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

OPEN ACCESS

**Review Article**

# Data Integrity in Pharmaceutical Quality Assurance: Regulatory Requirements, Challenges and Future Perspectives

**Avinash Sapkale*, Dr. Amit Kasabe, Rehan Sayyad**

*Department of Pharmaceutical Quality Assurance, PDEA SUCOPRC, Kharadi, Pune, India*

ARTICLE INFO

Published: 24 Jun 2026
Keywords:
Data integrity, ALCOA+, pharmaceutical quality assurance, 21 CFR Part 11, EU GMP Annex 11, audit trail, MHRA, regulatory compliance
DOI:
10.5281/zenodo.20839303

## ABSTRACT

Pharmaceutical quality assurance rests, fundamentally, on the trustworthiness of the data it produces. If that data cannot be relied upon, neither can any decision made from it- including decisions about whether a product is safe to release. Over the last decade or so, this has stopped being a theoretical concern. Enforcement actions with data integrity at their centre have risen sharply across the global pharmaceutical industry, to the point where agencies including the FDA, EMA, MHRA, WHO, and PIC/S all felt compelled to issue detailed guidance- most of it published between 2015 and 2023. This paper works through what that regulatory environment actually looks like, with GMP, GLP, and GCP settings each receiving attention, and with the ALCOA+ framework- Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, Available- as the organising thread. Using FDA warning letter records from 2015 to 2022, we look systematically at documented violations: audit trail tampering, backdating of records, deliberate deletion of out-of-specification results, and poorly managed access controls. There is also a frank assessment of the practical difficulties organisations face in meeting these standards, from the headaches created by hybrid paper-electronic systems to the cost and complexity of modernising legacy infrastructure and keeping tabs on outsourced supply chains. Technologies that have attracted attention as potential solutions- blockchain-based audit trails, machine learning anomaly detection, cloud electronic batch records, process analytical technology- are examined for what they can realistically deliver rather than what they promise in theory. We propose a five-tier data governance framework anchored in ICH Q9 and Q10, covering leadership accountability, risk-based controls, technical safeguards, procedural requirements, and quality culture. The paper closes by arguing that future progress depends on three things that currently remain incomplete: meaningful harmonisation of international standards, regulatory frameworks agile enough to keep pace with digital change, and a genuine shift in organisational culture that makes data integrity something people actually believe in rather than just comply with.

***Corresponding Author:** Avinash Sapkale
**Address:** *Department of Pharmaceutical Quality Assurance, PDEA SUCOPRC, Kharadi, Pune, India*
**Email** : avisapkale2122@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.

## INTRODUCTION

Ask any pharmaceutical quality professional what keeps them up at night, and data integrity tends to feature early in the conversation. The concept itself is straightforward enough — it refers to the completeness, consistency, and accuracy of data across its entire life, from first capture through processing, storage, archiving, and eventual destruction. In practice, maintaining that integrity across the full range of systems, people, and processes involved in modern pharmaceutical manufacturing is anything but straightforward. Regulators around the world have flagged data integrity failures as a root cause of serious GMP deficiencies with enough regularity that it can no longer be treated as a peripheral concern. The FDA alone issued more than 150 warning letters between 2015 and 2022 in which data integrity was a central issue, and manufacturers in India, China, and Southeast Asia appeared disproportionately among them.

This level of regulatory attention did not arrive suddenly. What galvanised it, more than anything else, was the Ranbaxy case of 2013 — and the stream of consent decrees involving Indian manufacturers that followed. These were not cases of sloppy record-keeping or minor procedural lapses; they exposed systematic, deliberate manipulation of data at scale. The response from regulators was to rethink how they read data integrity failures. Rather than treating them as isolated technical violations, agencies began interpreting them as indicators of something deeper — a company's overall quality culture and the seriousness with which it approaches its obligations. The WHO gave formal expression to this view in Technical Report Series No. 996 (2016),[4] and both the MHRA[3] and the FDA issued dedicated guidance in 2018.

The conceptual framework most regulators now work within is ALCOA+. The original five attributes — Attributable, Legible, Contemporaneous, Original, Accurate — are widely attributed to FDA investigator Stan Woolen, who articulated them in the 1990s. Four more were added later (Complete, Consistent, Enduring, Available) as electronic data environments introduced new ways for data to be compromised or simply lost.[5,6] Together the nine attributes have become a kind of universal checklist that applies equally in GMP, GLP, and GCP settings, giving inspectors a common language and giving industry a common target.

