



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Data Integrity In Pharmaceutical Quality Assurance: Implementation Of ALCOA+ Principles, Regulatory Challenges, And Future Perspectives

Firdos Inayat Ali Sayyed^{1*}

A.M. Ansari¹

Abstract:

Data integrity is a key part of making sure medicines are safe and work as they should. Important decisions about what a medicine is, how strong it is, how clean it is, how good it is, how safe it is, and how well it works all rely on the data collected during the whole life of the product. The more pharmaceutical companies use digital tools in development, production, quality checks, and supply chain management, the more they can track processes and control them better. However, this also brings new dangers like problems with computer systems, electronic records, data metadata, audit trails, data sharing, cybersecurity threats, the use of artificial intelligence, and reliance on outside service providers. The ALCOA+ framework—Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, and Available—offers a helpful way to make sure that important data used in regulated areas stay reliable from the time they are created until they are no longer needed.

This review looks at how the ALCOA+ principles are used in making sure pharmaceutical products are of high quality. It covers how these principles are applied in paper-based, electronic, and mixed environments. The review also discusses the rules and standards set by important authorities and international groups, including those in the U.S. Food and Drug Administration (FDA), Medicines and Healthcare products Regulatory Agency (MHRA), European Union (EU), Pharmaceutical Inspection Co-operation Scheme (PIC/S), World Health Organisation (WHO), and the regulatory bodies in India. Special care is taken with data governance, making sure computer systems are properly validated, managing audit trails, controlling who has access, using electronic signatures, handling data throughout its life, managing quality risks, training staff, and building a strong organizational culture. Major regulatory and operational challenges Big challenges in rules and how things work include old computer systems, messy spreadsheets that aren't controlled, mixed types of records, not checking the audit trail well, giving people too much access, missing or deleting data, not keeping good backups and records, using outside companies for some tasks, weak security for cyber threats, and not enough supervision from leaders.

The review also looks at new technologies like artificial intelligence, machine learning, cloud computing, continuous manufacturing, digital twins, advanced analytics, and automated data-integrity monitoring. Even though these technologies can help track things better and find problems more easily, they also bring up more needs for checking their accuracy, managing how they are used, keeping them safe from hackers, having people watch over them, and handling them through their whole life cycle. The future of pharmaceutical data integrity will probably shift from checking compliance at certain times to using

ongoing, risk-focused, and technology-supported data management. Sustainable implementation needs to include the ALCOA+ principles in the pharmaceutical quality system, quality risk management, computerized system lifecycle management, supplier governance, CAPA, management reviews, and building a strong quality culture. Data integrity must be seen not just as something required by rules, but as something essential for making decisions that are scientifically sound and for keeping patients safe.

Keywords:

Data integrity; ALCOA+; pharmaceutical quality assurance; data governance; GMP; computerized systems; audit trail; quality risk management; electronic records; regulatory compliance; artificial intelligence.

1. Introduction

The pharmaceutical industry relies on data throughout every step of the product's life. Development studies, analytical testing, process validation, environmental monitoring, manufacturing operations, stability studies, quality control, batch release, handling complaints, dealing with deviations, conducting investigations, taking corrective and preventive actions (CAPA), and submitting to regulatory authorities all depend on data to back up scientific and quality decisions. So, the trustworthiness of medicines depends entirely on how reliable the information is that is used to check them.

Data integrity is now a major concern for regulations and quality control because authorities have found problems like missing records, wrong changes to data, poor tracking of data activities, people accessing data without permission, not keeping the original data, and weak computer systems. The U.S. The Food and Drug Administration (FDA) says that all the information used to make decisions about making drugs and ensuring their quality must be trustworthy and correct. They also suggest clear, useful, and smart approaches based on risk to stop and find issues with the accuracy of data.[1]

The concept extends beyond preventing intentional falsification. Data integrity means having the right steps in place to make sure information stays reliable from the time it is first created until the end, like when it's used, changed, shared, saved, found again, kept for later, or finally removed. The FDA's lab control rules also say that data from GMP activities, whether it passes, fails, is questionable, or is wrong, should be kept and properly checked instead of being picked out or ignored.[2]

The increasing use of laboratory information management systems, chromatography data systems, electronic batch records, manufacturing execution systems, enterprise resource planning systems, cloud-based platforms, remote access, connected equipment, and automated decision-support tools has made the pharmaceutical data environment more complicated over time. Electronic records can include more than just the final result; they might also have the original data, extra details about the data, records of who did what and when, the steps used, mathematical work, settings used in the system, and other related information that gives more background. So, just keeping a printed or handwritten copy might not save the whole original record.

The ALCOA principles were created as a way to clearly show the basic requirements for having reliable and trustworthy records. The updated ALCOA+ framework includes the qualities of completeness, consistency, endurance, and availability. MHRA clearly explains that ALCOA stands for Attributable, Legible, Contemporaneous, Original, and Accurate. The "+" in ALCOA stands for Complete, Consistent, Enduring, and Available. It's important to note that the MHRA says the basic expectations stay the same whether you use the acronym ALCOA or ALCOA+.[3]

This review aims to closely look at how the ALCOA+ principles are applied in pharmaceutical quality control, check the rules and real-world difficulties related to data accuracy, and talk about how new technologies can help improve data management in the future.

2. Review Methodology

This review was created by looking at stories, rules, and scientific papers.

The main sources of information were official guidelines and standards released by the FDA, MHRA, European Commission, PIC/S, WHO, and the International Council for Harmonisation (ICH). Relevant pharmaceutical data-integrity literature was found using PubMed and other scientific and professional journal databases by combining several key terms.

“data integrity,” “ALCOA,” “ALCOA+,” “pharmaceutical quality assurance,” “GMP,” “audit trail,” “computerised systems,” “data governance,” “electronic records,” “quality risk management,” and “pharmaceutical manufacturing.”

