SKILLPAD®
www.skillpadcompliance.com

THE IMPORTANCE OF DATA INTEGRITY IN REGULATED INDUSTRIES

Why do we need to understand Data Integrity ?

Most organizations fail to understand the criticality of satisfying data integrity requirements. This is evident when one considers the increasing number of data integrity-related 483s and warning letters issued by the FDA and other regulatory bodies over the last decade. The direct impact of this misunderstanding is that regulators are not able to rely on the provided data to assure the safety, efficacy and quality of drugs.

From print to digital record formats

Years ago, quality systems and regulated processes were documented mainly on paper records. For example, laboratory notebooks, batch records, and procedures would be paper-based. The FDA defines this record format as 'static' – *a fixed-data record such as a paper record or an electronic image*.[1] With digitization, quality systems and regulated processes have moved from a largely, static, paper-based record system to an electronic-based system that is interactive and dynamic. The FDA defines this record format as 'dynamic' - *record format allows interaction between the user and the record content*.[1]

Whether the record is static or dynamic, however, regulatory data integrity standards still apply.

What is Data Integrity?

Data integrity is the assurance of the accuracy, completeness, and consistency of data over its entire lifecycle and applies to both paper-based and electronic-based systems. Data lifecycle refers to all phases in the life of data, from its initial generation and recording through processing, transformation or migration, use, retention, archiving, retrieval and destruction, as applicable.

Every organization is built around data. This data comes from many different sources – clinical research trials, manufacturing, quality testing, packaging, materials management, procurement, distribution, Quality Management Systems, and so on. If there are doubts about the accuracy and reliability of data, there could also be doubts about the quality, safety, and integrity of marketed products. This is why data integrity is such a critical issue!

When we refer to the integrity of data, this means all data collected and stored must be correct, traceable, reliable, accessible, and retrievable. The FDA states: "Complete, consistent, and accurate data should be [A]ttributable, [L]egible, [C]contemporaneously recorded, [O]riginal or a true copy, and [A]ccurate (ALCOA)."[1] The FDA has expanded ALCOA to ALCOA+ to include four other quality attributes: complete, consistent, enduring and available. These last four attributes account for the "+" in ALCOA+.

What does each element of ALCOA mean?

Attributable: *All data generated or collected must be attributable to the person generating the data. The date the data was generated or collected must also be recorded. This principle also applies to any changes made to generated or collected data. The identity of the individual who generated or collected the data must be recorded. This can be recorded manually by initialing and dating a paper record or by an electronic-based audit trail.*[2]

Legible: *The data recorded must be legible, readable, and permanent.*[2]

Contemporaneous: *A record of an activity (date and time) associated with the data generated or collected must be made at the time it takes place.*[2]

Original: *Original data is also known as source data. "The original record can be described as the first-capture of information, whether recorded on paper (static) or electronically (usually dynamic, …). "*[2]

Accurate: *The data recorded must be free from errors, complete, consistent, truthful, and reflective of the observation.*[2]

Current regulatory guidance

While the topic of data integrity is not new, regulators believe that a new level of data integrity awareness is warranted, given the recent reported increase in data integrity deficiencies and failures.

The increasing trend of these observed data deficiencies (such as those discussed within this paper) made it harder for regulators to determine whether or not drugs had been manufactured, packaged, tested, stored, or distributed in a manner that would assure drug safety and efficacy. As a result, several new guidance documents on data integrity came out in 2018 and 2019 by FDA, PIC/S, WHO, MHRA, and ISPE[1,2,3,4,5] to assist the industry.

The data integrity requirements originally addressed in the FDA's Part 11 of Title 21 of the Code of Federal Regulations; Electronic Records; Electronic Signatures (21 CFR Part 11)[6] and the European Commission's Eudralex Volume 4, Chapter 4 (*Documentation*) & Annex 11 (*Computerised Systems*)[7] remain unchanged at this time.

In this paper, common data integrity issues are highlighted as well as some key recommendations to reduce data integrity risk.

What has been observed?

Incomplete or missing records – examples would include missing data to support results, original records or complete records derived from all tests performed not retained. A warning letter was recently issued under *MARCS-CMS 557890 — March 04, 2019* for the inaccurate reporting test results - "*Your firm failed to ensure that laboratory records included complete data derived from all tests necessary to assure compliance with established specifications and standards (21 CFR 211.194(a))*“.[8]

Access control deficiencies – examples would include the use of shared login accounts for computer systems, inappropriate privilege levels assigned to individuals, or inadequate controls in place to restrict access to the records. It is important that appropriate controls be in place so that only authorized personnel have access to records, associated content, files, and settings. In addition, a listing of all authorized individuals and their associated access privileges is to be documented so that listings can be reconciled with actual practice. A warning letter was recently issued under *MARCS-CMS 588104 - December 05, 2019* for inappropriate privilege levels assigned to individuals - "*Your firm lacked sufficient controls over your gas chromatography (GC) instrument used to test the drug product prior to release. Specifically, your firm assigned administrative privileges to analysts conducting routine assay tests using your Empower chromatography software data system*“.[9]

