Available online on 15 Dec, 2025 at https://ijdra.com/index.php/journal

International Journal of Drug Regulatory Affairs

Published by Diva Enterprises Pvt. Ltd., New Delhi
Associated with Delhi Pharmaceutical Sciences & Research University

Review Article

Open Access

Data Integrity in Pharmaceuticals

Madhanraj S[*], Anton Smith A

Department of Pharmacy, Annamalai University, Annamalai Nagar, Chidambaram-608002, Tamil Nadu, India.

Abstract

In the pharmaceutical world, maintaining data integrity represents one of the most critical aspects of ensuring that medications reach patients safely and effectively. This concept goes far beyond simple record keeping it encompasses the entire journey of information from initial research through final product delivery, ensuring that every piece of data remains accurate, reliable, complete, and consistent throughout this process. The regulatory landscape has evolved significantly, with organizations like the FDA establishing comprehensive guidelines such as 21 CFR Part 11, alongside internationally recognized frameworks like ALCOA+ and ICH Q7. These standards emphasize that pharmaceutical data must be attributable, legible, contemporaneous, original, and accurate, while also being complete, consistent, enduring, and available whenever needed. The importance of data integrity extends well beyond regulatory compliance. When pharmaceutical companies maintain robust data practices, they build trust with patients, protect public health, and foster transparency across all operational levels. However, the path to achieving this ideal is fraught with challenges, including human errors, inadequate digital infrastructure, poor documentation practices, and increasingly sophisticated cybersecurity threats. To address these challenges, companies are implementing comprehensive risk-based approaches, investing in advanced digital technologies, and cultivating organizational cultures that prioritize quality and accountability. This paper explores the fundamental principles governing data integrity, examines regulatory requirements, identifies common pitfalls, and presents best practices for maintaining data integrity in pharmaceutical operations.

Keywords: Data Integrity; ALCOA and ALCOA++ principles; Data Retention; Data Governance; Organizational Culture; Cyber Security

Article Info: Received 30 Sep 2025; Review Completed 11 Nov 2025; Accepted 15 Nov 2025

Cite this article as:
Madhanraj S, Anton Smith A. Data Integrity in Pharmaceuticals. Int. J. Drug Reg. Affairs [Internet]. 2025 Dec15 [cited 2025 Dec 15]; 13(4):26-36. Available from: https://ijdra.com/index.php/journal/article/view/816

DOI: 10.22270/ijdra.v13i4.816

*Corresponding author. E-mail address: madhanrajsiva03@gmail.com (Madhanraj S).

1. Introduction

Data integrity, at its core, refers to maintaining the accuracy, completeness, and consistency of information throughout its entire lifecycle. (1) In the pharmaceutical industry, this concept takes on life-or-death significance, as the data generated during drug development, manufacturing, and distribution directly impacts patient safety and treatment efficacy. The pharmaceutical sector operates within a heavily regulated environment where every decision must be backed by trustworthy data. (2) From the earliest stages of drug discovery through post-market surveillance, companies generate vast amounts of information that must be carefully managed and preserved. This data serves as the foundation for regulatory submissions, manufacturing decisions, quality control measures, and safety assessments. (3) As the industry becomes more digital, maintaining data integrity has become more complex. Electronic systems manage everything from lab results to manufacturing data, creating both new benefits and new risks. Companies must ensure that all records electronic and paper remain accurate, reliable, and preserved in their original form. (4) It is fundamental to assuring product quality and represents a core requirement of Good Manufacturing Practice (GMP). (5) The stakes could not be higher. When data integrity fails, the consequences can include regulatory sanctions, product recalls, financial losses, and most importantly, potential harm to patients who depend on safe and effective medications. (6)

2. Need for Data Integrity

The pharmaceutical industry operates under a fundamental premise: every product that reaches a patient must be supported by comprehensive evidence demonstrating its safety and effectiveness. This requirement creates multiple layers of necessity for maintaining data integrity across all operations. (1)

Beyond patient safety, data integrity also ensures accurate evaluation of how well a product works, helps prevent adverse drug reactions through complete and reliable records, and supports research and development by providing trustworthy data for future improvements. (7)

