INTERNATIONAL JOURNAL OF PHARMACEUTICAL SCIENCES
[ISSN: 0975-4725; CODEN(USA): IJPS00]
Journal Homepage: https://www.ijpsjournal.com

OPEN ACCESS

Review Paper

Review on Data Integrity Based on The Principle of ALCOA

Gaikwad Swapnali*, Gaiwal Sanika, Ghodke Pratiksha, Ghorpade Ishwari, Gire Nishigandha, Dr. S. D. Mankar

Pravara Rural College of Pharmacy, Pravaranagar Loni Bk, Maharashtra India

ARTICLE INFO

Published: 28 Apr. 2025
Keywords:
Data Integrity, ALCOA, ALCOA+, CFR Part 11
DOI:
10.5281/zenodo.15298717

ABSTRACT

Data integrity is the cornerstone of 21 CFR Part 11, which was published in the United States, and is essential for enforcing rules. FDA officials wished to guarantee that accurate data was collected by the pharmaceutical industry along the course of the medication’s lifespan. Even if this information becomes one of the most valuable assets of any company, if they are not honest, they are not very useful to prevent data from being altered, copied, or transferred, it also entails using appropriate documentation practices. Regarding data integrity, all original records— whether stored electronically or on paper—including source data and metadata are referred to as data. Several regulatory agencies, such as the USFDA, Health Canada, and EMEA, recommended ALCOA to guarantee the accuracy of the data (Attributable, Legible, Contemporaneous, Original, and Accurate.

INTRODUCTION

The accuracy, consistency, dependability, and security of data throughout its whole lifecycle are all referred to as data integrity. It guarantees that information is kept accurate, complete, and safe from loss, corruption, and unauthorized changes. The significance of data integrity. It is crucial to sectors like manufacturing, healthcare, finance, IT, and pharmaceuticals where reliable data is necessary for compliance, decision-making, and operational efficiency [1] The English word integrity is derived from the Latin adjective integer, meaning full or complete. Integrity is the capacity for honesty and the possession of strong moral convictions. Generally speaking, upholding moral and ethical standards is a personal choice. Being truthful, accurate, and sincere in one’s actions is how many people define integrity in ethics. [2]

Importance of Data Integrity

1. **Ensure Regulatory Compliance**

***Corresponding Author:** Gaikwad Swapnali
Address: *Pravara Rural College of Pharmacy, Pravaranagar Loni Bk, Maharashtra India*
Email ✉: swapnaligaikwad431@gmail.com

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Assures Adherence to Regulations Global laws like FDA 21 CFR Part 11 (Electronic records and signatures) must be followed by organizations. WHO Good Practices for Data and Record Management. Computerized systems and validation are covered in EU GMP Annex 11 and 15. Information security management, or ISO 27001. GDPR stands for General Data Protection Regulation. Reputational harm, product recalls, and legal penalties can all be avoided with compliance.

2. Support Accurate Decision Making

In sectors like pharmaceuticals (which guarantee precise drug testing and manufacture), trustworthy data facilitates evidence-based decision-making. Healthcare (ensuring accurate diagnosis and patient records). Finance (making sure that transactions and risk evaluations are accurate).

3. Prevent Data Fraud and Manipulation

Intentional falsification and illegal alterations are prevented by robust data integrity rules. Traceability is guaranteed by the use of audit trails and electronic record management.

4. Enhance product and Process Quality.

Accurate data maintenance helps to avoid errors in manufacturing and medicines. Ensures adherence to regulations and Good Manufacturing Practices (GMP).

5. Strengthen Cybersecurity and Data Protection

Shields private information from illegal access, cyber threats, and hacking. Guarantees data protection through encryption, access restriction, and safe backups.

6. Reduce Business Risk and Financial Losses

Prevents monetary losses brought on by inaccuracies, duplication, or corrupted data. Stops financial transaction fraud and false reporting.

7. Facilitates Digital Transformation and Innovation

Encourages the use of big data analytics, cloud computing, blockchain, and artificial intelligence. Makes sure that the switch from paper-based to digital record-keeping goes smoothly. Reduces manual labor and human mistakes by improving automation.

8. Ensures Data Availability and Long-Term Reliability

Keeps data traceable, retrievable, and accessible over time. Prevents important records from being lost as a result of system malfunctions or inadvertent deletion.