Deleting or destroying original GMP records – this could apply to both paper-based and electronic-based records for which laboratory notebooks or test records are thrown away or data is deleted on electronic systems. A warning letter was issued under *MARCS-CMS 495920 — December 23, 2016)* for the destruction of CGMP documentation (paper-based) - *"CGMP documentation was discarded without being assessed by your quality unit. Our investigator found torn and shredded equipment maintenance documents, raw material labels, and change control work orders in your scrap yard awaiting incineration. Your staff lacked knowledge of your corporate procedure for the destruction and incineration of documents* “.[10]

Audit trail deficiencies - examples would include computerized systems generating critical data with no audit trail capabilities, disabling of audit trails, and review of audit trails not performed. A warning letter was issued to under *MARCS-CMS 496395 — October 13, 2016)* for the failure to perform a routine audit trail review - "*Your firm failed to exercise appropriate controls over computer or related systems to assure that only authorized personnel institute changes in master production and control records, or other records. (21 CFR 211.68(b))… Your stand-alone computer systems lacked controls, such as routine audit trail review and full data retention, to prevent analysts from deleting data…We acknowledge your commitment to strengthening your procedures to assure user access restrictions and implement audit trails for computerized systems.* “[11]

ALCOA+

With the recent introduction of ALCOA+ by the FDA, the basic concepts of ALCOA have been expanded with an emphasis on data quality. The acronym ALCOA+ stands for ALCOA in addition to the following attributes: *Complete, Consistent, Enduring,* and *Available*.

Complete: No deletion of recorded data or no lost data has taken place since its generation. [2]

Consistent: The data is generated, recorded, dated, and time-stamped chronologically in the expected sequence (traceable). [2]

Enduring: The data must be maintained, intact, and accessible throughout the record retention period. Storage and archiving measures should be taken into consideration to ensure that data and records are maintained in a secure location protected from environmental damage during their retention period. [2]

Available: The data must be readily accessible in human readable form for review throughout the retention period for the record. [2]

Key recommendations to reduce data integrity risk

Audit your Audit Trails

All data generated or collected must be attributable to the person generating the data. Therefore, the creation, modification, and deletion of regulated electronic records must be captured through audit trails. The FDA refers to audit trails as “…those that track creation, modification, or deletion of data (such as processing parameters and results) and those that track actions at the record or system level (such as attempts to access the system or rename or delete a file) “.[1]

The audit trail should include the following parameters: [2]

- *Action*
- *Object*
- *Property/field*
- *Old value*
- *New value*
- *User*
- *Date*
- *Time*

A formal process to examine the audit trail to ensure data integrity is a requirement in the regulated environment. It is not enough just to have the audit trail in place; it needs also to be reviewed, and actions taken accordingly. As per the FDA guideline, “Data Integrity and Compliance with Drug CGMP”, the audit trail review is to be performed by the “personnel responsible for record review under CGMP …. as they review the rest of the record“.[1] In terms of the frequency of the review, the FDA states that it is to follow the frequency as defined in the CGMP regulations. If not applicable, audit trail review is to be defined based on system risk and criticality.[1] The ISPE GAMP Guide: Records & Data Integrity[5] provides guidance on risk-based approaches which may be helpful to establish the process for audit trail review. Overall, the audit trail review process should be based on the complexity of the system and its intended use.

It is important to note that not all data in an audit trail needs to be followed or verified in the audit trail review. A risk management approach should be used to evaluate what data needs to be reviewed. It is also possible that different data is reviewed at different times, depending on criticality.

Data Integrity Policies

Currently, there is no regulatory requirement for a specific data integrity policy. However, a policy which outlines an organisation’s approach to total data governance, including audit trail review in compliance with the requirements of ALCOA/ALOCA+ principles should be implemented and followed. Such a policy would allow upper management to formally enforce data integrity principles. This would likely lead to fewer warning letters and 483s as well.

Personnel should be trained on implementing good data integrity practices and detecting data integrity issues.

Unique usernames and passwords

Access to electronic records must be controlled by a unique login, with username and password. This applies to the creation, modification, or deletion of data. It is important that all actions performed are attributable to a specific individual; therefore, unique user logins are imperative. Moreover, a username should not be reused or reassigned to another person.

The FDA is very concerned with the use of shared login accounts for computer systems - “When login credentials are shared, a unique individual cannot be identified through the login and the system would not conform to the CGMP requirements in parts 211 and 212“[1]. Two-factor authentication is becoming ubiquitous and should be implemented to discourage or prevent the sharing of login credentials.

Best practices for account security should be applied. This includes enforcing strong password policies, automatically logging out users a period of inactivity and locking out users after a certain number of failed password attempts. Alternate approaches including biometrics authentication (e.g., fingerprint, retinal scan) are also starting to be used in the industry as a form of authentication and access control. Since technology exists to enable stronger preventive measures, companies should avail themselves of this if they can.

