# A Solution for Pharmaceutical and Life Sciences Industry

## Important to Know About Data Integrity

*by Dr Marco Kleine, Head of Informatics Group, Shimadzu Europa GmbH, 47269 Duisburg, Germany, makl@shimadzu.eu*

**To ensure data integrity in laboratories in the pharmaceutical or life sciences industry, it is necessary to talk about procedural, behavioural and technical controls. While regulated companies are responsible for data integrity within their organisations, both laboratory instruments and their data management suppliers must assure that all aspects of compliance like fulfilling the ALCOA+ principle are addressed. It must be comprehensible at all times who did what and why.**

This article outlines the controls needed to achieve data integrity in the laboratory, and provides an overview of the procedural and behavioural issues that must be considered. It also explains how the responsibilities for technical compliance with regulatory data integrity requirements can be met using Shimadzu's LabSolutions CS analysis data management system.

### Current regulatory position (regulatory concerns, inspections, common findings and enforcement actions)

In the 1980s and 1990s, data integrity had already been an issue for regulatory authorities. However, the primary focus was on the integrity of data in automated process and equipment control systems, many of which were custom designed or customised. In the mid- to late 1990s, the focus shifted to the use of electronic signatures in the industry, leading the U.S. FDA to publish US 21CFR Part 11, Electronic Records, Electronic Signatures. Confusion over the scope and enforcement of 21CFR Part 11 shifted the focus away from a broader consideration of data integrity concerns.

Data integrity is currently the focus of attention in the pharmaceutical and wider life sciences industries. To respond appropriately to recent regulatory guidance [1] on data integrity, it is important that regulated companies put recent enforcement actions in proper context and do not over-react to the fear, uncertainty and doubt which is generated in some quarters.

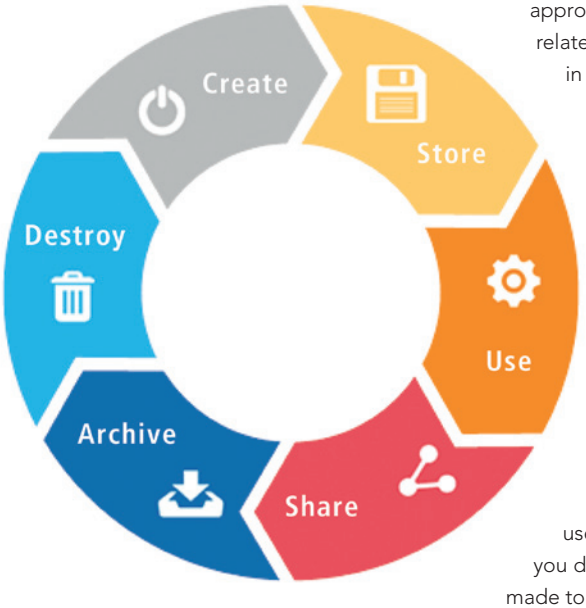


*Figure 1: The Data Lifecycle model.*

### US FDA Warning Letter excerpts

- "Your firm has failed to exercise appropriate controls over computer or related systems to assure that changes in master production and control records, or other records, are instituted only by authorised personnel."
- "Your firm did not put in place requirements for appropriate usernames and passwords to allow appropriate control over data collected by your firm's computerised systems including UV, IR,HPLC, and GC instruments. All employees in your firm used the same username and password. In addition, you did not document the changes made to the software or data stored by the instrument."
- "Your firm had no system in place to ensure appropriate backup of electronic raw data and no standard procedure for naming and saving data for retrieval at a later date."
- "You have not implemented security control of laboratory electronic data. All laboratory analysts share the same password for the HPLCs in the QC analytical chemistry lab. In addition, analysts have access to the HPLCs which allow them to create and/or modify validated methods."
- "Your firm deleted multiple HPLC data files acquired in 2013 allegedly to clear up hard drive space without creating back ups. Your QC management confirmed that there is no audit trail or other traceability in the operating system to document the deletion activity. Furthermore, your analysts do not have unique usernames and passwords for the computer and laboratory information systems; your QC analysts use a single shared user identifier and password to access and manipulate multiple stand-alone systems."
- "The inspection of your facility documented multiple incidents of performing "trial" testing of samples, disregarding test results, and reporting only those results from additional tests conducted."
- "Your firm failed to have adequate procedures for the use of computerised systems in the quality control (QC) laboratory. Our inspection team found that current computer users in the laboratory were able to delete data from analyses. Notably, we also found

that the audit trail function for the gas chromatograph (GC) and the X-Ray Diffraction (XRD) systems was disabled at the time of the inspection. Therefore, your firm lacks records for the acquisition, or modification, of laboratory data."