The volume of guidance now available would suggest that the solutions are well understood. In some respects they are. But the industry continues to struggle with implementation in ways that point to something more than a knowledge gap. Hybrid paper-electronic systems create integrity risks at every handover point. Legacy software platforms were simply not built to meet today's expectations. Training programmes vary enormously in quality. And in too many organisations, the culture around data — the everyday norms about what gets recorded, how, and when — hasn't really shifted.[7,11,12] Meanwhile, cloud computing, blockchain, artificial intelligence, and electronic batch record systems are opening up real possibilities, but also introducing their own compliance uncertainties.

This review draws on primary regulatory guidance documents, peer-reviewed research, and FDA enforcement data to work through the regulatory landscape, document what violations actually look like in practice, examine where implementation is hardest, and sketch a governance framework that quality professionals can put to use. The authors have tried to be practically minded throughout — this is not intended as an abstract survey but as a

resource that connects regulatory expectations to real-world challenges.

## 2. REGULATORY LANDSCAPE AND APPLICABLE GUIDELINES

### 2.1 Evolution of Data Integrity Regulation

The regulatory story of pharmaceutical data integrity begins with 21 CFR Part 11, published by the FDA in 1997. That rule established something that was genuinely novel at the time: electronic records and electronic signatures could be treated as legally equivalent to paper. Subsequent guidance has refined and extended the rule, but its core logic — that digital data is regulated data — remains foundational to the US framework.[8] The predicate rules, meaning the underlying GMP regulations that Part 11 applies to, have been progressively interpreted to require rigorous data governance across all record types, not just those generated electronically.

Europe took a different path. EU GMP Annex 11 (2011), together with Chapter 4 on documentation,[20] set out detailed expectations for computerised systems — covering validation requirements, audit trail capability, access controls, and data backup — without creating a single overarching electronic records rule on the Part 11 model. The result is a framework that is arguably more flexible but also harder to apply uniformly. At the international level, the most significant development in recent years has been PIC/S PI-041-1 (2021),[5] which is now recognised by more than 50 regulatory authorities and represents the broadest consensus document on data integrity in GxP environments currently in existence.

**Table 1: Comparative Overview of Key Regulatory Frameworks Governing Data Integrity in Pharmaceutical Quality Assurance**

| Regulatory Body | Guideline / Regulation | Year | Key Data Integrity Requirements |
|---|---|---|---|
| FDA (USA) | 21 CFR Part 11 | 2003 | Electronic records, electronic signatures, audit trail requirements |
| FDA (USA) | Guidance for Industry: DI and cGMP | 2018 | ALCOA+ principles, complete data, predicate rules |
| EMA (Europe) | EU GMP Chapter 4 & Annex 11 | 2011/ 2015 | Computerised systems, paper records, validation |
| MHRA (UK) | GxP Data Integrity Guidance | 2018 | Data governance, audit trail review, risk assessment |
| WHO | Technical Report Series No. 996 | 2016 | Data governance framework, DI in GMP/GLP/GCP |
| PMDA (Japan) | PIC/S PI-041 | 2021 | Audit trail review, backup verification, raw data |
| PIC/S | PI-041-1 | 2021 | Risk-based approach to data governance; SOPs |
| CDSCO (India) | Revised Schedule M | 2023 | Data integrity aligned with PIC/S standards |
| TGA (Australia) | Data Integrity Guidance | 2019 | Hybrid systems, metadata, migration controls |

*Adapted from FDA (2018)[1], EMA (2011)[2], MHRA (2018)[3], WHO (2016)[4], PIC/S (2021)[5]*

### 2.2 ALCOA+ Framework: The Universal Standard

The ALCOA+ framework is the closest thing the industry has to a universal standard for data quality, and it operates across GMP, GLP, and GCP alike. It started as five attributes and was extended to nine when the growing complexity of electronic data environments made the original five feel insufficient — there were simply too many ways that digital data could be compromised or rendered inaccessible that the original model didn't cover.[6,13] Each attribute has regulatory teeth, and each comes up routinely in inspection findings

and warning letters. The implications vary depending on whether data is paper-based, electronic, or a hybrid of the two — but the underlying expectations remain constant.

**Table 2: ALCOA+ Principles — Definitions and Regulatory Applications**

| Attribute | Definition | Regulatory Application |
|---|---|---|
| Attributable | All data must be traceable back to whoever performed the task or recorded the observation — with a clear time stamp | Audit trails, electronic signatures (21 CFR Part 11, EU GMP Annex 11) |
| Legible | Records must be permanently readable and free from ambiguity for as long as they are retained | Ink permanence standards, scan quality requirements, no correction fluid |
| Contemporaneous | Data must be captured at the moment the activity happens — recording it later is not acceptable | Backdating prevention; real-time timestamp verification |
| Original | The first recorded observation is the reference point; where transcription occurs it must be traceable to the source | Raw data retention policies; source data verification in clinical trials |
| Accurate | Data must honestly and completely reflect what was observed or measured | Calibration records, method validation, OOS investigation procedures |
| Complete (+) | All data — including repeat tests and results that failed — must be recorded without exception | Selective deletion classed as a critical GMP failure (MHRA 2018) |
| Consistent (+) | Records must follow a logical, unbroken sequence with dates and times that match the order of events | Timestamp auditing; sequence verification in audit trails |
| Enduring (+) | Data must be kept on stable media for the full required retention period without deterioration | 21 CFR 211.68 — electronic records carry the same legal weight as paper |
| Available (+) | Data must be retrievable whenever it is needed throughout the retention period | Disaster recovery, backup validation, archive retrieval procedures |