Regulatory compliance is also a key part of data integrity. Since pharmaceutical regulations differ across countries, maintaining accurate and reliable data helps companies meet these requirements and ensures smoother inspections and submissions. (8)

From a business standpoint, data integrity lowers operational risks by preventing errors and recalls. It ensures full traceability across manufacturing and distribution, helping companies address problems quickly. Strong data integrity in clinical trials also reduces the chances of regulatory rejection and financial loss. (9)

3. Regulatory Framework

Data integrity is essential in pharmaceuticals because it affects product quality and patient safety. Regulatory agencies strictly enforce rules to ensure proper data handling, and companies must use SOPs with clear steps for recording and managing data. Authorities have also increased data integrity requirements to improve compliance.(3)

a) FDA

Under 21 CFR guideline part 11: Verifying the integrity and authenticity of electronic records and signatures, are trustworthy, secure, reliable, and equivalent to handwritten records. (10) The Federal Register publishes federal rules, including FDA regulations. These rules are then compiled into Title 21 of the Code of Federal Regulations, which is updated each year. (11)

b) WHO

WHO guidelines emphasize data integrity to protect patients, requiring manufacturers to provide accurate and reliable data to regulatory authorities, following GMP and GLP standards. (12)

Annex 4 of Technical Report Series, 1033 of WHO: The guideline emphasizes maintaining data reliability and trustworthiness throughout pharmaceutical product development, production, and registration.

Guideline on Data Integrity- Technical Report Series, 1033 (2021): This guideline provides a framework for enhancing data integrity in product quality, safety, and efficacy, offering practical guidance and recommendations. (10)

c) MHRA

Guidance on GxP Data Integrity (2018): This guidance aims to enhance data governance compliance by highlighting essential elements, addressing inspection-related issues, and providing educational support. (10) Data integrity guidelines for pharma companies focus on ensuring medication quality, in line with GMP requirements for APIs and dosage forms. (12) The MHRA's GMP data integrity guideline enhances EU standards for active ingredients and dosage forms, emphasizing data integrity's critical role in ensuring medication quality. (11)

d) EMA

Good record-keeping practices guarantee data accuracy and compatibility, supporting informed decisions and regulatory compliance in the pharmaceutical industry. (12) The EMA updated its GMP guidelines to improve data quality, helping regulators and companies assess a medicine’s quality, safety, and effectiveness throughout its lifecycle. (11)

EudraLex Volume 4: Volume 4 outlines the (EU-GMP) guidelines, which establish the documentation standards necessary for ensuring compliance with GMP requirements.

Annex 11: This annex focuses on computerized systems, highlighting their importance in data storage, processing, and retrieval. (10)

e) cGMP

Data integrity-related cGMP violations have led to warning letters, import alerts, and consent decrees. To address this, the FDA issued guidance on “Data Integrity and Compliance with cGMP” for the industry. (13) Firms should adopt a risk-based strategy for data integrity, utilizing process understanding and knowledge management to effectively regulate and mitigate risks in accordance with cGMP regulations. (12)

f) GDP

GDP guidelines provide best practices for data documentation, emphasizing completeness, accuracy, and traceability through clear and organized recording of observations, procedures, and results. (3) Good documentation practices ensure records are clear, traceable, permanent, and accurate, whether on paper or electronic. These principles help maintain reliable and trustworthy documentation. (11)

g) GUIDELINE, 21 CFR PART “11”

As per 21 CFR Part 11, electronic records and signatures must ensure the security, integrity, traceability, and proper use of electronic data and signatures. (14) The regulation 21 CFR Part 11 provides guidelines for the pharmaceutical industry on electronic records and signatures, emphasizing authenticity, integrity, and reliability. (3) Data migration involves transferring records from one validated system to another, and 21 CFR Part 11 requires that all data be copied accurately and completely during this process. (15)

4. Principles of Data Integrity

The US FDA's ALCOA+ principles ensure data is Attributable, Legible, Contemporaneous, Original, and Accurate, with additional attributes for data integrity, including being comprehensive, consistent, long-lasting, and accessible. (4)

4.1 ALCOA principles

i. *Attributable*

To maintain data integrity, secure login practices are crucial, including the use of unique user IDs and electronic signatures to track data interactions. (1)