Priority was given to existing or official regulatory documents, and then to peer-reviewed articles that discuss the history, how these issues were handled, how regulations were understood, and ways to fix problems with pharmaceutical data integrity. Rattan's review gives a key look at the history of data integrity in pharmaceuticals and how regulations have developed over time, while Shafiei et al. looked at the regulatory steps taken and how human mistakes contribute to data integrity problems.[4,5]

Because rules and guidelines are updated from time to time, the current regulatory status was checked separately from any new or planned requirements. This review treats the European Commission's 2025 consultation on changes to EU GMP Chapter 4, Annex 11, and the proposed new Annex 22 on artificial intelligence as an emerging regulatory trend, not as a rule that is already in effect.[6]

3. Concept of Pharmaceutical Data Integrity

3.1 Definition

Data integrity means how well data stays full, correct, dependable, and true from the time it is created until it is no longer needed.

The term should be different from data quality and data security.

Data quality checks if the data is right, has no missing parts, and works well for the job it's meant to do.

Data security is about keeping information safe from people who shouldn't have access, preventing it from getting lost, damaged, or changed without permission.

Data integrity includes these points but also means being sure that the data correctly show the real activity or observation they came from.

So, even if a database is very secure, it might still have problems with data integrity if people can change records in the wrong way, if information about the data is missing, if there's no record of who did what, or if some of the original data isn't included.

Data integrity covers more than just information technology. The MHRA has pointed out that risks related to how data is managed can happen in paper, electronic, and mixed environments, and they can occur at every stage of how data is handled.[3]

3.2 Data Lifecycle

A pharmaceutical data lifecycle can be shown as:

Data is created, then it is recorded, followed by processing, then it goes through a review, gets approved, is reported, stored, retrieved when needed, kept in archives, and finally disposed of properly.

Controls should be established at each stage.

For example, laboratory chromatographic data can go through several steps, starting with receiving and preparing the sample, then using the instrument to get the data, processing that data, having the analyst

check it, going through a quality control check, creating a report, and finally storing the data for future use. If something goes wrong at any step, it can affect how reliable the final quality decision is.

Data integrity needs to be handled throughout its entire life cycle, not just as a separate task done once.

4. ALCOA+ Principles

ALCOA+ is a real-world approach used to create and check data-governance controls. It should not replace the proper GMP rules, but instead act as a way to show that the data is reliable.

4.1 Attributable

Data should be linked back to the person or system that created, changed, checked, or gave approval to it.

In paper systems, people usually assign credit by using properly managed signatures, initials, dates, and other ways to identify who did something. In electronic systems, having unique user accounts, electronic signatures, authentication checks, and audit records are key ways to ensure security and track activity.

Shared user accounts are a big problem because they make it hard to know who is responsible for what, and they can stop people from figuring out who did something.

Implementation controls include:

- unique user identification;
- role-based access;
- controlled privileges;
- electronic signatures;
- password and authentication controls;
- segregation of duties; and
- periodic review of user access.

The MHRA stresses that the person who fills out a record must be clearly identified.[7]

4.2 Legible

Data needs to stay clear and easy to understand for the whole time it is required to be kept.

For paper records, the entries need to be permanent, easy to read, and clearly written. For electronic records, legibility means being able to get and understand the information, along with any related metadata and other connected records.

A database that can still be accessed technically but cannot be properly understood because the related software, metadata, or system information is missing may not achieve the real goal of keeping data intact.

4.3 Contemporaneous

Data should be written down when the activity happens.

Making recordings at the same time as events happen lessens the need to remember things and cuts down on chances for someone to create a story or do things that weren't properly documented in between.

Examples of non-contemporaneous practices include:

completing equipment logbooks retrospectively;

After the testing is done, enter the laboratory observations.

reconstructing manufacturing records from memory;

Instead of taking notes on environmental conditions when you see them, wait until the end of your shift to record the results.

Electronic systems can help record things at the same time using automatic time stamps, but having automatic time stamps alone doesn't make sure everything is done correctly. System time settings, user login checks, records of who did what, and rules for managing tasks must all be properly managed.

4.4 Original

The original record or a properly checked true copy needs to be kept.

In electronic settings, the original record can have much more information than what is shown in the final printed version. For example, analytical raw data may include:

- instrument acquisition data;
- sample sequence;
- analytical method;
- integration parameters;
- processing methods;
- system suitability information;
- metadata;
- audit-trail information; and
- associated calculations.

The FDA's rules about lab control highlight the need to keep all lab data, not just the final result that gets reported.[2]

4.5 Accurate

Data should accurately show the observation, measurement, or activity that is being recorded.

Accuracy depends on:

- qualified personnel;
- calibrated equipment;
- validated analytical methods;
- controlled calculations;
- appropriate data-entry controls;
- suitable system configuration; and
- effective review.

Accuracy is something that both the data and the system used to create and handle that data should have.

4.6 Complete

Complete data contains all the information needed to rebuild and fully understand the related activity.

Completeness includes appropriate retention of:

- original records;
- raw data;
- metadata;
- audit trails;
- failed results;
- atypical results;

- repeat analyses;
- calculations;
- relevant system information; and
- associated documentation.

The FDA clearly says that all lab results, like mistakes and data that passes, fails, or is questionable, must be part of the CGMP records and checked properly.[2]

Therefore, removing or ignoring a result that you don't like just because it's troublesome is not true to the idea of keeping data accurate and reliable.

4.7 Consistent

Data needs to be written down in a clear and time-based order.

For example, the sequence of:

Sample preparation, analysis, review, approval, and reporting.

should be consistent with the actual activity.

Inconsistent time stamps, missing explanations for gaps, conflicting information, or differences between paper and digital records might show problems in how data is handled throughout its life.

4.8 Enduring

Data needs to stay saved and accessible for the whole time it is required to be kept.

Endurance requires consideration of:

- storage media;
- environmental conditions;
- backup;
- disaster recovery;
- archival;
- system migration;
- software obsolescence;
- metadata preservation; and
- long-term accessibility.

When a computer system is no longer used, the organization still has to keep the records that were created while the system was working.

4.9 Available

Data needs to be easy to find for people who are allowed to access it, for checking quality, doing audits, looking into issues, and for regulatory inspections.

Availability requires more than maintaining a backup.

Organizations should show that records are really able to:

- retrieved;
- interpreted;
- associated with the correct context;

- presented in a readable form; and
- made available to authorized reviewers and inspectors.

5. Implementation of ALCOA+ in Pharmaceutical Quality Assurance

5.1 Data Governance

Data governance is the system that helps an organization set up who is responsible for data, who owns it, how it should be controlled, the standards it must follow, and who makes the important decisions about it.