Separate administrator and user access rights

It is imperative that user roles be delineated. The FDA suggests that the “system administrator role, including any rights to alter files and settings, should be assigned to personnel independent from those responsible for the record content. To assist in controlling access, it is important that manufacturers establish and implement a method for documenting authorized personnel’s access privileges for each CGMP computer system”[1]. Further, they suggest “to assist in controlling access, it is important that manufacturers establish and implement a method for documenting authorized personnel’s access privileges for each CGMP computer system in use (e.g., by maintaining a list of authorized individuals)”[1].

User access controls should enforce the strict segregation of duties and ensure that no conflict of interest between personnel functional roles in the system and access levels granted exist. The "principle of least privilege "or "need to know" basis in relation to granting access levels to personnel should be applied.

In addition, by clearly defining and assigning user roles, each user can have a tailored workflow which ensures actions are attributable to a specific individual.

Data Integrity must remain a priority

In addition to the recommendations proposed in this paper, there are many other practices companies could put in place to ensure their compliance with data integrity requirements. Ongoing training is essential, and this training must be matched to different roles, depending on the role’s involvement with data.

For instance, if applied properly, 21 CFR Part 11 compliant electronic signatures are more effective in preventing the possibility of backdating records. The FDA states “electronic signatures with the appropriate controls can be used instead of handwritten signatures or initials in any CGMP required record“[1]. Before using electronic signatures, ensure controls are in place to identify the person who signs the electronic records and the FDA is notified (21 CFR Part 11.100(c)[6]).

Risk management and data Integrity

Controls over the data lifecycle should be proportional to the level of risk. A risk management approach should be utilised to determine the importance of each data/processing step and should consider data criticality and data risk. Factors to consider include the opportunity for data alteration and deletion, vulnerability of a computerized system to inadvertent or unauthorized modifications to critical configuration settings, and likelihood of detection / visibility of changes by the routine review processes.

Overall, risk management, together with audit trail reviews, should be used on a routine basis to assess possible issues for data integrity.

Professional Resources

Interested in knowing more about data integrity solutions and recommendations?

Contact Skillpad Compliance and our experts will support you with data integrity compliance within your organization.

Conclusion

Data integrity is essential and adherence to ALCOA+ principles is the best way to achieve this. Together, the accuracy and completeness of data form a critical cornerstone of sound research as well as product development. Implementing a strong data integrity foundation will go a long way not only to ensuring product quality and patient safety, but also earning the trust of both regulators and customers.

References

[1] Data Integrity and Compliance with Drug CGMP, U.S. Department of Health and Human Services Food and Drug Administration, December 2018.

[2] Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments, PIC/S Guidance (*Draft*), PI 041-1 (Draft 3), 30 November 2018.

[3] World Health Organization, Guideline on Data Integrity (*Working document QAS/19.819, October 2019, Draft for comments*).

[4] Medicines & Healthcare products Regulatory Agency (MHRA), 'GXP' Data Integrity Guidance and Definitions, Revision 1: March 2018.

[5] ISPE GAMP Guide: Records & Data Integrity, March 2017.

[6] FDA U.S. Food & Drug Administration, Guidance Document - Part 11, Electronic Records; Electronic Signatures – Scope and Application - Guidance for Industry (August 2003).

[7] 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 – Chapter 4: Documentation (January 2011) and Annex 11: Computerised Systems (Revision January 2011).

[8] FDA U.S. Food & Drug Administration, Warning Letter - Hospira Healthcare India Pvt. Ltd. - MARCS-CMS 557890 - March 04, 2019 - https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/hospira-healthcare-india-pvt-ltd-557890-03042019.

[9] FDA U.S. Food & Drug Administration, Warning Letter - Tismor Health and Wellness Pty Limited - MARCS-CMS 588104 - December 05, 2019 - https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/tismor-health-and-wellness-pty-limited-588104-12052019.

[10] FDA U.S. Food & Drug Administration, Warning Letter - Wockhardt, Ltd.MARCS-CMS 495920 — December 23, 2016 -https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/wockhardt-ltd-495920-12232016.

[11] FDA U.S. Food & Drug Administration, Warning Letter - Teva Pharmaceutical Works Private Limited Company MARCS-CMS 496395 — October 13, 2016 - https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/teva-pharmaceutical-works-private-limited-company-496395-10132016.

In Our Next Issue – *The effects of organizational culture on Data Integrity*

Skillpad Canada Inc.
6600 Trans Canada Hwy, Suite 710
Pointe Claire, Quebec, Canada, H9R 4S2
514-316-2339

GTA
Steve Diedrich
Lead Consultant, Compliance
905-716-5375 mobile
514-316-2339 ext. 301
sdiedrich@skillpad.com E-mail
www.linkedin.com/in/skillpadontario

BUSINESS DEVELOPMENT
Alicia Espinoza, B.Sc., PMP
Head of Customer Success and Operational Excellence
514-892-0533 mobile

aespinoza@skillpad.com E-mail
https://www.linkedin.com/in/aliciaespinoza1

SKILLPAD®
www.skillpadcompliance.com