossible to work properly with a username (aimed to ensure employee identification) for various reasons. Some are related to local technical limitations, others could be related to restrictions on usage, etc. In such cases using SDMS could be a relevant solution, based on controlled configurations.

Qualification training

Another related challenge can come up when the organization is implementing a qualification training for new users (https://bit.ly/3mYbNP7, https://bit.ly/342VJCY).

Typically, an employee qualification process includes theoretical training, observing a qualified employee, performing under supervision and self-performance. The challenge faced by the organization is related to the point when to issue a new username and password which will enable verifying that the data was indeed carried out by the employee during the training phase. In some systems, issuing of the username and password means giving permission to the system even before the employee is qualified, which may result in a “chicken and egg situation”. This also has various solutions, and systems that allow qualification management in an orderly manner making it possible to conduct tutorials for very specific systems or store information in a specific folder designated for the trainee.

If you are interested in hearing more about the issue and debating appropriate solutions, the team of Agaram technology and myself will be happy to answer your questions.

In the next part of the Whitepaper, we will discuss the term: “Legible”

About Author

Galit Lisaey established Gal.IT Data Integrity Consulting to assist organizations with customized solutions for implementing Data Integrity processes, including risk-based computer system validation management. She has a MSc in Animal Studies from the Hebrew University of Jerusalem and 20 years of experience in regulatory environments. Running Facebook community on Data Integrity for professionals as well as individuals, based on reliable data from daily life decision making experience in regulatory environment.

Galit can be reached at galit.lisaey@dintegrity.net