A pharmaceutical data-governance program should identify:

- critical data;
- data owners;
- data stewards;
- data-generating systems;
- data flows;
- interfaces;
- applicable retention periods;
- data criticality;
- integrity risks;
- access requirements; and
- control mechanisms.

The MHRA sees data governance as a key part of having a compliant GxP system and uses this idea throughout the whole life of a pharmaceutical product.[3]

5.2 Data Criticality and Quality Risk Management

Not all data have identical regulatory significance.

Data that plays a key role in deciding whether a batch is released or if patient safety is at risk is usually more important than data that only slightly affects the quality of the product.

Data integrity risk can therefore be assessed based on:

potential impact on product quality;

- impact on patient safety;
- regulatory significance;
- likelihood of unauthorized alteration;
- opportunity for detection;
- complexity of the process;
- degree of automation;
- data lifecycle duration; and
- dependence on external providers.

ICH Q9 offers a structured way to manage quality risks, and ICH Q10 sets up the pharmaceutical quality system where risk management and ongoing improvements are part of the process.[8,9]

A risk-based approach stops organizations from using the same controls for all data and lets them focus their efforts on the processes that are most likely to cause problems.

5.3 Computerized System Validation

Computer systems that are used to create, change, handle, save, or share data that follows Good Manufacturing Practices need to be properly managed at every stage of their life.

Important lifecycle activities include:

User needs are first understood and turned into a system design. Then, possible risks are checked and managed. The system is tested to make sure it works properly. Once it's ready, it's used in real situations. Changes to the system are carefully controlled. The system is regularly checked to ensure it keeps working well. Eventually, the system is taken out of use and replaced.

EU GMP Annex 11 talks about computerised systems and sets out what is expected regarding validation, keeping data secure, tracking changes with audit trails, using electronic signatures, and controlling the system.[10]

The FDA's rules also need proper controls for computer systems used in CGMP operations. The FDA's data integrity guidance says companies should use real and good risk-based controls that are based on how their processes work, the technology they use, and their business models.[1]

Validation should therefore show that the software works properly and that the computerised system is suitable for its intended GMP purpose and properly protects important data.

6. Audit Trails and Data Review

Audit trails are a key technical measure that helps keep electronic data accurate and trustworthy.

An audit trail should allow you to recreate important activities, including the right details about:

who performed the activity;

- what was changed;
- when it occurred;
- previous and subsequent values where applicable;
- reasons for changes where required; and
- relevant system events.

Just having an audit trail doesn't mean the data is accurate or reliable.

A system might work well with a technically functional audit trail, but the organisation could still fail to:

activate it;

restrict its modification;

review it;

define review frequency;

investigate anomalies; or

retain it with the associated record.

Risk-based audit-trail review plays a key role in ensuring good data governance.

7. Paper, Electronic, and Hybrid Systems

7.1 Paper-Based Records

Paper systems remain relevant in pharmaceutical manufacturing.

Common integrity risks include:

- undocumented corrections;
- use of pencil or erasable ink;
- missing dates;
- unclear initials;
- retrospective completion;
- uncontrolled blank forms;
- transcription errors;
- uncontrolled copies; and
- inappropriate destruction of original records.

Good documentation practices should be based on the same basic data-integrity rules that are used for electronic systems.

7.2 Electronic Systems

Electronic systems introduce additional risks, including:

- shared accounts;
- excessive privileges;
- data deletion;
- uncontrolled configuration;
- inadequate audit trails;
- inappropriate data reprocessing;
- insecure interfaces;
- unvalidated spreadsheets;
- software obsolescence;
- inadequate backup; and
- cybersecurity vulnerabilities.

Moving from paper to electronic systems doesn't remove the risk of data integrity; it just changes how that risk appears.

7.3 Hybrid Systems

Hybrid systems are tough because the organization needs to figure out how paper records and electronic records relate to each other.

For example, a lab might write down the final result on paper, but the machine keeps the original electronic data. If the organisation doesn't clearly identify which records are part of the original data set and how they are matched up, important information could be missed.

The MHRA clearly states that paper, electronic, and hybrid systems can all be sources of data integrity issues.[3]

8. Data Integrity in Pharmaceutical Quality Control Laboratories

Quality control labs are one of the busiest areas in pharmaceutical production when it comes to handling a lot of data.

Common systems include:

- HPLC/UPLC;
- GC;
- UV-visible spectroscopy;
- dissolution testing;
- Karl Fischer titration;
- TOC analysis;
- microbiological testing;
- stability systems;
- LIMS; and
- laboratory instrument software.

Laboratory data-integrity risks may involve:

- unofficial trial injections;
- deletion of failing chromatograms;
- inappropriate reintegration;
- manipulation of analytical sequences;
- repeated testing without documented justification;
- inadequate audit-trail review;
- inappropriate use of shared accounts;
- incomplete metadata;
- uncontrolled processing methods; and
- failure to retain original electronic data.

The FDA clearly says that using product samples for unofficial tests, like trial injections, is not allowed. They also stress that any data from product testing should be kept and checked carefully.[2]

This shows that keeping data accurate needs to be part of all lab work, handling unexpected results, managing how tests are done, making sure equipment is set up right, and running the lab smoothly.

9. Data Integrity in Manufacturing

Data integrity is not just something that happens in the lab.

Manufacturing data may include:

- batch manufacturing records;
- batch packaging records;
- equipment logs;
- cleaning records;
- environmental monitoring;
- in-process controls;
- weighing and dispensing records;
- process parameters;
- temperature and humidity data;
- maintenance records;
- calibration records;
- electronic batch records; and
- manufacturing execution-system data.

Possible problems could be writing records after the fact, changing processes without keeping notes, adjusting settings in a way that's not clear, not fully documenting equipment use, and differences between digital and physical records.

Therefore, a complete program to ensure data accuracy needs to cover every step of the manufacturing process.

10. Regulatory Framework

10.1 United States FDA

The FDA's 2018 Data Integrity and Compliance With Drug CGMP: Questions and Answers is still a main guide used by the U.S. for ensuring proper data handling in drug manufacturing. The FDA states that data must be trustworthy and correct, and that companies should use strong and practical plans based on risk to stop and find issues with data quality.[1]

The framework works together with 21 CFR Parts 210 and 211, and when needed, also follows 21 CFR Part 11 for electronic records and electronic signatures.