*Sources: FDA Guidance (2018)[1], MHRA Guidance (2018)[3], PIC/S PI-041-1 (2021)[5]*

### 2.3 Specific Requirements by GxP Context

Data integrity requirements reach their highest level of specificity in GMP environments. Analytical results, batch manufacturing records, environmental monitoring data, stability outcomes — all of these are subject to detailed expectations about how they are captured, reviewed, and retained. The FDA's 2018 guidance is explicit that audit trail review must be proportionate to risk and must be completed before batch release.[1,19] That last point is not always observed in practice, and it is a recurring inspection finding.

GLP settings are governed by the OECD Principles of GLP, which set equivalent expectations for raw data integrity in non-clinical safety studies. Clinical data integrity falls under ICH E6(R2) and the EMA's Reflection Paper on Source Data (2010).[33] The fact that similar principles apply across all three GxP contexts has prompted a growing argument — one this paper shares — that a unified data governance approach, applied consistently across the whole organisation, is more effective than maintaining separate compliance programmes for each context.

## 3. COMMON DATA INTEGRITY VIOLATIONS AND ENFORCEMENT TRENDS

### 3.1 Categories of Data Integrity Violations

A systematic review of FDA Warning Letters and Form 483 Observations from 2015 to 2022 yields a reasonably clear picture of where data integrity

failures cluster. Six main categories account for virtually all documented cases. Table 3 sets these out along with frequency estimates drawn from a focused analysis of 94 warning letters that explicitly named data integrity as a concern.[40]

**Table 3: Categories, Consequences, and Frequencies of Data Integrity Violations in Pharmaceutical Manufacturing (2015–2022)**

| Violation Category | Description / Example | Regulatory Consequence | Frequency (%)* |
|---|---|---|---|
| Audit Trail Manipulation | Deletion or modification of electronic records; system clock changes; shared login credentials | Warning Letter / Import Alert | 28% |
| Backdating / Pre-dating | Entries recorded before or after the actual event; falsified timestamps | 483 Observation / OAI | 22% |
| Selective Data Deletion | OOS results discarded; arbitrary re-testing without scientific rationale | Consent Decree | 19% |
| Inadequate Documentation | Incomplete batch records; missing OOS investigations; no audit trail review | 483 Observation | 17% |
| Unauthorised Data Access | Shared login credentials; absent access controls; ghost user accounts | Warning Letter | 8% |
| Data Migration Failures | Metadata lost during system upgrades; backup restoration never tested | 483 Observation | 6% |

**Estimated frequency based on analysis of 94 FDA Warning Letters (2015–2022). Source: Yadav and Mane (2023)*[40]

### 3.2 Audit Trail Manipulation

Audit trail manipulation is the single most commonly documented category, accounting for roughly 28% of cases. It takes several forms: unauthorised editing of electronic records, deliberate changes to system clocks to shift timestamps, and the use of shared login credentials that make it impossible to identify who actually did what.[19,40] The 2015 warning letter to Sun Pharmaceutical Industries is often cited as a textbook example — inspectors found that system clocks had been systematically altered to hide out-of-specification analytical results.[15] What makes this category particularly serious from a regulatory standpoint is that it strikes directly at the Attributable and Contemporaneous attributes of ALCOA+. Once the audit trail is compromised, the entire data set it was meant to protect becomes suspect.

### 3.3 Backdating and Pre-dating of Records

Backdating sits at the more serious end of the violation spectrum because it goes directly to the Contemporaneous principle — the requirement that data be recorded at the time the activity happens. Regulators draw a distinction between deliberate falsification and honest documentation mistakes, but both require investigation, both require corrective action, and both tend to attract scrutiny.[7,13] The most reliable technical defence is server-based timestamping that is locked from operator access. If the system clock cannot be changed by the person doing the work, backdating becomes much harder to achieve.

