International Journal of Pharmaceutical Research and Development

ISSN Print: 2664-6862
ISSN Online: 2664-6870
Impact Factor: RJIF 8.55
IJPRD 2025; 7(2): 882-886
www.pharmaceuticaljournal.net
Received: 10-10-2025
Accepted: 13-11-2025

Patel Richi
Rakeshkumar, M. Pharm (Pharmaceutical Quality Assurance), Gujarat Technological University, Ahmedabad, Gujarat, India

Rajgor Hiral A
M. Pharm (Pharmaceutical Quality Assurance), Gujarat Technological University, Ahmedabad, Gujarat, India

Corresponding Author:
Patel Richi
Rakeshkumar, M. Pharm (Pharmaceutical Quality Assurance), Gujarat Technological University, Ahmedabad, Gujarat, India

Data Integrity in Pharmaceutical Quality System

Patel Richi and Rajgor Hiral A

DOI: https://doi.org/10.33545/26646862.2025.v7.i2j.253

Abstract
Data integrity has become a cornerstone of pharmaceutical quality systems, directly influencing patient safety, regulatory compliance, and product quality. As pharmaceutical operations increasingly rely on both manual and electronic data, ensuring the accuracy, consistency, and reliability of information throughout its lifecycle is critical. Regulatory authorities such as the US FDA and EMA emphasize strong data governance through frameworks like cGMP, 21 CFR Part 11, and EU Annex 11. Central to these requirements are the ALCOA and ALCOA+ principles, which define good documentation practices. This article presents a concise yet comprehensive overview of data integrity concepts, principles, classifications, risks, regulatory expectations, and modern digital approaches, highlighting strategies to strengthen pharmaceutical quality systems and sustain regulatory trust.

Keywords: Data integrity, ALCOA+, pharmaceutical quality system, regulatory compliance, digital transformation

Introduction
In the pharmaceutical industry, data is not merely supportive documentation but a scientific and regulatory asset that underpins decision-making, product quality, and patient safety [1,7]. Data is generated across the entire product lifecycle—from development and manufacturing to quality control, distribution, and post-marketing surveillance [3]. Whether recorded on paper or within computerized systems, data must remain trustworthy from creation to archival [4].
Regulatory agencies require pharmaceutical organizations to establish systems that ensure data is complete, accurate, and secure [5]. The concept of the data lifecycle encompasses creation, processing, review, storage, retrieval, and eventual disposal of data [1]. Any weakness within this lifecycle can compromise product quality and regulatory confidence, making a strong data integrity culture essential [2].

Principles of Data Integrity
Regulatory guidance documents highlight the ALCOA principles as the foundation of good documentation practices in the pharmaceutical industry [1, 4, 7]. These principles define expectations for data reliability across both paper-based and electronic systems.

Attributable: Data must clearly identify who performed an action and when [1].
Ex. = During a stability study in a pharmaceutical company, a temperature correction was made to a data logger record. However, the adjustment was entered manually on paper without identifying who made the change or why it was necessary.

Legible: Records should be readable, permanent, and understandable [7].
Ex. = A lab technician handwrites the pH measurement of a solution in their lab notebook. Although the value is correct, the number is written with unclear digits—it's difficult to tell whether it reads 7.1 or 7.7. This ambiguity leads to confusion during a batch review, delaying batch release.

Contemporaneous: Data must be recorded at the time the activity occurs [4].

Ex. = A microbiologist performs an environmental monitoring test in a sterile room and collects surface swab samples at 10:15 AM. Instead of recording the sampling time immediately, they wait until the end of their shift and fill in the data sheet around 5:00 PM, estimating the times from memory.

Original: The first recorded data or true copy must be preserved [1].
Ex. = An HPLC operator captures a chromatogram of a drug sample and prints the result to review it. Instead of saving the original electronic file, they annotate the printed copy, scan it, and upload only the scan to the batch record system—discarding the raw digital output.