The FDA's lab control Q&A highlights the need to fully keep and check all lab data, including data that doesn't meet standards and data that might be questionable.[2]

The U.S. approach treats data integrity as part of the existing CGMP rules instead of requiring it as a separate compliance task.

10.2 European Union

EU GMP rules cover the use of computer systems and how documents are handled, especially when it comes to making sure data is accurate and trustworthy.

Annex 11 talks about computerized systems and includes controls related to:

- validation;
- data storage;
- accuracy checks;
- audit trails;
- change control;
- periodic evaluation;
- security;
- electronic signatures;
- business continuity; and
- archiving.[10]

The European Commission's present EudraLex Volume 4 covers Chapter 1 about the Pharmaceutical Quality System and Chapter 4 on Documentation, along with Annex 11 which deals with computerized systems.[11]

Emerging EU regulatory direction

In 2025, the European Commission asked experts and other interested parties for their input on changes to Chapter 4, Annex 11, and a new Annex 22 related to artificial intelligence.

The proposed revisions place greater emphasis on:

- lifecycle management of computerized systems;
- quality risk management;
- supplier oversight;
- data integrity;
- audit trails;
- electronic signatures;
- security;
- hybrid documentation; and
- AI model governance.

The new Annex 22 would cover AI and machine learning systems used in making drugs. It would look at things like what the systems are meant to do, the data they are trained on, how they are checked to work properly, how their performance is tracked, how changes to the systems are managed, and how people review their use. These documents should be seen right now as suggested regulatory changes, not as fully accepted GMP standards.[6]

10.3 United Kingdom: MHRA

The MHRA's GxP Data Integrity Guidance and Definitions outlines specific requirements for managing data properly in GxP settings. This guidance is for companies that work in the pharmaceutical industry and covers issues found during inspections.[3]

One key part of the MHRA's method is understanding that the risk to data integrity comes from:

- data criticality;
- opportunities for data alteration or deletion;
- detectability;
- process complexity;
- paper systems;

- electronic systems; and
- hybrid systems.

The MHRA clearly explains the ALCOA+ framework and highlights that data governance must ensure data is complete, consistent, enduring, and available throughout its entire life cycle.[3]

10.4 PIC/S

The PIC/S guidance document PI 041-1 outlines best practices for managing data and ensuring its integrity in regulated GMP and GDP environments, with a focus on how inspections should be conducted. It started working on 1 July 2021.[12]

This guidance is important for multinational pharmaceutical companies because it helps ensure that inspection standards are more consistent among the different regulatory agencies involved.

10.5 World Health Organization

A specific guideline on data integrity was adopted by WHO as part of its system to ensure the quality of pharmaceutical products. The WHO guideline was included as Annex 4 in Technical Report Series 1033 in 2021.[13]

The guideline was later added to the guidance documents approved by the WHO Expert Committee on Specifications for Pharmaceutical Preparations in TRS 1044.[14]

WHO's approach supports the idea that having accurate data is key for making good quality decisions and managing medicines properly.

10.6 India: CDSCO and Revised Schedule M

India's pharmaceutical regulatory environment is especially important because Indian manufacturers provide medicines to both their own country and strict international markets.

In 2023, a new version of the Schedule M framework was introduced, which made India's GMP system stronger and brought it closer to international GMP standards. Data governance needs to be looked at along with other important parts of pharmaceutical quality systems, like documentation, validation, risk management, and computerized processes.

For Indian manufacturers who sell products in international markets that are regulated, compliance should not be considered only based on what is required at home. Companies need to create data management systems that can meet the requirements set by CDSCO and the rules of the countries where their products are sold.

Because there have been recent changes in the regulations related to Schedule M and the Indian guidelines, companies need to check the latest official notices, transition rules, and guidance from CDSCO when creating their specific compliance plans for each site.

11. Comparative Regulatory Perspective

Area FDA EU MHRA PIC/S WHO

Data integrity means making sure that data is accurate, reliable, and trustworthy. Risk-based CGMP expectations are part of Good Manufacturing Practice and Quality System requirements, and they are included in computerized system controls. There are specific guidelines for data integrity related to GxP, data management, and data integrity itself.

ALCOA+ characteristics are discussed in the context of documentation and computerized system requirements. The terms related to ALCOA+ are clearly stated. The principles of data integrity are also covered.

Audit trails should be in place whenever it's needed for electronic records, as required by Annex 11. There is a strong focus on this requirement. It is also a key part of the data-governance framework.

Computerized systems should follow CGMP and Part 11 rules when needed. Annex 11 covers these rules. GxP data-governance controls are also important. GMP and GDP data-integrity controls must be in place. Computerized-system and data-governance controls are required.

Risk management involves creating a data-integrity plan that is based on risk. This is done through an integrated quality risk management approach. It considers how important the data is and the risks that naturally come with it. A risk-based inspection system is also used, along with a quality approach that is guided by risk assessment.

Organizational culture Management responsibility PQS responsibility Explicit cultural emphasis Inspection focus Quality-system approach

The main rule in regulations is that keeping data accurate and reliable is something that needs to be managed throughout the whole process, not just about writing down what happened in the lab.[1,3,6,9,12,13]

12. Major Regulatory Challenges

12.1 Legacy Computerized Systems

Many pharmaceutical companies still use old equipment and programs that weren't made with today's data management rules in mind.

Common deficiencies include:

- lack of audit trails;
- inadequate user management;
- limited electronic signatures;
- inability to export complete data;
- obsolete operating systems;
- inadequate backup;
- uncontrolled configuration; and
- dependence on unsupported software.

It might not be possible to replace all old systems right away. A good plan for fixing risks should involve checking the system, figuring out which data is most important, using extra safety measures when needed, and having a schedule for updating things.

12.2 Uncontrolled Spreadsheets

People often use spreadsheets for doing calculations, tracking trends, managing inventory, analyzing stability, performing lab calculations, and keeping track of quality standards.

They might cause problems with honesty since formulas can be altered without being noticed, there could be many different versions that aren't kept track of, and it might not be clear who used them.