### 3.4 Selective Data Deletion

This is perhaps the most straightforward form of data manipulation to understand, and one of the hardest to detect when it is done carefully. Discarding out-of-specification results — whether by deleting injections from a chromatography sequence, failing to open required OOS investigations, or authorising re-testing without adequate scientific justification — violates both the Complete and Accurate attributes of

ALCOA+. The MHRA's 2018 guidance did not mince words: it characterised selective data deletion as a critical GMP failure, equivalent to outright data fraud.[3] Chromatographic data systems are particularly vulnerable because individual injections and entire sequence files can be deleted without leaving obvious traces if audit trail controls are inadequate.

## 4. IMPLEMENTATION CHALLENGES IN PHARMACEUTICAL ORGANISATIONS

### 4.1 Hybrid Paper-Electronic Systems

Walk through almost any pharmaceutical manufacturing facility today and you will find a mixed picture: some processes are fully electronic, others still rely on paper, and many sit somewhere in between. These hybrid arrangements are not inherently problematic, but they create specific data integrity risks wherever paper and electronic records interact. The most common flashpoint is manual transcription — when readings from electronic instruments are written onto paper batch records by hand.[13,22] Transcription errors are easy to introduce and hard to catch. Regulators require that original electronic data always be retained, that any transcription is independently verified, and that discrepancies between the electronic record and the paper record are investigated. In practice, these requirements are inconsistently met.

### 4.2 Legacy Computerised Systems

A significant proportion of the pharmaceutical industry still runs on legacy LIMS, chromatography data systems, and manufacturing execution systems that predate current data integrity expectations by a decade or more. These platforms often lack configurable audit trails. They may not support role-based access controls. They may not generate timestamped logs of user actions in a format that satisfies regulators.[11,37] Replacing them is expensive, time-consuming, and requires full system re-validation. For smaller organisations working with limited capital budgets, it can feel like an impossible ask — and in the meantime, they remain exposed to inspection findings that legacy systems make almost inevitable.

### 4.3 Supply Chain and Outsourcing Challenges

The pharmaceutical supply chain has become genuinely global, and that creates data integrity exposure at every link. When a company outsources quality control testing to a CRO, or contracts API synthesis to a CMO in a different country, it retains full regulatory responsibility for the data those organisations generate. An inspection finding at the CMO is a finding against the originating company.[14,27]

PIC/S PI-041-1 (2021) addresses this directly.[5] It requires contracts to specify data integrity obligations in detail, mandates that oversight audits are conducted, and insists that all data remains accessible to the principal company throughout the contract and after it ends. The difficulty is that actually delivering on these requirements across different time zones, languages, regulatory environments, and levels of quality culture maturity is enormously complicated. Audit programmes help, but they have limits.

### 4.4 Quality Culture Deficiencies

Systems and procedures matter, but the research literature is increasingly clear that culture is what makes the difference between an organisation that manages data integrity consistently and one that struggles with repeat findings. The pattern is recognisable: staff under pressure to hit release targets, management that either doesn't know or

doesn't want to know about documentation shortcuts, and a set of norms that gradually normalise practices that would fail any objective compliance review.[29,34] ICH Q10 names quality culture as a foundational element of an effective pharmaceutical quality system and is explicit that senior leadership must treat data integrity as a genuine organisational value.[9] That framing is right. The challenge is that culture cannot be created by writing a policy. It requires visible leadership behaviour, consistent messaging, and consequences — real ones — when data integrity is compromised.

## 5. TECHNOLOGICAL SOLUTIONS AND DIGITAL TRANSFORMATION

### 5.1 Overview of Enabling Technologies

The range of digital tools now available to pharmaceutical quality operations is genuinely broader than it has ever been. Some of what is being discussed — blockchain-based record-keeping, AI-driven anomaly detection — represents a real shift in what is technically possible. Other developments, such as improved audit trail functionality in modern chromatography platforms, are more incremental but no less valuable for that.[12,17] Table 4 provides a structured overview of the main enabling technologies, covering their specific applications to data integrity, where they currently stand regulatorily, and the practical obstacles that stand between a company and successful implementation.

**Table 4: Emerging Technologies for Pharmaceutical Data Integrity — Applications, Regulatory Status, and Implementation Challenges**

| Technology | Data Integrity Application | Regulatory Status | Implementation Challenges |
|---|---|---|---|
| Blockchain / DLT | Immutable audit trails; tamper-evident batch records; supply chain provenance | Emerging (FDA pilot 2022) | Scalability; integration with legacy LIMS |
| AI / Machine Learning | Anomaly detection in audit logs; predictive OOS flagging; automated review support | Accepted with validation (21 CFR 11) | Black-box risk; model drift; regulatory acceptance uncertainty |
| Cloud LIMS / ELN | Centralised data storage; version control; real-time access restrictions | Validated per Annex 11 / 21 CFR 11 | Data sovereignty; vendor lock-in; Part 11 compliance |
| Electronic Batch Records (eBR) | Automated data capture; no manual transcription; timestamped records at point of generation | Widely adopted (PAT guidance) | Change control complexity; training burden; upfront cost |
| Process Analytical Technology (PAT) | Real-time in-process monitoring; automated alerts; continuous data streams | Promoted by FDA PAT Guidance 2004 | High capital investment; method validation requirements |
| Digital Signatures (PKI) | Non-repudiation of approvals; audit trail integrity; 21 CFR Part 11 compliance | Required (21 CFR 11.50) | Certificate management; key rotation policy |