Accurate data management requires capturing details about data collectors, action takers, and timestamps to maintain data integrity. (4) Qualified personnel and compliant electronic systems, adhering to 21 CFR Part 11, are essential for ensuring data validity and integrity. (2) Attributability is measured by checking how much of the data is correctly linked to the person who collected it. The attributable score shows the proportion of data properly assigned to the responsible staff member, ensuring data accountability. (16)

ii. *Legible*

This process requires the implementation of secure and unique user logins, as well as electronic signatures. Unique user logins should be used to ensure accountability, while generic login IDs and shared credentials are strictly prohibited. (1) Records should be legible, with identifiable signatures, and may include both raw data and metadata. (3) Information should be accurate, clear, and easy to understand. Avoid buzzwords or informal terms that may change over time and create confusion. (8) Data should be in electronic format, encoded in UTF-8 and decimal numbers must be formatted consistently and free text should use standard dictionary words. (15)

iii. *Contemporaneous*

This addresses the issue of timely and accurate data recording is crucial for both human-generated and system-generated data. (4) Delayed documentation can lead to errors, inaccuracies, and compromised data quality. (17) Contemporaneous data recording is checked by confirming that entries include correct date and time stamps. The contemporaneous score shows the percentage of data with accurate timestamps. (16)

iv. *Original*

Original data, also known as source data or primary data, can be recorded on paper or in electronic format. (4) Original records should be maintained in their native form, rather than relying on duplicates or transcriptions, particularly for manual record-keeping. (1) Data originality is verified through a blockchain-based Smart Contract, ensuring the report's authenticity. The original score is calculated as follows: 100 if the data is original, and 0 if any tampering is detected. (16)

v. *Accurate*

Accurate records reflect actual events without errors or discrepancies. (4) All edits should be documented and annotated to maintain transparency and accountability. (1) Measurements and observations should accurately reflect actual values, ensuring precision and truthfulness. (17) Data accuracy is assessed through range checks and outlier detection, ensuring numerical fields fall within acceptable limits. (16)

4.2 ALCOA++ principles

i. *Complete*

All captured data requires a comprehensive audit trail to ensure transparency and accountability, demonstrating no data loss or deletion. (4) Additionally, any reanalysis of samples must be documented in the records. (10) Data should be accompanied by relevant metadata to ensure thorough documentation. (18) Data completeness is evaluated by verifying that required fields in reports were filled. The completeness score was calculated as the percentage of fulfilled fields out of the total expected fields. (16)

ii. *Consistent*

Data requires sequential timestamps in ascending order. (4). Data is preserved in proper chronological order to maintain sequence and consistency. (18) Consistency is assessed by checking that tracking start dates come before end dates. The consistency score shows the percentage of data that meets this requirement, ensuring accuracy and reliability. (16)

iii. *Enduring*

Long-term data storage ensures data remains accessible and interpretable. (4) Data is preserved for future use, remaining readable and understandable. (18) The enduring score is determined by the presence and validity of a certified expiration date,

Score 100: The expiration date is included and kept up-to-date.

Score 0: Expiration date is missing or has expired. (16)

iv. *Available*

This describes data's capability to be accessible to all interested parties at any point in its lifecycle. (4) It supports accessibility and enables verification by authorized personnel. (18) Additionally, all necessary data or records must be available whenever an audit takes place. (10) The evaluation checks for a certified expiration date to access the report, scoring 100 if it's included and up-to-date, and 0 if it's missing or expired. (16)

v. *Traceble*

Data must be traceable throughout its entire lifecycle, encompassing stages such as creation, processing, usage, retention, and final disposition. (19)

The FDA issued a warning letter on February 24, 2025, after a September 2024 inspection found data integrity-related cGMP violations. The company’s October 8, 2024, response was deemed inadequate, leading to the citation of non-compliance under 21 CFR Part 211.

Table 1. Overview of ALCOA and ALCOA++ principles of data integrity in pharmaceutical sector

PRINCIPLES	DESCRIPTION
Attributable	The data must clearly indicate the individual who carried out the action and the exact time it was performed.