The MHRA has pointed out the possible risks related to how data is managed, especially when data from spreadsheets can't be found anywhere else or is very important for a GxP activity.[15]

When spreadsheets are used for important GMP tasks, organizations should think about:

- access control;
- version control;

- formula protection;
- validation;
- change control;
- backup;
- user identification; and
- independent verification where appropriate.

12.3 Inadequate Audit-Trail Review

Having an audit trail does not mean the organization has a good process for reviewing audit trails.

- Common deficiencies include:
- no defined review frequency;
- unclear responsibility;
- review limited to selected records without justification;
- failure to investigate unusual events;
- inadequate documentation of review;
- inappropriate administrative access; and
- failure to preserve audit-trail data.

A good system should have an audit trail checked based on risk, considering how important the data is and how much it could affect the product's quality.

12.4 Shared Accounts and Excessive Privileges

Shared accounts undermine attribution.

Having too much control over system settings can be risky because people might have access to do things that aren't needed for their job, like changing how the system works, deleting important information, or adjusting security rules.

Role-based access and separating duties are key parts of managing electronic data properly.

12.5 Data Exclusion and Selective Reporting

One of the biggest issues with honesty happens when companies keep only the information that backs up what they want to prove.

Examples include:

- deleting failed chromatograms;
- repeating analyses without documenting the reason;
- excluding unexpected stability results;
- omitting failed environmental-monitoring results;
- discarding unsuccessful development experiments; or
- reporting only selected process data.

The FDA clearly wants labs to keep all types of test results, like passing, failing, questionable, or wrong data, showing how important it is to have full and accurate records.[2]

2.6 Outsourcing and Third-Party Providers

Pharmaceutical companies are relying more and more on outside groups like contract labs, contract manufacturers, cloud service companies, software providers, calibration labs, and other similar external businesses.

Outsourcing a task doesn't mean you don't need to watch over the related data properly.

Quality agreements should address:

- data ownership;
- data access;
- retention;
- backup;
- audit trails;
- cybersecurity;
- change control;
- incident reporting;
- inspection rights;
- system validation; and
- business continuity.

Third-party risk needs to be considered when choosing suppliers and when checking their performance over time.

12.7 Cybersecurity and Data Integrity

Cybersecurity and data integrity are connected but they are not the same thing.

Cybersecurity helps keep systems and information safe from people trying to get in without permission or do harmful things. Data integrity also needs to make sure that the information correctly shows what is actually happening.

Potential cybersecurity-related integrity threats include:

- credential compromise;
- ransomware;
- unauthorized remote access;
- malware;
- malicious alteration;
- compromised interfaces;
- unauthorized database access; and
- loss of availability.

Therefore, drug companies need to combine cybersecurity risk checks with GMP data integrity reviews.

13. Quality Culture and Human Factors

Technology alone cannot eliminate data-integrity failures.

Human factors may include:

- inadequate training;
- excessive workload;
- unrealistic production targets;
- insufficient staffing;
- fear of reporting errors;
- weak management oversight;
- ambiguous responsibilities;
- inadequate supervision; and
- organizational pressure to produce favorable results.

Studies looking into regulatory actions have found that human factors play a key role in issues related to data integrity.[5]

A strong culture that values data integrity should encourage employees to report:

- errors;
- unexpected results;
- deviations;
- equipment failures;
- documentation mistakes; and
- potential integrity concerns.

The goal is to create a place where honest information is seen as more important than information that sounds good.

Management should also be careful not to use performance measures that might encourage hiding problems—for example, judging departments only based on how many deviations or OOS investigations they have.

14. Data Integrity and CAPA

Data integrity issues need to be handled within the pharmaceutical quality system.

An appropriate response to a data-integrity event may involve:

- immediate containment;
- preservation of potentially affected records;
- assessment of the scope of the issue;
- figuring out which products, batches, studies, or submissions are affected.
- investigation of root causes;
- evaluation of patient and product risk;
- regulatory assessment and notification where applicable;
- corrective actions;
- preventive actions;
- effectiveness verification; and
- management review.

A weak CAPA system might fix the immediate technical issue but doesn't solve the bigger, underlying problem.

For example, just changing the shared account won't really fix the problem if the company doesn't have rules for managing user access, regular checks on who has access, or someone responsible for overseeing access management.

15. Practical Framework for ALCOA+ Implementation

A pharmaceutical company can use the ALCOA+ framework by following this lifecycle model:

Step 1: Establish Governance

Define management accountability, data ownership, data stewardship, quality assurance oversight, IT responsibilities, and the process for escalating issues.

Step 2: Inventory Data and Systems

Identify:

- critical GMP data;
- data-generating systems;
- paper records;
- electronic records;
- hybrid systems;
- interfaces;
- spreadsheets; and
- external data sources.

Step 3: Map Data Flows

Record how important data moves from when it is first made until it is stored for the long term.

Step 4: Determine Data Criticality

Assess the effect of data on:

- patient safety;
- product quality;
- regulatory decisions;
- batch release;
- process control; and
- scientific conclusions.

Step 5: Conduct Integrity Risk Assessment

Identify opportunities for:

- unauthorized modification;
- deletion;
- concealment;
- inappropriate processing;
- loss;
- transcription;
- uncontrolled access; and
- inadequate review.

Step 6: Implement Controls

Controls may include:

- unique accounts;
- role-based access;
- audit trails;
- electronic signatures;
- validation;
- backup;
- cybersecurity;
- controlled procedures;
- independent review; and
- physical controls.

Step 7: Train Personnel

Training should be tailored to each job role and include real examples of data integrity issues.

Step 8: Monitor Effectiveness

Useful indicators include:

- audit-trail exceptions;
- access-control violations;
- repeated data-processing events;
- unexplained data deletion;
- backup failures;
- overdue periodic reviews;
- recurring documentation errors;
- repeated deviations; and
- data-integrity investigations.

Step 9: Continually Improve

Integrate findings into:

- CAPA;
- change control;
- internal audits;
- management review;
- supplier qualification;
- validation;
- periodic system review; and
- quality-risk-management activities.

16. Future Perspectives

16.1 Artificial Intelligence and Machine Learning

Artificial intelligence is probably going to play a bigger role in ensuring the quality of medicines in the future.