*Sources: Bhatt et al. (2022)[12], Jiang et al. (2022)[17], Krinke and Hartmann (2020)[35], FDA PAT Guidance (2004)*

### 5.2 Blockchain Technology

Blockchain's appeal as a data integrity tool comes from a specific structural feature: once a record is written to a distributed ledger with appropriate cryptographic controls, changing it retroactively becomes technically impractical. There is no single point of failure that an adversary — or a compliance-minded employee under pressure — can target.[12] The pharmaceutical applications that have attracted the most attention include immutable batch manufacturing records, supply

chain provenance tracking (particularly relevant given the challenge of multi-tier outsourcing), and certificate of analysis verification. The FDA's DSCSA pilot programmes, running between 2019 and 2022, moved blockchain traceability from a theoretical proposition to something that has been tested against real supply chain data. Scalability and integration with existing legacy systems remain the primary barriers to wider adoption.

### 5.3 Artificial Intelligence and Machine Learning

Audit trail review, done properly, is labour-intensive work. Modern pharmaceutical systems generate enormous volumes of records, and manually checking them for irregularities — especially when you do not know in advance what you are looking for — is both slow and prone to human error. Machine learning models trained on historical audit trail data can help. They can identify statistical patterns associated with known manipulation behaviours, flag anomalies for human review, and help prioritise which records deserve closer attention.[17,32]

The regulatory position on AI-based tools is cautiously accepting. Both the AAPS and the FDA have acknowledged the potential, but the conditions they attach are significant: rigorous validation, transparent model documentation, and evidence that the AI system does not itself introduce new risks to data integrity.[32] The black-box problem — the difficulty of explaining why a model flagged a particular record — remains a live regulatory concern, and one that vendors of AI-based quality tools have not fully resolved.

### 5.4 Electronic Batch Records and Cloud LIMS

Electronic batch records address what is, in practice, one of the most common sources of data integrity failure: the moment when a number generated by an instrument has to be written down by a person. eBR systems eliminate that step by capturing instrument readings automatically at the point of generation, applying timestamps, and feeding data directly into the batch record.[16,26] Cloud-based LIMS platforms extend this logic by providing centralised storage with comprehensive access controls, full version histories, continuously running audit trails, and disaster recovery capabilities that most legacy on-premise installations simply cannot match. Compliance with Annex 11 and 21 CFR Part 11 in cloud environments requires careful validation, but the tools to do it exist.

## 6. PROPOSED DATA GOVERNANCE FRAMEWORK

### 6.1 Framework Architecture

Any governance framework serious about data integrity has to tackle the problem from multiple directions at once. Technical controls alone will not fix a culture that tolerates shortcuts. Culture change without proper systems will not survive an inspection. A well-written policy without leadership commitment will sit on a shelf. The five-tier framework proposed here — grounded in ICH Q9 (risk management) and ICH Q10 (pharmaceutical quality system)[9,10] — attempts to address all of these dimensions in a way that is integrated rather than piecemeal (Figure 1).

**Figure 1: Proposed Five-Tier Data Governance Framework for Pharmaceutical Quality Assurance**

| Tier | Focus Area | Key Elements |
|---|---|---|
| TIER 1 | Leadership and Policy | Senior management commitment \| Data Governance Policy (DGP) \| Designated Data Integrity Officer |
| TIER 2 | Risk Management (ICH Q9) | Data flow mapping \| Risk assessment across all GxP systems \| Criticality classification of records |

| | | |
|---|---|---|
| TIER 3 | Technical Controls | Access control matrices \| Audit trail configuration \| System validation \| Backup and recovery |
| TIER 4 | Procedural Controls | SOPs for data review \| Change control \| Vendor oversight \| OOS investigation procedures |
| TIER 5 | Training and Culture | Annual DI training \| Competency assessment \| Open reporting culture \| Metrics and KPIs |

*Adapted from ICH Q10 (2008)[9] and ICH Q9(R1) (2023)[10]*

### 6.2 Data Governance Checklist

Table 5 translates the framework into a practical implementation checklist. Nine core governance elements are covered, each with a specific requirement, a priority level, and the relevant regulatory reference. It is intended as a working document rather than an audit tool — something a quality team can use to identify gaps and structure improvement activities.