Accurate: Data must correctly reflect the activity performed without errors or bias [7]. Ex. = A production technician documents the quantity of tablets produced as 25,000 units based on the planned batch size. However, the actual count from the final packaging line was 24,760 units, and the difference was not reconciled or corrected in the record. The value was rounded up for simplicity.
To strengthen these concepts, ALCOA+ principles were introduced, adding [7]:

- **Complete:** All relevant data, including repeats and failed results, must be retained.
- **Consistent:** Data should follow a logical order with aligned timestamps.
- **Enduring:** Records must remain intact and accessible throughout the retention period.
- **Available:** Data should be readily retrievable for review or inspection.
- **Traceable:** The full history of data must be reconstructable.

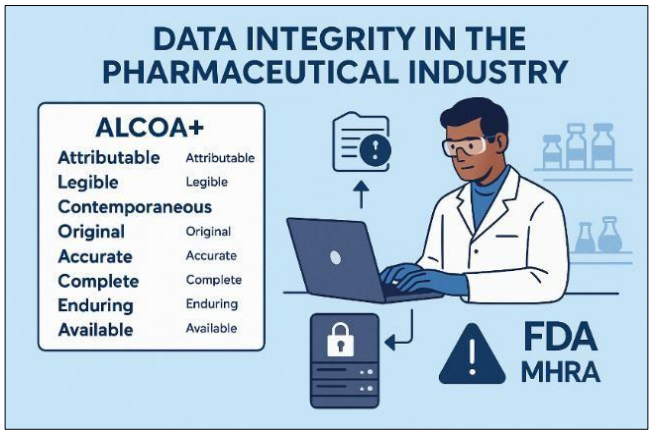

Fig 1: Principle of Data integrity

Types and Classification of Data

Types of Data

Pharmaceutical data can be categorized based on its origin, use, and context [7]:

- **Primary Data:** Original observations directly recorded during an activity.
- **Metadata:** Contextual information describing how, when, and by whom data was generated.
- **Analyzed Data:** Processed or interpreted data derived from primary data.
- **Time-Responsive Data:** Data that changes dynamically over time.
- **Digital Records:** Electronically stored data requiring specific security and validation controls.

Classification of Data Integrity

Data integrity is commonly classified into physical and logical components [1,7]:

- **Physical Integrity:** It talks about the challenges of storing data and retrieving it. Ensure that data is not lost due to events such as natural disasters, computer failures, or other mishaps. This aspect of data integrity deals with safeguarding information against threats that may arise from the environment or system failures. It focuses on the ability to properly store, preserve, and retrieve data without loss or distortion.
- **Logical Integrity:** The consistency, accuracy, and reliability of the information included in a system at the conceptual or logical level is known as logical integrity. It comprises ensuring that the data accurately depicts the actual-existence entities that it is meant to capture and maintaining the connections and constraints that define the data's structure. There are a few essential components of logical integrity.

Importance of Data Integrity [1, 6]

In the pharmaceutical industry, data is more than just numbers and records—it is the invisible thread that ties scientific discovery to patient safety.

Protecting Patient Wellbeing

Trustworthy data ensures that medicines are safe for human use. If the data used to test and approve medications is compromised, the health and lives of patients may be put at risk. Thus, data accuracy is a direct shield for patient safety [1].

Fueling Innovation and Discovery

Reliable information is the backbone of scientific breakthroughs. Without truthful and traceable data, researchers cannot draw valid conclusions, delaying the development of novel therapies and treatments [6].

Maintaining Product Excellence and Therapeutic Effect

The consistency and performance of pharmaceutical products are driven by validated data. If quality data is preserved, it guarantees that each unit of the product

performs as expected, meeting its intended health outcomes [1].

Ensuring Information Privacy and Protection
The security of digital and recorded information is crucial, not only to protect internal processes but also to uphold ethical standards regarding personal and clinical data. Data integrity helps avoid breaches and unauthorized access [1].

Smooth Operation of Supply Chain Systems
From raw material sourcing to final distribution, clean and consistent data enables every step of the pharmaceutical supply chain to operate without disruption. It reduces errors in tracking, logistics, and inventory handling [6].