Potential applications include:

- anomaly detection;
- automated audit-trail analysis;
- trend detection;

- predictive maintenance;
- automated deviation classification;
- process monitoring;
- quality-risk prediction;
- document review; and
- continuous data-integrity monitoring.

However, AI itself creates new data-integrity challenges.

Organizations will need to control:

- training-data quality;
- model versioning;
- intended use;
- model validation;
- performance monitoring;
- model drift;
- cybersecurity;
- human oversight;
- change control; and
- preservation of model outputs and relevant metadata.

The European Commission's proposed Annex 22 shows this new direction by focusing on intended use, training data, validation, performance metrics, ongoing monitoring, managing changes, and human checks.[6]

16.2 Continuous Data-Integrity Monitoring

Traditional methods usually depend on regular checks and reviews.

Future systems might start using ongoing monitoring more often to detect:

- unusual login patterns;
- abnormal data deletions;
- unexpected sequence changes;
- atypical data-processing behavior;
- repeated reintegration;
- unusual result patterns;
- unauthorized configuration changes; and
- missing audit-trail events.

This method might change how pharmaceutical quality is checked from doing it only at certain times to keeping it under control all the time and taking action early when needed.

16.3 Cloud-Based Pharmaceutical Systems

Cloud computing can improve:

- scalability;
- accessibility;
- centralized data management;
- backup;
- disaster recovery; and
- system integration.

Nevertheless, organizations must establish controls for:

supplier qualification;

- data ownership;
- data location;
- access control;
- cybersecurity;
- business continuity;
- backup responsibility;
- system configuration;
- auditability; and
- regulatory inspection access.

Cloud deployment should be checked using the same steps and rules for quality and risk that are used for other computerized systems.

16.4 Digital Twins and Continuous Manufacturing

Pharmaceutical companies are starting to use continuous manufacturing more often, along with better process control, real-time monitoring of production, and digital models of how manufacturing works.

Digital twins can potentially support:

- real-time process understanding;
- predictive quality;
- process optimization;
- equipment monitoring; and
- advanced control strategies.

However, digital twins also raise questions about the reliability of the models, including the data used, the assumptions made, how the model stays updated with real-world changes, the accuracy of the simulations, how the model is kept current, and how people interact with it.

Recent studies have pointed out specific issues related to data integrity in digital twins and continuous pharmaceutical manufacturing, showing that traditional ALCOA+ principles need to be expanded to cover more complex digital environments.[16]

16.5 Blockchain and Immutable Records

Blockchain and other similar technologies that use a shared record system have been suggested as ways to make tracking easier and to create records that show if they have been changed.

- Potential applications include:
- supply-chain traceability;
- clinical-trial records;
- serialization;
- transaction history; and
- verification of data provenance.

However, immutability does not guarantee accuracy.

If wrong information is put into a system that can't be changed, the system might keep that wrong information very well.

So, blockchain should be seen as a potential tool to help with tracking and verifying the origin of things, but it shouldn't take the place of ALCOA+ standards, validation processes, or human supervision.

16.6 Advanced Analytics and Predictive Quality Assurance

Machine learning and statistical analysis can help companies find patterns that are hard to spot using traditional methods.

For example, algorithms may identify:

- unusual analyst behavior;
- abnormal laboratory result distributions;
- unexpected data-entry timing;
- unusual equipment usage;
- repeated data-processing events; and
- deviations from historical process patterns.

These tools might play a key role in monitoring quality based on risk.

Even though automated alerts are useful, they should be checked and looked into by trained professionals to make sure they are accurate. An algorithm should help, but not take the place of scientific and quality decisions.

17. ALCOA+ and the Future Pharmaceutical Quality System

The future of pharmaceutical quality systems will probably become more digital, linked together, and based on data.

This transformation creates a need to integrate:

English language content rephrased in a simple tone using simple words, without shortening or excluding any details, and made to sound natural and human:

ALCOA principles plus managing quality risks, handling the lifecycle of computerized systems, ensuring cybersecurity, guiding the use of artificial intelligence, and fostering a strong quality culture.

Instead of handling data integrity as a separate compliance task, companies should include it in all the right quality processes.

For example:

- Quality Process Data-Integrity Application
- Deviation management Preserve complete investigation records
- CAPA should keep track of data about the main causes and how effective the solutions were.
- Change control involves checking how changes will affect data creation and system setup.
- Validation Demonstrate integrity controls throughout system lifecycle
- Supplier qualification Assess external data-governance capability
- Internal audit Evaluate ALCOA+ controls
- Management review Monitor data-integrity indicators
- Batch release should have full and trustworthy supporting data.
- OOS investigation Preserve all relevant analytical information
- Training Establish data-integrity competence

Cybersecurity helps keep data safe from being changed or lost without permission.

This integration matches the idea from ICH Q10 about a pharmaceutical quality system that includes process performance, quality checks, taking corrective or preventive actions, managing changes, and ensuring management is responsible.[9]

18. Recommendations

Based on the rules and science that have been looked at, drug companies should think about these suggestions:

18.1 Establish Executive Accountability

Senior leaders need to take full responsibility for making sure data is accurate and reliable, and they should make sure there are enough resources to fix problems, update systems, train people, and keep an eye on things.

18.2 Develop a Site-Wide Data Governance Program

The program should include topics like laboratory work, manufacturing processes, engineering, quality assurance, quality control, supply chain management, regulatory affairs, and activities that are done by outside companies.

18.3 Maintain a Data and System Inventory

Companies need to understand where important data is created, handled, saved, moved, and kept long-term.

18.4 Apply Risk-Based Controls

Controls should be matched to how important the data is and how likely and easy it is to detect problems with its accuracy.

18.5 Modernize High-Risk Legacy Systems

Legacy systems should be handled based on how important the data is and the risk to data accuracy, instead of just because they are old.

18.6 Strengthen Audit-Trail Review

Audit trail reviews need to be based on risk, properly recorded, supported by scientific reasons, and connected with quality checks.

18.7 Control Spreadsheets

Important spreadsheet files need to be properly managed, checked for accuracy, kept up to date with versions, limited to approved users, and looked at regularly.

18.8 Strengthen Third-Party Oversight

Contracts and quality agreements need to clearly define who is responsible for data ownership, keeping data safe, storing it properly, controlling who can access it, making backups, ensuring data is accurate, and preparing for regulatory inspections.