Legible	Records must remain readable and durable throughout their entire lifespan.
Contemporaneous	Data must be documented immediately as the activity takes place.
Original	The original data capture or an authenticated exact copy must be preserved.
Accurate	Data must be free from errors and accurately represent the true observations.
Complete	All data, encompassing metadata and audit trails, must be thoroughly included.
Consistent	Data must maintain a coherent order, with timestamps and version control properly applied.
Enduring	Data must be stored in a stable format that ensures its preservation for the entire required retention duration.
Available	Data must be readily available for inspection, auditing, and regulatory review.
Traceble	Data must be traceable throughout its entire lifecycle, including any modifications and transfers.

5. Types of Pharmaceutical Data

The pharmaceutical industry produces many types of data, each with its own integrity needs and challenges. Knowing these data categories helps companies apply the right controls and management strategies, as shown in Figure 1.

Raw data includes original records or certified true copies kept in their initial form. As defined in 21 CFR 58.3, it covers worksheets, notes, memoranda, and exact copies of original observations. These records must be captured accurately and permanently at the time of observation so studies can be properly reconstructed and evaluated. (1)

Metadata gives context to other data by describing its attributes, structure, and relationships. It helps organize, retrieve, and manage information, and also links data to the individuals responsible, ensuring accountability and traceability. (2)

Static data refers to information stored in fixed formats, like paper records or non-editable electronic files. For example, printed chromatography data becomes static because it can no longer be reprocessed or reviewed in detail. (20)

5.1 Clinical Data

Clinical trials are essential for medicine development, generating data on patient details, treatments, side effects, and effectiveness. This information supports regulatory decisions and improves understanding of a medicine's safety and effectiveness. (20) Clinical trial data are collected, verified, coded, and analyzed to assess a drug's safety, effectiveness, and quality. Clinical Data Management ensures this information is accurate and reliable for regulatory submissions, using compliant electronic systems to store forms, protocols, and outcomes. (21,22)

5.2 Manufacturing Data

Manufacturing data include information on raw materials, process parameters, in-process controls, and final product testing. Modern systems use sensors and lab testing for continuous monitoring. These data covering material attributes, process trends, intermediate results, and final quality test are stored in databases for complete quality evaluation. (23)

5.3 Regulatory Data

Regulatory data includes documents submitted for drug applications, patent details, approvals, compliance reports, and regulatory guidelines required by health authorities. (21) This also includes summaries of clinical data, manufacturing records, safety evaluations, and quality control results. Regulatory submissions are now increasingly digital, using structured formats and digital platforms to improve efficiency and data exchange with agencies like the FDA and EMA. Cloud-based tools support faster, more collaborative reviews and real-time data sharing. (24,25)

5.4 Development and Research Data

Early drug development generates data on molecular structures, pharmacology, preclinical results, and clinical updates. This analysis helps identify promising candidates and assess their potential.

6. Challenges in Maintaining Data Integrity

Many pharmaceutical industries face numerous challenges in maintaining data integrity, many of which are reflected in FDA Form 483s and warning letters that highlight recurring compliance issues. (18)·

Technical Challenges

Many companies still use outdated systems without proper controls or audit trails. Upgrading them is costly and time-consuming, requiring careful planning to avoid disruptions. (18)

6.1 Complexity of Systems

The pharmaceutical supply chain involves many external partners, making data integrity difficult to maintain. Common issues include poor data retention and missing raw data or metadata. Failure to follow ALCOA++ principles harms data quality and can lead to regulatory non-compliance. (18) A breach of data integrity occurs when the accuracy, consistency, or reliability of data is compromised. (26) Such violations can result in warning letters, import alerts, and financial penalties. These issues often arise from poor practices, weak organizational culture, and inadequate systems, increasing the risk of data manipulation. (27)