- "Multiple analysts, testing multiple drugs, deleted unknown peaks without justification. These manipulations made the drugs appear to meet their specifications. Of concern, one of these unknown peaks was for a residual solvent known to be a genotoxic impurity."

### Key principles of data integrity with respect to laboratory systems

While organisational and cultural issues must be addressed, customers should also ensure that appropriate technical controls are established to assure data integrity and meet the electronic records and signature requirements. In the laboratory, this needs instruments and systems capable of complying with current data integrity expectations and, more importantly, equipment must be configured in a way to enforce data integrity controls. As described below, analysis data management software (e.g. Shimadzu's LabSolutions CS) provides comprehensive functionality to serve these demands.

In addition, other, broader aspects of technical compliance must also be considered; these are summarised below.

### Instrument Qualification

The qualification of laboratory instruments is usually achieved through Installation Qualification (IQ) and Operational Qualification (OQ). They ensure that the instrument is installed and set up correctly, and performs according to the vendors' published specifications. This process utilises IQ and OQ scripts or protocols normally provided by the vendor. These may either be executed by the regulated company or a qualified third-party.

With respect to data integrity, it is essential that these scripts verify that the instrument's configuration leverages the built-in data integrity features and controls, and that they cannot be disabled in everyday use.

### IT Infrastructure qualification, including system backup and data archiving

Besides the laboratory instruments qualification, any supporting IT infrastructure should also be qualified. This covers any data management systems or LIMS, including physical or virtual servers, network storage, and any active or passive network components such as bridges and switches and structured cabling of the local area network (physical or virtual LAN). The same is true for wide area networks (WANs) which connect remote locations with central systems.

### General information security controls

A great deal of electronic records and data integrity compliance is based on effective information security controls. While simply implementing them will not be sufficient to meet regulatory expectations, they do form a sound base upon which other electronic records and data integrity compliance can be built.

While formal registration to a standard such as ISO 27001 [2] is not essential, implementing applicable controls from this standard (and more than a dozen related standards) can help regulated companies ensure that they have adequate, risk-based controls in place to ensure the basic security of records and data. As this will not prevent fraudulent data from being entered, implementing basic information security controls will help addressing data integrity issues such as accidental deletion, lack of availability, corruption etc.

### Compliant laboratory data management

While general IT controls must be set up, LabSolutions CS provides comprehensive functionality to assure data integrity. The broad nature of these controls makes it quick and easy to establish a compliant data management environment, whether working with a small number of instruments in a single laboratory or multiple systems across many labs.

This includes the ability to:

- manage additional, non-analytical instruments in a compliant manner (e.g. balances / weighing scales)

- capture additional laboratory data in a compliant and integrated way

- integrate common third-party instruments from multiple vendors into a single compliant data management environment.

LabSolutions CS provides several features and functions supporting compliance with data integrity and electronic records/ electronic signatures. These general features are described below, and specific features are mapped to requirements of 21CFR Part 11 (Electronic Records, Electronic Signatures), EU Eudralex 4 Annex 11 / PIC/S PI001-3 Computerised Systems and data integrity ALCOA+.

### Software and analytical methods validation

In addition to qualifying the instrument and IT infrastructure, the software of the instrument or data management system software should be adequately validated. This can leverage the vendor activities and documentation to reduce the scope of such validation, but regulated companies are responsible for ensuring that the software is able to meet their specific requirements reliably and repeatably.

While the basic operation of an instrument can be verified during OQ, user-specific requirements are usually validated as part of Performance Qualification (PQ). This verifies that the software is capable of meeting the particular needs of the regulated company when using a validated analytical method in the context of a defined set of laboratory processes (sequence).

In most cases, IQ and OQ are performed, and the software associated with a particular instrument and data management system are validated in detail. Once this is done, the analytical methods are validated to prove that instrument and software are capable of repeatedly delivering expected results following a defined sequence of events and analytical techniques. Such protocols can be recorded in the LabSolutions CS database and prove clear evidence that the analytical methods have been properly validated.