18.9 Develop Data-Integrity Culture

Employees should feel comfortable sharing mistakes and strange outcomes without feeling forced to hide bad news.

18.10 Prepare for AI Governance

Companies that use AI should create rules and management systems before putting it into action. This should include figuring out what the AI will be used for, making sure it works properly, controlling the data it learns from, keeping track of how well it performs, having people check on its decisions, and managing any changes to the system.

18.11 Measure Effectiveness

To properly assess how well data-integrity programs work, we should look at real results and numbers, not just check if people followed the rules or completed training.

19. Conclusion

Data integrity is very important for making sure pharmaceutical quality is reliable because the trustworthiness of product quality depends entirely on the accuracy of the data used to support it. The ALCOA+ framework offers a useful and thorough way to make sure data is Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, and Available all through its life.

To implement something effectively, you need much more than just writing down procedures. Data integrity should be part of the pharmaceutical quality system, quality risk management, managing computerized systems throughout their lifecycle, laboratory controls, manufacturing processes, monitoring suppliers, corrective and preventive actions, change control, cybersecurity, employee training, and management reviews.

The ways that the FDA, MHRA, EU authorities, PIC/S, WHO, and ICH handle regulations use different terms and structures, but they all have one main goal: pharmaceutical companies must show that the data used for quality and regulatory decisions are trustworthy, full, trackable, and properly managed.[1,3,6,8,9,12,13]

The biggest problems are no longer just about easy lies. Today's data integrity risks come from many different sources. These include complicated computer systems, older technology platforms, mixed types of records, uncontrolled spreadsheets, connections between different systems, cloud-based services, outside service providers, security threats, too much access permission, incomplete tracking of actions, and the wrong use of powerful data analysis tools.

Future pharmaceutical quality systems will more and more rely on AI, machine learning, cloud computing, continuous manufacturing, digital twins, automated audit-trail analysis, and continuous monitoring. These technologies can greatly help improve the accuracy of data, but they will also bring about new rules and regulations that need to be followed. New rules about AI in making drugs show that in the future, regulators will pay more attention to what the AI is meant to do, how good the data is, testing the AI's results, keeping track of changes, and making sure people are involved in checking the AI's work.[6]

So, the future of ensuring reliable pharmaceutical data isn't about picking between people and technology. It will depend on how well people, processes, technology, quality risk management, cybersecurity, and organizational culture are combined together.

Ultimately, ALCOA+ should not be viewed as a simple checklist for inspections. It should act as a guiding principle for managing data in the pharmaceutical industry—making sure that the evidence used to make decisions about drug quality is scientifically reliable, clear, able to be reviewed again, and can be trusted. The main goal is not just to follow rules but to make sure patients are safe by ensuring medicines are of good quality.

References

1. U.S. Food and Drug Administration. *Data Integrity and Compliance with Drug CGMP: Questions and Answers—Guidance for Industry*; U.S. Department of Health and Human Services, Food and Drug Administration: Silver Spring, MD, 2018. <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-integrity-and-compliance-drug-cgmp-questions-and-answers>.
2. U.S. Food and Drug Administration. *Questions and Answers on Current Good Manufacturing Practice Requirements—Laboratory Controls*; U.S. Department of Health and Human Services, Food and Drug Administration: Silver Spring, MD. <https://www.fda.gov/drugs/guidances-drugs/questions-and-answers-current-good-manufacturing-practice-requirements-laboratory-controls>.
3. Medicines and Healthcare Products Regulatory Agency. *GxP Data Integrity Guidance and Definitions*; MHRA: London, U.K., 2021. <https://www.gov.uk/government/publications/guidance-on-gxp-data-integrity>.
4. Rattan, A. K. Data Integrity: History, Issues, and Remediation of Issues. *PDA J. Pharm. Sci. Technol.* **2018**, 72 (2), 105–116. <https://doi.org/10.5731/pdajpst.2017.007765>.
5. Shafiei, N.; De Montardy, R.; Rivera-Martinez, E. Data Integrity—A Study of Current Regulatory Thinking and Action. *PDA J. Pharm. Sci. Technol.* **2015**, 69 (6), 762–770. <https://doi.org/10.5731/pdajpst.2015.01082>.
6. International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use. *ICH Q9(R1): Quality Risk Management*; ICH: Geneva, Switzerland, 2023. <https://www.ich.org/page/quality-guidelines>.
7. International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use. *ICH Q10: Pharmaceutical Quality System*; ICH: Geneva, Switzerland, 2008. <https://database.ich.org/sites/default/files/Q10%20Guideline.pdf>.
8. European Commission. *EudraLex Volume 4: Good Manufacturing Practice Guidelines for Medicinal Products for Human and Veterinary Use, Annex 11: Computerised Systems*; European Commission: Brussels, Belgium. https://health.ec.europa.eu/medicinal-products/eudralex/eudralex-volume-4_en.
9. European Commission. *EudraLex Volume 4: Good Manufacturing Practice Guidelines for Medicinal Products for Human and Veterinary Use, Chapter 4: Documentation*; European Commission: Brussels, Belgium. https://health.ec.europa.eu/medicinal-products/eudralex/eudralex-volume-4_en.
10. Pharmaceutical Inspection Co-operation Scheme. *PIC/S Guidance PI 041-1: Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments*; PIC/S: Geneva, Switzerland, 2021. <https://picscheme.org/docview/4234>.
11. World Health Organization. *WHO Guideline on Data Integrity*; WHO Technical Report Series No. 1033, Annex 4; World Health Organization: Geneva, Switzerland, 2021. <https://www.who.int/publications/m/item/annex-4-trs-1033>.
12. U.S. Food and Drug Administration. *Part 11, Electronic Records; Electronic Signatures—Scope and Application*; U.S. Department of Health and Human Services, Food and Drug Administration: Silver Spring, MD. <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application>.
13. European Commission. *Stakeholders' Consultation on EudraLex Volume 4—Good Manufacturing Practice Guidelines: Chapter 4, Annex 11 and New Annex 22*; European Commission: Brussels, Belgium, 2025. https://health.ec.europa.eu/consultations/stakeholders-consultation-eudralex-volume-4-good-manufacturing-practice-guidelines-chapter-4-annex_en.