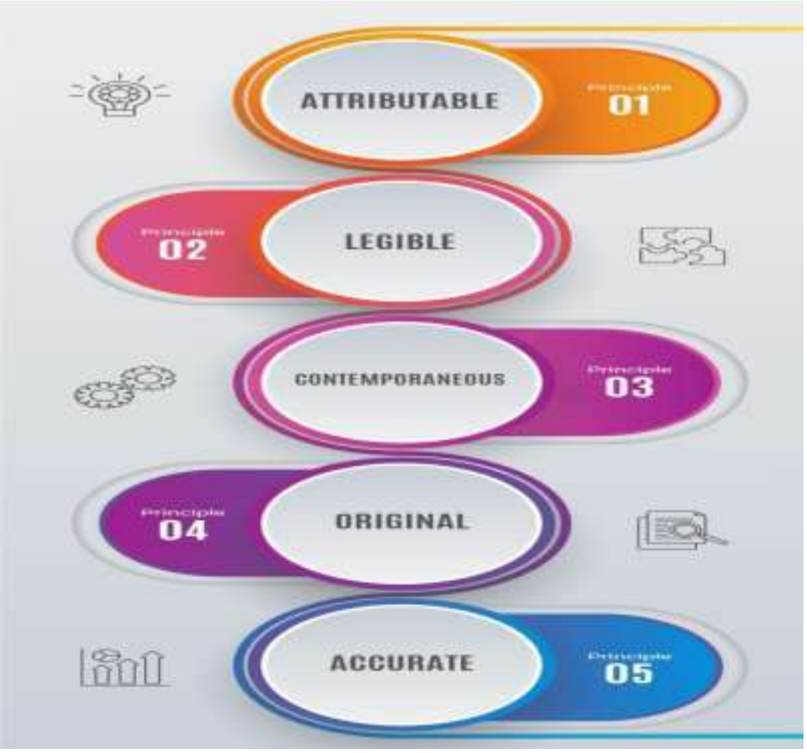
9. Improves Trust and Transparency

Strong data integrity procedures help businesses win over stakeholders, consumers, and regulators.

Maintains the integrity of financial institutions, public health, and scientific research

Principles of Data Integrity Based On ALCOA

The principles based on ALCOA govern data integrity. To ensure that the quality of the evidence is maintained in compliance with regulatory criteria, the pharmaceutical industry uses ALCOA. Many regulatory bodies, such as the FDA, Health Canada, and the EMEA, recommend using ALCOA to ensure that pharmaceutical documentation follows correct protocols. ALCOA stands for Attributable, Legible, Contemporaneous, Original, and Accurate, per US FDA regulations. Because they pertain to data, whether it is digital or paper-based, these simple rules ought to be included in your GDP, data integrity, and data lifecycle initiatives. It facilitates the creation of strategies for preserving the accuracy of the data in both research and manufacturing. ALCOA's role in the following has been discussed: [3,4]



Attributable

The following needs to be noted to guarantee that data that is gathered, created, or modified can be traced back to its source: The name of the individual, system, sensor, apparatus, or gadget that created, gathered, or updated the data The data's origin The time and date Whether the data is gathered, created, or updated automatically or manually, the aforementioned is true. Since all current (and many older) systems and software

Legible

Ensuring data is legible is about more than being able to read the data, although that is important in situations where manual record-keeping takes place. Being able to make out words and figures is much less of a problem with electronic data, though. That said, legibility still has relevance when data is digitally created, generated, or updated, as it is essential that data can be read and understood years and even decades after it's recorded. This point is as relevant to digitally recorded data as it is to data recorded in notebooks. So, it's important to avoid using clichés and unusual phraseology as this may be difficult to decipher in the future without getting clarification from the originator of the data, a person who may no longer be available.

Contemporaneous

Every time an event or activity occurs, it is imperative that people or systems record the data. Timestamping is typically standard procedure when dealing with electronic data, but there are a few things to keep in mind. Along with making sure system clocks are precise and time zones are noted, this also entails making sure data processes are not queued up, which could cause delays in timestamping. However, another factor that is more pertinent to manual record-keeping is contemporaneous data recording. Avoiding the habit of adding or changing data at a later time is the primary goal. Errors may occur when data is captured after an event or action, such as when sections are omitted, details are lost,

Original

Original records are preferable to transcriptions or reproductions. Once more, this primarily pertains to manual recordkeeping. For instance, it can lead to mistakes if you write information on a piece of paper to finish the primary record later. Rather, whether the data is on paper or in a digital system, the primary record should remain the original recording. Technical and procedural safeguards must be in place for digitally recorded data to guarantee that the original recording cannot be altered.