Defending Ownership of Scientific Creations
Intellectual property such as formulations, protocols, or innovations is safeguarded when the data supporting them is untampered. Authentic data can legally defend patents and proprietary rights in competitive environments.[6]

Supporting Transparent and Accurate Recordkeeping
An unbroken and verifiable documentation trail ensures that all actions are recorded and traceable. This helps internal reviews and external audits and ensures full regulatory compliance [1].

Common Data Integrity Challenges
Despite regulatory guidance, pharmaceutical companies frequently encounter data integrity challenges [1, 4, 6] including:

- Weak or shared login credentials
- Inadequate access control
- Backdating or manipulation of records
- Poor documentation practices
- Disconnected information systems
- Unvalidated system changes

These issues often arise from systemic weaknesses rather than isolated individual errors [7].

Root Causes and Risk Factors
Root Causes
Common root causes of data integrity failures include staffing shortages, insufficient training, production pressure overriding quality priorities, and intentional data falsification [1, 6, 7]. Weak quality culture and lack of management oversight further increase vulnerability [2].

Risk Factors
Data integrity risks are broadly classified into organizational, technical, and human factors [3, 4, 6]:

- **Organizational:** Poor governance and limited leadership commitment
- **Technical:** Legacy systems and inadequate validation
- **Human:** Skill gaps, ethical lapses, and unclear responsibilities

Way to reduce Data integrity risk factor [6]
Ensure protection of critical data through controlled storage and restricted handling.
Maintain complete traceability of actions by implementing reliable activity logging systems

- Adopt structured backup and restoration procedures to safeguard information against loss or corruption.
- Establish strict user authentication and role-based access to sensitive data environments.
- Use personal identification mechanisms

Regulatory Expectations
Multiple regulatory frameworks define expectations for data integrity in pharmaceutical operations [5,6,9] including:

Good Manufacturing Practice (GMP)
GMP regulations establish a structured approach to maintain the quality and reliability of pharmaceutical production activities. These standards encompass provisions related to data accuracy, proper documentation, systematic record maintenance, and effective data handling at every stage of the manufacturing process.

21 CFR Part 11 (US)
In the U.S., the regulation known as 21 CFR Part 11 defines the standards for managing electronic records and electronic signatures within the pharmaceutical sector. It offers directives to ensure that digital records remain genuine, accurate, and dependable, covering aspects such as electronic data collection systems and the secure use of digital signatures.

EU Annex 11
Annex 11 of the EU Good Manufacturing Practice (GMP) standards addresses the use of computerized systems in pharmaceutical production. It sets out criteria for maintaining data accuracy, managing electronic records and signatures, and verifying that computerized systems operate as intended through proper validation.

Good Laboratory Practice (GLP)
GLP standards outline the fundamental rules for performing non-clinical laboratory research. They highlight the need for maintaining strong data integrity by ensuring that study information is recorded precisely and in full, following established standard operating procedures, and properly noting any deviations or modifications made during the study.

Good Clinical Practice (GCP)
GCP standards define the requirements for planning, executing, overseeing, and documenting clinical trials. They stress the importance of preserving data integrity and ensuring trustworthy records by accurately capturing trial information, following approved protocols, and retaining complete source documents.

The General Data Protection Regulation
GDPR is an extensive privacy law in the European Union that applies to any sector managing the personal information of EU citizens. It enforces rigorous data protection requirements, emphasizing principles such as data integrity and precision.

ISO 27001
ISO 27001 sets the criteria for creating, applying, sustaining, and continuously enhancing an Information Security Management System (ISMS). Within this framework, data integrity is recognized as a key element of

information security and is addressed as part of the standard's requirements.

Data Integrity Maturity Model [6]

The Data Integrity Maturity Model (DIMM) is a structured framework that describes how an organization's practices for ensuring the accuracy, consistency, and reliability of data evolve over time. It divides progress into stages—from unorganized and error-prone practices at the lowest level, to fully standardized, controlled, and continuously improving systems at the highest level.