**Table 5: Data Governance Implementation Checklist — Elements, Requirements, and Regulatory References**

| Governance Element | Implementation Requirement | Priority | ICH / FDA Ref. |
|---|---|---|---|
| Data Governance Policy | A written, formally approved policy that defines roles, responsibilities, and scope across all GxP data systems | Critical | ICH Q10 |
| Risk Assessment | Periodic data flow mapping; vulnerability scoring; criticality ranking of all relevant systems | Critical | ICH Q9 |
| Audit Trail Review | Regular, risk-proportionate audit trail review with formal documented evidence | Critical | 21 CFR 211.68 |
| Access Control & Security | Role-based access; unique user IDs; regular access reviews; multi-factor authentication | Critical | Annex 11/4.3 |
| Training Programme | Data integrity training at onboarding and annually; formal competency assessment | High | ICH Q10 |
| Change Control | Formal change control covering systems, processes, and data migration activities | High | 21 CFR 211.100 |
| Backup & Recovery Validation | Periodic tested restoration; off-site storage; validated backup integrity checks | High | Annex 11/7.1 |
| Vendor Management | CRO/CMO qualification; contractual data integrity obligations; ongoing audit programme | Medium | ICH Q7 |
| Metrics & KPIs | Monthly DI metrics dashboard; OOS trend analysis; repeat deviation tracking | Medium | ICH Q10 |

*Sources: ICH Q9(R1) (2023)[10], ICH Q10 (2008)[9], 21 CFR 211.68, EU GMP Annex 11[2]*

### 6.3 Audit Trail Review Protocol

Both the MHRA (2018) and PIC/S (2021) set out clear expectations for audit trail review: it must be periodic, proportionate to risk, performed by someone who is not the analyst who generated the data, and formally documented as part of the batch release or study sign-off process.[3,5] Figure 2 sets out a step-by-step workflow that translates these requirements into a laboratory-level process. The five steps cover scope definition, audit trail configuration and validation, report generation, independent review, and formal documentation — including escalation pathways for critical findings.

**Figure 2: Audit Trail Review Workflow for GMP Laboratory Computerised Systems**

| Step | Action | Key Considerations |
|---|---|---|
| Step 1: Define Scope | List all GxP computerised systems; classify each by criticality (High / Medium / Low); set review frequency based on that classification | Risk-based classification per ICH Q9 |
| Step 2: Configure Audit Trail | Switch on logging for user actions, system events, and any data changes; lock server time; validate the configuration through IQ/OQ/PQ | Settings must be tamper-evident throughout |
| Step 3: Generate Report | Produce audit trail reports — automated where possible — covering the full review period with no events excluded | Output must be unfiltered and complete |
| Step 4: Independent Review | A qualified reviewer checks for anomalies, deletions, inconsistent timestamps, and shared login use — this person must be separate from the analyst who generated the data | Independence of the reviewer is non-negotiable |
| Step 5: Document and Escalate | Record the outcome of the review formally; open deviations for any findings; escalate critical issues to QA management without delay | The review itself must leave a documented audit trail |

*Adapted from MHRA (2018)[3] and PIC/S PI-041-1 (2021)[5]*

## 7. FUTURE PERSPECTIVES

### 7.1 Regulatory Harmonisation

The gap between different national regulatory frameworks is a real compliance burden for manufacturers operating across multiple markets. The FDA and EU Annex 11 systems diverge on questions that matter in practice: what exactly constitutes 'raw data,' how often audit trails need to be reviewed, whether a printed copy can ever serve as a GMP record.[1,2,5] These are not trivial differences. They force globally operating companies to maintain parallel compliance programmes in a way that adds cost without improving data quality. A more harmonised international standard — perhaps developed through ICH, where the institutional structures for this kind of work already exist — would be worthwhile for both industry and regulators, and it would almost certainly improve overall standards.

### 7.2 Adaptive Regulatory Frameworks for Digital Technologies

One tension that runs through the current regulatory landscape is between the pace of digital innovation and the pace at which guidance can be developed, consulted on, and issued. Cloud computing, AI, blockchain, and IoT-enabled continuous manufacturing are already being deployed in GxP environments — often in the absence of dedicated regulatory frameworks to guide their implementation.[32,35,37] The FDA's Digital Health Center of Excellence and the EMA's digital transformation programme are signs that the agencies understand this gap. The likely trajectory for future frameworks is away from prescriptive, technology-specific rules and towards principle-based requirements that specify what outcomes need to be achieved and leave organisations more latitude in determining how to achieve them.