14. • Rogers, C. A.; Ahearn, J. D.; Bartlett, M. G. Data Integrity in the Pharmaceutical Industry: Analysis of Inspections and Warning Letters Issued by the Bioresearch Monitoring Program Between Fiscal Years 2007–2018. *Ther. Innov. Regul. Sci.* **2020**, 54 (5), 1123–1133. <https://doi.org/10.1007/s43441-020-00129-z>.
15. • Chen, Y.; Yang, O.; Sampat, C.; Bhalode, P.; Ramachandran, R.; Ierapetritou, M. Digital Twins in Pharmaceutical and Biopharmaceutical Manufacturing: A Literature Review. *Processes* **2020**, 8 (9), 1088. <https://doi.org/10.3390/pr8091088>.
16. • Leal, F.; Chis, A. E.; Caton, S. J.; González-Vélez, H.; García-Gómez, J. M.; Durá, M.; Sánchez-García, A.; Sáez, C.; Karageorgos, A.; Gerogiannis, V. C.; Xenakis, A. Smart Pharmaceutical Manufacturing: Ensuring End-to-End Traceability and Data Integrity in Medicine Production. *Big Data Res.* **2021**, 24, 100172. <https://doi.org/10.1016/j.bdr.2020.100172>.
17. • Alosert, H.; Savery, J.; Rheume, J.; Cheeks, M.; Turner, R.; Spencer, C.; Farid, S. S.; Goldrick, S. Data Integrity within the Biopharmaceutical Sector in the Era of Industry 4.0. *Biotechnol. J.* **2022**, 17 (6), e2100609. <https://doi.org/10.1002/biot.202100609>.
18. • Nagy, B.; Galata, D. L.; Farkas, A.; Nagy, Z. K. Application of Artificial Neural Networks in the Process Analytical Technology of Pharmaceutical Manufacturing—A Review. *AAPS J.* **2022**, 24, 74. <https://doi.org/10.1208/s12248-022-00706-0>.
19. • Sim, C.; Zhang, H.; Chang, M. L. Improving End-to-End Traceability and Pharma Supply Chain Resilience Using Blockchain. *Blockchain Healthc. Today* **2022**, 5, 10.30953/bhty.v5.231. <https://doi.org/10.30953/bhty.v5.231>.
20. • Charoo, N. A.; Khan, M. A.; Rahman, Z. Data Integrity Issues in Pharmaceutical Industry: Common Observations, Challenges and Mitigations Strategies. *Int. J. Pharm.* **2023**, 631, 122503. <https://doi.org/10.1016/j.ijpharm.2022.122503>.
21. • Pedro, F.; Veiga, F.; Mascarenhas-Melo, F. Impact of GAMP 5, Data Integrity and QbD on Quality Assurance in the Pharmaceutical Industry: How Obvious Is It? *Drug Discovery Today* **2023**, 28 (11), 103759. <https://doi.org/10.1016/j.drudis.2023.103759>.
22. • Maguire, J.; Fisher, A.; Harouaka, D.; Rakala, N.; Lundt, C.; Yambot, M.; Viehmann, A.; Stiber, N.; Gonzalez, K.; Canida, L.; Buhse, L.; Kopcha, M. Lessons from CDER's Quality Management Maturity Pilot Programs. *AAPS J.* **2023**, 25, 14. <https://doi.org/10.1208/s12248-022-00777-z>.
23. • Fischer, R.-P.; Volpert, A.; Antonino, P.; Ahrens, T. D. Digital Patient Twins for Personalized Therapeutics and Pharmaceutical Manufacturing. *Front. Digit. Health* **2023**, 5, 1302338. <https://doi.org/10.3389/fdgth.2023.1302338>.
24. • Gholipour, E.; Bastas, A. State-of-the-Art Review of Neural Network Applications in Pharmaceutical Manufacturing: Current State and Future Directions. *J. Intell. Manuf.* **2024**, 35 (7), 3003–3035. <https://doi.org/10.1007/s10845-023-02206-0>.
25. • Raja, J. R.; Kella, A.; Narayanasamy, D. The Essential Guide to Computer System Validation in the Pharmaceutical Industry. *Cureus* **2024**, 16 (8), e67555. <https://doi.org/10.7759/cureus.67555>.
26. • Sabale, M. M.; Pande, V. A.; Tagalpallewar, A. A.; Swami, A. G.; Pawar, A. T.; Baheti, A. M. Maintaining Data Safety and Accuracy through Data Integrity (DI): A Comprehensive Review. *Res. J. Pharm. Technol.* **2024**, 17 (5), 2431–2440. <https://doi.org/10.52711/0974-360X.2024.00381>.
27. • Ullagaddi, P. Safeguarding Data Integrity in Pharmaceutical Manufacturing. *J. Adv. Med. Pharm. Sci.* **2024**, 26 (8), 64–75. <https://doi.org/10.9734/jamps/2024/v26i8708>.
28. • Padma, A.; Ramaiah, M. Blockchain Based Solution for Secure Information Sharing in Pharma Supply Chain Management. *Heliyon* **2024**, 10 (22), e40273. <https://doi.org/10.1016/j.heliyon.2024.e40273>.
29. • Mastrantonas, A.; Kokkas, P.; Chatzopoulos, A.; Papoutsidakis, M.; Stergiou, C.; Vairis, A.; Kanetaki, Z. Identifying the Effects of Industry 4.0 in the Pharmaceutical Sector: Achieving the Sustainable Development Goals. *Discover Sustainability* **2024**, 5, 460. <https://doi.org/10.1007/s43621-024-00716-2>.
30. • Kerr, J.; Polonsky, M. Evaluating the PDA Quality Culture Assessment Tool as a Foundation to Advance Quality Management Maturity. *AAPS J.* **2026**, 28, 76. <https://doi.org/10.1208/s12248-026-01234-x>.
31. • Ramprasath, P.; Bonthu, M. G. Data Integrity Failures in Pharmaceutical Digital Twins and Continuous Manufacturing: An ALCOA++ Framework Integrating Human Factors and Simulation Vulnerabilities. *J. Pharm. Innov.* **2026**, 21, 553. <https://doi.org/10.1007/s12247-026-10778-6>.