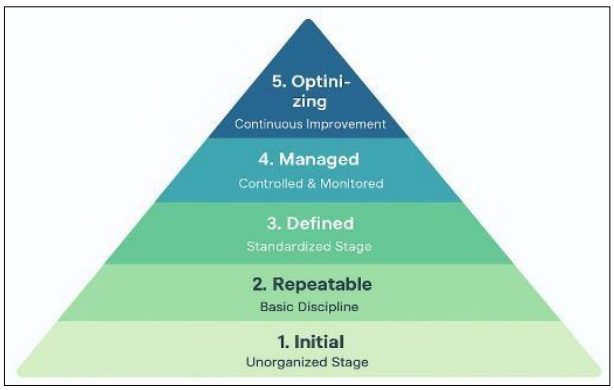

Fig 2: Maturity Model of Data integrity

Level 1 – Initial (Unorganized Stage)
Key Risks

- High chance of data loss, errors, or manipulation.
- No reliable audit trails; difficult to prove compliance.
- Regulators would see this as high risk for data integrity breaches.

Example Situation

An analyst records test results in a notebook but forgets to sign or date them. Another analyst uses a different format, making it hard to compare results.

Level 2 – Repeatable (Basic Discipline Stage)
Key Improvements

- Teams begin following some rules, like documenting who did the work and when.
- More consistency across different employees.
- Basic training on good documentation practices starts.

Limitations

- Processes are still vulnerable to mistakes since oversight is minimal.
- Compliance may depend too much on individuals' honesty and discipline.

Example Situation

Lab staff start using templates for test records, but each site or department still has slight variations.

Level 3 – Defined (Standardized Stage)
Key Improvements

- Policies, SOPs (Standard Operating Procedures), and templates are consistent.
- Roles and responsibilities (e.g., who approves, who reviews) are clearly set.
- Greater alignment with regulatory requirements.

Benefits

- Easier to train staff because processes are the same everywhere.
- Reduces ambiguity and mistakes.

Example Situation

Every laboratory in the company uses the same electronic template, with mandatory fields (date, analyst, instrument ID).

Level 4 – Managed (Controlled Stage)
Key Improvements

- Routine monitoring of processes.
- Audit trails and electronic records are reviewed to detect irregularities.
- Risks are assessed proactively, not just reactively.

Benefits

- Data integrity is built into the system, not left to chance.
- Regulatory inspections become smoother, as evidence of compliance is available.

Example Situation

Audit trails of HPLC (High-Performance Liquid Chromatography) systems are reviewed weekly to confirm no unauthorized changes were made.

Level 5 – Optimizing (Continuous Improvement Stage)
Key Improvements

- The company has a culture of "quality first."
- Data integrity is part of everyday decision-making, not just compliance.
- Emerging technologies (AI, blockchain, cloud-based solutions) may be adopted.

Benefits

- Sustained trust from regulators, partners, and patients.
- Reduced cost of rework, investigations, and CAPAs (Corrective and Preventive Actions).

Example Situation

An organization invests in predictive analytics to monitor data patterns and prevent issues before they occur, while also running regular workshops to refresh staff knowledge.

1. Digital Transformation and Emerging Technologies

Digital transformation has become a key enabler for strengthening data integrity in pharmaceutical quality systems [3, 10]. Technologies such as electronic quality management systems, digital batch records, real-time monitoring tools, and blockchain-based traceability improve transparency, reduce human error, and enhance regulatory confidence [3, 10].

Blockchain technology, in particular, offers tamper-resistant records and end-to-end visibility across the pharmaceutical supply chain, supporting authenticity and traceability [3].

Best Practices to Improve Data Integrity [4]
Customized Training Modules Based on Job Functions

General training is not enough. Data integrity training should be tailored to specific roles—for example, production staff should focus on batch record accuracy, while analysts should concentrate on electronic data entries

and audit trails. This role-specific approach makes training more relevant, easier to retain, and more effective in preventing data errors.