### 7.3 Continuous Manufacturing and Real-Time Data Integrity

The move from batch to continuous pharmaceutical manufacturing — encouraged by the FDA's PAT guidance and now with dedicated treatment in ICH Q13 — changes the data integrity problem in fundamental ways.[24] A continuous process generates data without interruption. There is no natural batch end-point at which records are reviewed and released; instead, integrity assurance has to be built into the process itself, at the sensor

level, with validated data acquisition pipelines, tamper-evident monitoring systems, and direct links to automated disposition decisions. The regulatory frameworks for batch manufacturing data integrity do not map cleanly onto this environment, and developing fit-for-purpose approaches remains work in progress.

### 7.4 Strengthening Quality Culture as a Sustainable Control

The evidence from enforcement history is consistent: organisations that maintain robust data integrity over time share cultural characteristics that go beyond good systems and procedures. Leaders who are visibly committed to data quality, not just verbally but in the decisions they make when data integrity conflicts with production schedules. An environment in which staff feel safe reporting anomalies without fear of blame. Quality metrics that are taken seriously at the most senior level. These things are harder to audit than a validated system, but they are also more durable.[29,34] The long-term answer to pharmaceutical data integrity problems is probably more cultural than technical — and that means thinking about how these values are instilled, starting with undergraduate and postgraduate pharmaceutical education.

## 8. CONCLUSION

Data integrity is not a regulatory technicality. It is the basis on which every consequential decision in pharmaceutical quality assurance depends — batch release, regulatory submission, ultimately patient safety. When it fails, everything built on top of it becomes unreliable. This review has tried to show that while the regulatory landscape has developed substantially — with converging frameworks from the FDA, EMA, MHRA, WHO, and PIC/S now establishing broadly consistent expectations — the gap between those expectations and what industry actually delivers remains wide, particularly in developing markets and smaller organisations.[1,3,5]

The ALCOA+ framework gives the industry a common language and a common standard. The enforcement record confirms that the most common failures are not exotic or technically complex — audit trail manipulation, backdating, selective deletion of inconvenient results — and that the same violations keep recurring across organisations and geographies. Emerging technologies offer genuine improvements: blockchain can make retrospective manipulation technically impractical, AI can make audit trail review faster and more sensitive, electronic batch records can eliminate the transcription step that introduces so much risk. But all of these tools require careful implementation within change-controlled, validated frameworks, and none of them substitutes for a quality culture that treats data integrity as something that actually matters.[12,17,24]

The five-tier governance framework put forward here is designed to address the problem at all levels simultaneously — leadership commitment, risk-based controls, technical safeguards, procedural standards, and the cultural foundations that make written policies stick.[9,10] Making real progress from this point will require regulatory frameworks to catch up with digital innovation more quickly than they currently do, greater harmonisation across national systems, and a sustained commitment from organisations to treat data integrity as a professional and ethical obligation rather than a compliance exercise.

## REFERENCES

1. FDA Guidance for Industry. Data Integrity and Compliance with Drug CGMP. U.S.

Department of Health and Human Services; 2018.
2. European Medicines Agency. EU Guidelines for Good Manufacturing Practice for Medicinal Products for Human and Veterinary Use, Annex 11: Computerised Systems. EMA; 2011.
3. MHRA. GXP Data Integrity Guidance and Definitions. Medicines and Healthcare products Regulatory Agency; 2018.
4. WHO. Guidance on Good Data and Record Management Practices. WHO Technical Report Series No. 996, Annex 5. World Health Organization; 2016.
5. PIC/S. Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments. PI-041-1. Pharmaceutical Inspection Co-operation Scheme; 2021.
6. Holm T, Loennechen T. Data integrity requirements in the pharmaceutical industry. J Pharm Biomed Anal. 2019;175:112779.
7. Raman NV, Harikumar SL. Data integrity in pharmaceutical quality systems. Int J Pharm Sci Rev Res. 2020;62(1):115-122.
8. Liebler JM, McConnell ML. A Practical Guide to FDA's Food and Drug Law and Regulation. 5th ed. Washington DC: Food and Drug Law Institute; 2018.
9. ICH Harmonised Tripartite Guideline. Pharmaceutical Quality System Q10. International Conference on Harmonisation; 2008.
10. ICH Harmonised Guideline. Quality Risk Management Q9(R1). International Council for Harmonisation; 2023.
11. Kovacs E, Somogyi J, Kocsis B. Electronic data integrity in GMP-regulated environments: challenges and solutions. Pharm Dev Technol. 2021;26(5):549-558.
12. Bhatt P, Kambli S, Desai N. Blockchain technology as a tool for pharmaceutical data integrity. J Drug Deliv Sci Technol. 2022;72:103326.
13. Sandle T. Data integrity in the pharmaceutical and biotech industries -- a GMP perspective. Am Pharm Rev. 2019;22(4):14-20.
14. Calnan N, O'Sullivan A. Managing data integrity in outsourced environments. Eur J Pharm Sci. 2021;160:105754.
15. FDA. Warning Letter: Sun Pharmaceutical Industries. FDA Warning Letter Database. U.S. FDA; 2015.
16. Desai A, Shah RB. Electronic laboratory notebooks and their role in GMP environments. J Pharm Sci. 2020;109(12):3499-3506.
17. Jiang H, Shen YL, Liu Q et al. Application of artificial intelligence in pharmaceutical data integrity management. J Pharm Innov. 2022;17(3):840-851.
18. Patel JP, Patil ND. Data governance framework for pharmaceutical companies: a systematic approach. IJPSR. 2021;12(8):4123-4135.
19. Nanda S, Arora M. Audit trail management in pharmaceutical industry: regulatory overview and best practices. Int J Pharm Qual Assur. 2020;11(4):682-689.
20. European Commission. EU GMP Chapter 4: Documentation. European Commission; 2011 (Rev. 2014).
21. Siegfried A, Moreira IP. Data integrity compliance in computerised systems in pharmaceutical industry. J Pharm Sci Innov. 2021;10(6):371-379.
22. Ramaiah M, Narasimha Rao P. Challenges and remediation strategies for data integrity in Indian pharmaceutical companies. IJPSR. 2022;13(3):1052-1063.
23. Hubbard DW. How to Measure Anything: Finding the Value of Intangibles in Business. 3rd ed. Hoboken NJ: Wiley; 2014.