Evolution of Alcoa To ALCOA+

Regulatory organizations like the U.S. Food and Drug Administration (FDA) first proposed the ALCOA principle to guarantee data conformity, integrity, and dependability in sectors including manufacturing, pharmaceuticals, and healthcare. ALCOA was extended into ALCOA+ to further enhance data governance as digital recordkeeping and data management techniques developed over time. ## The necessity of expansion Introduction [5]

Need for Expansion:

Introduction of ALCOA+

As cloud storage, automation, AI-driven data management, and electronic recordkeeping proliferated, more specifications were required to guarantee total data integrity. As a result, ALCOA evolved into ALCOA+, which added four more principles:

Complete

No information should be omitted or deleted; all necessary data should be present. All information is kept in a single file, including user inputs, measured data, and electronic signatures. The “old value, new value, and reason for change” store user inputs and changes. To guarantee the exact temporal sequence and completeness of the data records from the moment of initial capture to the subsequent processing, each data record is stamped with the date and time.

Consistent

Data should follow a logical sequence, with proper timestamps and audit trails. As near to the procedure as feasible, the data is captured using the digital Memograph M RSG45 Data Manager and saved as raw data. The audit trail is an inexhaustible system function that cannot be turned off or reset. The consistency of the data from the time it is recorded and moved to the database until it is printed in hard copy on the graph or chart is ensured by the synchronized system time built into the data records.

Enduring

For the necessary retention time, data must be kept in a secure location. All information is kept in the Memograph M on industrially compliant storage media (SD cards, non-volatile memory). A battery buffers nonvolatile memory (RAM), and an internal emergency procedure guarantees a further backup of the memory contents in the case of a power outage. The data is saved in approved databases and made accessible for additional usage (analysis, reporting, printout, etc.)

Available

When data is required for inspections, audits, or decision-making, it should be available. Data can be shown in the FDM software or on a monitor on the RSG45. The data can be made available at any moment in digital exchange forms including PDF, XLS, and CSV for documentation and auditing needs. These files can be produced manually or by a batch procedure that is automated and time-controlled. Authorized individuals with the proper access authorization can access the data at any time through secure remote access, for example, for verification. [16]

World Regulatory Recommendations For Data Integrity:

USFDA: 21-CFR: The executive departments and agencies of the federal government use the federal register to publish permanent, wide regulations that are enshrined in then 21 CFR (Code of Federal Regulation). Title 21 of the CFR contains the regulations set forth by the Food and Drug Administration. Each book or volume has its CFR modified once annually on or around April 1st [6, 7, 8]

MHRA: The pharmaceutical quality system, which ensures that drugs are of the required quality, heavily relies on data integrity. The MHRA's guideline on GMP data integrity requirements for the pharmaceutical sector is intended to improve the EU's current GMP standards for active ingredients and dosage forms. [6,9,10]

TGA: The Australian regulatory body known as the Therapeutic Goods Administration (TGA) establishes the benchmark for data integrity as a deficiency. A process or method fault that has caused or could cause a significant risk of producing a product that is hazardous to users. It also occurs when the maker is found to have misled, misrepresented, or fabricated products [6, 7]

cGMP: The FDA acknowledged the trend of increasing data integrity breaches in its guidelines on Data Integrity and Compliance with cGMP, which were created in response to the importance of this issue. cGMP-compliant records-keeping practices prevent data obscuration or loss. [11,12]

Good Documentation Practices: In the context of these suggestions, good practices are defined as techniques that together and separately ensure that documentation, whether electronic or paper, is accountable, legible, traceable, permanent, contemporaneously documented, original, and accurate. [6]

WHO: In the context of these suggestions, "good practices" refers to the techniques that collectively and separately ensure that documentation, whether electronic or paper, is accountable, legible, traceable, permanent, contemporaneously documented, original, and accurate. A critical stage in the process, which includes numerous participants and activities, is ensuring the accuracy and dependability of the data manufacturers give to national [10,1]

Data Integrity Risk: A variety of circumstances can jeopardize the integrity of data contained in a database. Here are a few examples:

Human Error: Data integrity is compromised when someone enters incorrect information, copies or removes data, disregards the proper protocol, or makes mistakes when carrying out the process for information security goals.

Transfer Errors: There has been a transfer error when information cannot be successfully moved between locations in a database. In relational databases, transfer errors happen when a piece of data is present in the destination table but absent from the source table.

Bugs and viruses: Software elements that can infiltrate a computer and alter, remove, or steal data include viruses, spyware, and malware.

Compromised Hardware: Serious failures that could point to hardware problems include sudden and unplanned server or computer failures, as well as problems with the operation of a computer or other system. Hardware compromise can result in missing or erroneous data, limit or stop data access, or make information impossible to use. [14,15]

Future Scope of Data Integrity Based On Alcoa Principles:

Integration of AI & Machine Learning for Data Integrity

Automated anomaly detection: AI-powered tools will proactively spot fraudulent data changes, human mistakes, and discrepancies. Real-time validation: To guarantee adherence to ALCOA standards, machine learning models will automate data validation procedures. Predictive analytics: AI will evaluate risk variables that compromise data integrity and suggest fixes before problems occur.