### Key data integrity features

To ensure data integrity, it is important that laboratory instruments and data processing systems have the features and functions to support data integrity expectations. While this may seem obvious and basic, these features are not always available on instruments and in software from vendors that do not specialise in the life sciences market.

In other cases, only newer versions of equipment and software support these features. It may then be necessary for regulated companies to replace instruments and/or upgrade software to ensure compliance with data integrity expectations.

It is worth noting, however, that based upon a well-documented data lifecycle model and risk assessment, it may be possible to establish effective procedural controls on an interim basis that allow investments in replacements or upgrades to be planned and prioritised based on risk.

*Figure 2: Probably the most important points today – data integrity and data security*

In addition to basic information security controls, the following features are key to understand and effectively implement. Wherever they are available, they must be configured and reviewed following an effective IQ process.

**User access permissions**

As described above, it is important that the rights and permissions of users and system administrators are segregated to eliminate conflicts of interest regarding the authority of any single person

This requires that instruments and systems are able to define and enforce permissions for specific user groups, i.e., users, supervisors, quality assurers etc. Individuals should be assigned to user groups with predefined permissions, and checks should be in place to ensure that no single person has a conflict of interest e.g., as a user and System Administrator, or as a supervisor and a QA user.

**Audit trails**

While this is mandatory for electronic records, audit trails should be established for all critical data and metadata. This has to cover instrument raw data which typically must be retained to allow subsequent reprocessing, but should also be extended to critical datasets and files such as

- analytical methods and sequences (both changes to validated analytical methods and changes made to methods or sequences during an analytical run, where permitted)
- report templates
- user groups and permissions
- results data.

Audit trails should capture:

- what kind of data/meta data has been created, changed, or deleted, including the old value(s) and new value(s)
- when the data/meta data was created, changed or deleted
- who created, changed or deleted the data/metadata (traceable to a uniquely and legally identifiable person)
- why the data / metadata has been changed. This may be implicit because of the nature of the operation (i.e. a specific step in an analytical method) or may require the user to enter a reason.

Such audit trails need to be generated automatically, excluding the possibility to be turned off by the users. The same should apply for system administrators, especially for GMP related activities. Such audit trails must be readable by humans and should be retained as long as the record they relate to.

**Record, file locking and signatures**

Not all data is considered as a record (as defined by US 21CFR Part 11 Scope and Application guidance2), but when this is the case, at least partly, additional and specific controls are then required to comply with US 21CFR Part 11 [3].

Based on a documented data life cycle model and risk assessment, it may also be possible to apply such controls to data that are not strictly considered as electronic records. All such records and files should be secured through good information security practices and provided with audit trails.

**Forensic data analysis**

Regulators are increasingly demanding access to databases to analyse datasets. This is to identify any data integrity issues. Examples include checking the date and time stamps of data from different laboratory instruments to confirm that the time stamps reflect the analytical sequence and schedule associated with the approved analytical method.

**Regulatory compliance analysis - Supplier responsibilities**

- develop, supply and support mature products with appropriate technical controls to address all aspects of regulatory compliance
- assure, as far as is practically possible, backward and forward compatibility across different software versions, for the availability and readability of complete laboratory data throughout regulatory retention periods
- provide flexibility in terms of instrument and data management software architecture and hardware support to cover a wide range of solutions, including on-premises installations, use of dedicated physical servers and virtualisation, and use of off-site infrastructure as a service installation
- be open and transparent with customers about potential regulatory issues related to legacy instruments and software, and assist customers in implementing and upgrading appropriate procedural and behavioral controls
- be committed to thoroughly understand the regulatory environment in which the life sciences customers operate
- show commitment to providing product support and upgrades to keep pace with evolving regulatory expectations, including data integrity.

## References

1. UK "'GXP' Data Integrity Guidance and Definitions", March 2018

US FDA "Data Integrity and Compliance with Drug CGMP" Data Integrity and Compliance with Drug CGMP, December 2018

WHO "Guidance on good data and record management practices", Part of Technical Report 996, May 2016

PIC/S draft "Good practices for data management and integrity in regulated GMP/GDP environments", November

2. ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements

3. US Code of Federal Regulations, Chapter 21, Part 11 - Electronic Records; Electronic Signatures