24. Seer LA. Process Analytical Technology: Enabling Data Integrity Through Continuous Verification. J Pharm Technol. 2020;36(4):195-204.
25. Chen B, Wang Y, Zhang H. Risk-based approach to data integrity in clinical trial data management. Clin Trials. 2021;18(2):161-170.
26. Kim S, Park J. Implementation of electronic batch record systems in Korean pharmaceutical manufacturing. J Pharm Sci. 2020;109(5):1733-1740.
27. Frey KA, Lam AM. Data integrity in contract manufacturing organisations: regulatory expectations. Pharm Technol. 2021;45(8):28-33.
28. Burgess K. Quality Management Systems for the Food Industries. 2nd ed. London: Springer; 2019.
29. Smith G, Alpert O. The role of quality culture in sustaining pharmaceutical data integrity. PDA J Pharm Sci Technol. 2020;74(1):30-40.
30. Sorger PK, Altman RB. Cells, Knowledge and Future Medicine. Sci Transl Med. 2018;10(467):eaau2485.
31. Bansal RK, Gupta PK. Implementation of ICH Q10 pharmaceutical quality system for data integrity. Indian J Pharm Sci. 2020;82(2):332-340.
32. Abuhelwa AY, Williams DB, Foster DJ. Regulatory perspectives on machine learning in pharmaceutical quality. AAPS J. 2022;24(2):38.
33. European Medicines Agency. EMA Reflection Paper on Expectations for Electronic Source Data and Data Transcription to Electronic Data Collection Tools in Clinical Trials. EMA; 2010.
34. Hussain AS. The data integrity crisis: implications for pharmaceutical development and regulation. J Pharm Sci. 2019;108(1):56-60.
35. Krinke B, Hartmann A. Cloud computing in pharmaceutical environments: compliance with GxP requirements. Pharm Ind. 2020;82(11):1476-1483.
36. Lachman L, Lieberman HA, Kanig JL. The Theory and Practice of Industrial Pharmacy. 3rd ed. Philadelphia: Lea & Febiger; 1986.
37. Schnieders J, Singh R. GMP requirements for digital transformation: bridging legacy systems and modern data integrity. ISPE Pharmaceutical Engineering. 2021;41(6):20-28.
38. Tran DT, Nguyen TV. Assessment of data integrity in Vietnamese pharmaceutical manufacturing. Asian J Pharm. 2022;16(4):451-459.
39. Wawrzyniak MJ. Data integrity in pharmaceutical quality control laboratories: a practical review. Lab Med. 2021;52(5):e71-e79.
40. Yadav S, Mane PP. Regulatory inspections and data integrity deficiencies: analysis of FDA warning letters 2015-2022. Regul Toxicol Pharmacol. 2023;130:105131.

HOW TO CITE: Avinash Sapkale, Dr. Amit Kasabe, Rehan Sayyad, Data Integrity in Pharmaceutical Quality Assurance: Regulatory Requirements, Challenges and Future Perspectives, Int. J. of Pharm. Sci., 2026, Vol 4, Issue 6, 6234-6246. https://doi.org/10.5281/zenodo.20839303