Blockchain for Immutable Data Records

Audit trails that are impenetrable to tampering: Blockchain technology guarantees data immutability, enabling every transaction to be tracked and validated, hence confirming accurate and attributable data. Decentralized data integrity: By preventing unwanted changes and guaranteeing transparency, smart contracts will uphold the ALCOA principles.

Edge Computing for Real-Time Data Integrity

Decentralized data processing: By enabling data validation at the point of generation, edge computing will guarantee accurate and timely data recording.

CONCLUSION:

By implementing ALCOA principles alongside best practices such as access controls, encryption, Validation checks, and auditing, organizations can strengthen data integrity, minimize risks, and comply with regulatory requirements. A culture of accountability and continuous monitoring Further enhances data reliability, ensuring that it remains a trustworthy asset for decision-making and compliance. When data is gathered and used to make decisions about manufacturing and quality, the Quality Risk Management (QRM) approach can help prevent, identify, and reduce potential risks while guaranteeing that the data is reliable and trustworthy. The preservation of electronic data is guaranteed by data integrity. The quality of reports depends on the information they are founded on. Information that is not kept on a computer can also be considered data-integrated.

REFERENCES

1. Qas19-819-Rev1-Guideline-on-Data-Integrity.Pdf. https://www.who.int/docs/defaultsource/medicines/norms-and-standards/current-
2. What is Data Integrity? Definition, Types & Tips. https://www.digitalguardian.com/blog/what-dataintegrity-data-protection-101
3. Nikam, N. R.; Patil, P. R.; Vakhariya, M. R. R.; Mohite, D. S. K. DATA Integrity: An Overview. 2020, 11.
4. Boritz, J. E. IS Practitioners' Views on Core Concepts of Information Integrity. Int. J. Account. Inf. Syst. 2005, 6 (4), 260–279. https://doi.org/10.1016/j.accinf.2005.07.001.
5. WHO-Guideline-on-Data-Integrity-Draft.Pdf .https://rx360.org/wpcontent/uploads/2018/08/WHOGuideline-on-Data-Integrity-Draft.pdf (accessed 2023-04-19)
6. Ahmad, S.; Kumar, A.; Hafeez, A. Importance of Data Integrity & Its Regulation in Pharmaceutical Industry; preprint; Preprints,

2022. https://doi.org/10.22541/au.166265947.70683270/v1.

7. Hart, S. Data Integrity: TGA Expectations.
8. Rachel, P. K.; Gupta, N. V. Data Integrity – Regulations and Current Scenario. No. 05.
9. Data_integrity_definitions_and_guidance_v2_Withdrawn.Pdf https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/697053/Data_integrity_definitions_and_guidance_v2_Withdrawn.pdf (accessed 2023-04-19).
10. New MHRA "GxP Data Integrity Guidance and Definitions" published – ECA Academy. https://www.gmp-compliance.org/gmp-News/new-mhra-gxp-data-integrity-guidance-and-definitions-published (accessed 2023-04-19).
11. McLaughlin, E. Guidance for Industry. Quest. Answ. 2018.
12. Ensuring CGMP Standards for Data Integrity. https://www.pharmtech.com/view/ensuring-cgmpstandards-for-data-integrity (accessed 2023 -04-19)
13. What is Data Integrity and Why is it Important? | Egnyte. https://www.egnyte.com/guides/governance/data-integrity (accessed 2023-04-19)
14. IT Data Integrity Risk – Open Risk Manual. https://www.openriskmanual.org/wiki/IT_Data_Integrity_Risk (accessed 2023-04-20).
15. Spilka, S. Data Integrity: Relevancy, Risks and the Appropriate Use. ANEXIABlog.https://anexia.com/blog/en/data-integrity- Relevancy-risks-and-the-appropriate-use/ (accessed
16. In the context of the Memograph M RSG45 Data Manager combined with Field Data Manager (FDM) Analysis software.

HOW TO CITE: Gaikwad Swapnali*, Gaiwal Sanika, Ghodke Pratiksha, Ghorpade Ishwari, Gire Nishigandha, Dr. S. D. Mankar, Review on Data Integrity Based on The Principle of ALCOA, Int. J. of Pharm. Sci., 2025, Vol 3, Issue 4, 3184-3190. https://doi.org/10.5281/zenodo.15298717