Layered Authorization in Computerized Systems

To reduce the risk of unauthorized data access or alterations, pharmaceutical companies should implement multi-tiered user access levels in computerized systems. Each layer (e.g., data entry, review, approval) must be separated with unique login credentials and password policies. This structured control ensures traceability and minimizes intentional or accidental data manipulation.

Auto-Validation in Electronic Data Capture Systems

Modern electronic systems should not only store data but also validate it in real time. For example, during equipment calibration or test result entries, systems can auto-flag abnormal values, missing data, or time inconsistencies. This immediate feedback loop can prevent errors from progressing further and ensure real-time data reliability.

Two-Way Communication Channels Between Departments

Data integrity is often compromised when departments (like QA, QC, and production) work in silos. Introducing structured, two-way communication protocols—such as shared data review dashboards, inter-departmental alerts for anomalies, and collaborative investigation meetings—can reduce misunderstandings and promote joint accountability.

Audit-Ready Dashboards for Real-Time Monitoring

Developing central dashboards that visually show real-time trends—such as missing signatures, delayed entries, or duplicate records—can alert teams before issues escalate. These dashboards should be accessible to QA leads and plant heads, encouraging real- time correction rather than post-event justification during audits.

Conclusion

Data integrity is fundamental to pharmaceutical quality systems and cannot be treated as a one- time compliance exercise. It requires continuous attention, strong governance, skilled personnel, and modern digital tools. By applying ALCOA+ principles, addressing root causes, and leveraging digital transformation, pharmaceutical organizations can protect patient safety, maintain regulatory confidence, and support sustainable innovation. Ultimately, safeguarding data integrity ensures that every decision based on data is ethical, scientific, and reliable.

Acknowledgement

I would like to express sincere gratitude to the faculty members of A.R. College of Pharmacy and G.H. Patel Institute of Pharmacy for their valuable guidance, academic support, and encouragement throughout the preparation of this article. Special thanks are extended to mentors and colleagues for their constructive suggestions and continuous motivation, which significantly contributed to the successful completion of this work.

Conflict of Interest

I declare that there is no conflict of interest related to the publication of this article.

References

1. Gokulakrishnan D, Venkataraman S. Ensuring data integrity: Best practices and strategies in pharmaceutical industry. Intelligent Pharmacy. 2024.
2. Wolf K. Why data integrity is impossible without a quality culture. Pharmaceutical Online. 2019.
3. Leal F, Chis AE, Caton S, González–Vélez H, García–Gómez JM, Durá M, *et al*. Smart pharmaceutical manufacturing: Ensuring end-to-end traceability and data integrity in medicine production. Big Data Research. 2021;24:100172.
4. Ullagaddi P. Safeguarding data integrity in pharmaceutical manufacturing. Journal of Advances in Medical and Pharmaceutical Sciences. 2024;26(8):64-75.
5. James R, Das S, Kumari A, Rekdal M, Kulyadi GP, Sathyanarayana MB. A recent regulatory update on consequences of data integrity issues and its management in pharmaceutical scenario. Indian Journal of Pharmaceutical Education and Research. 2021;55(2):S616-S22.
6. Ronolo SC. Assuring Data Integrity towards Regulatory Compliance: A Study on Process Improvement in Data Integrity Compliance of Computerized Systems. 2023.
7. Sabale MM, Pande VA, Tagalpallewar AA, Swami AG, Pawar AT, Baheti AM. Maintaining data safety and accuracy through data integrity (DI): A comprehensive review. Research Journal of Pharmacy and Technology. 2024;17(5):2431-40.
8. Vignesh M, Ganesh G. Current status, challenges and preventive strategies to overcome data integrity issues in the pharmaceutical industry. Int J Appl Pharm. 2020;12:19-23.
9. Ingale M, Tayade M, Patil Y, Salunkhe R. Data Integrity Violations in the Pharmaceutical Industry and Regulatory Measures. International Journal of Pharmaceutical Quality Assurance. 2023;14(2):416-20.
10. Ullagaddi P. Digital transformation strategies to strengthen quality and data integrity in pharma. International Journal of Business and Management. 2024;19(5):16-26.