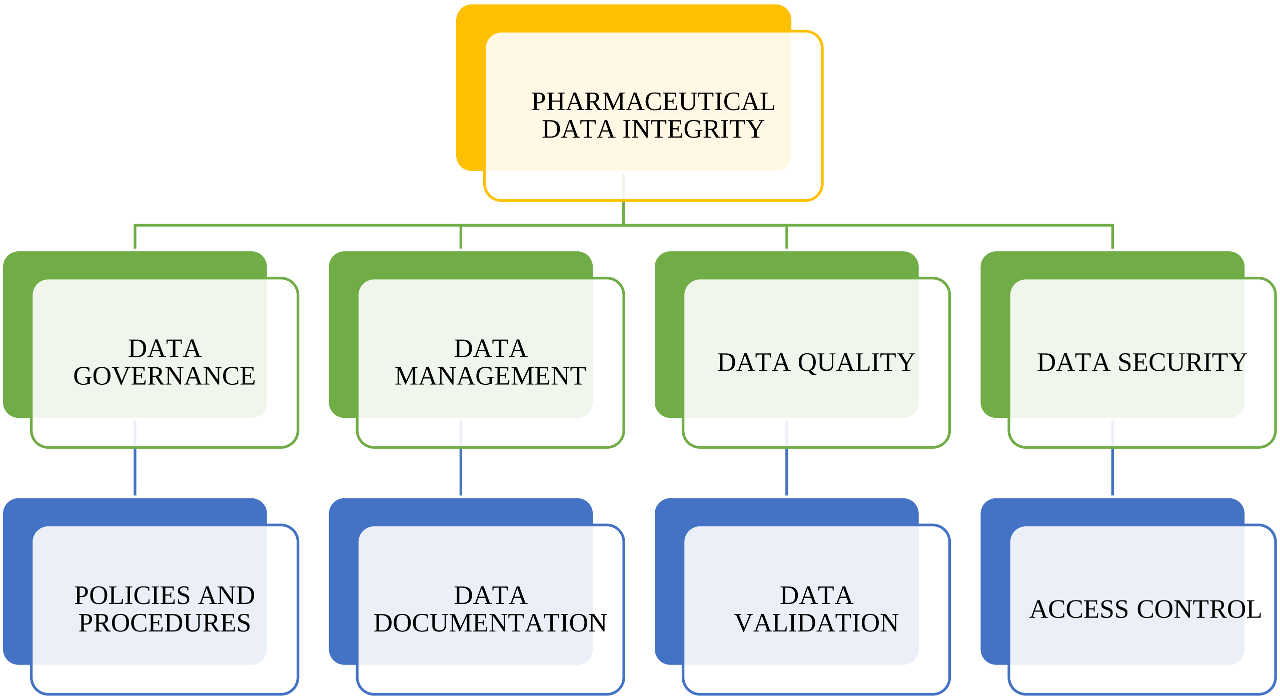


Figure 1. Data Integrity Lifecycle Management

Transfer Errors: Data integrity issues arise when information is not accurately transferred between different sections of a database, causing inconsistencies between the source and destination tables. (5)

6.2 Human Error

Data integrity violations can occur due to failure to adhere to standard operating procedures, omission of necessary documentation steps, or deliberate manipulation of data to evade extra work or delays. (18) Such issues often stem from human error. Training on ethics and data integrity should be organized for the employees. (27) Errors made during data entry, duplication, deletion, or by following improper procedures can negatively impact data integrity. (7)

Mistakes during entering the data into the system: Such mistakes may be minor, like spelling errors, but they can become significant when interpreting data. Overlooking important details can also lead to inaccuracies.

Data Manipulation or Accidental deletion of data: Unintentional changes or deletions of data can compromise the integrity of records.

Lack of Training and Awareness of new System or Technology: Insufficient training on new data integrity practices can cause employees to make errors and miss critical details.

Manually Entering the Data: Handwritten records are more susceptible to errors caused by human mistakes. (10)

6.3 Cyber Security Threats

Cyber attackers exploit software weaknesses to steal data or compromise integrity. Protecting data is vital for compliance, trust, and reputation. (28) Digitizing records has many benefits, but it also increases the risk of cyberattacks. If hackers compromise protected research data, formulas, or technology, it can seriously damage a company’s intellectual property and progress. (10) Wi-Fi networks are vulnerable to hackers, especially when weak passwords are used. Strong password policies and proper employee training such as not sharing passwords or personal information help prevent unauthorized access or data changes, ensuring staff can only access data within their roles. (29)

Cyber-attacks: Hackers can threaten data integrity using multiple techniques such as injecting malicious code, exploiting system vulnerabilities, or making unauthorized modifications.

Insider Threats: Individuals or employees with system access might deliberately manipulate data for reasons such as personal gain, revenge, or other motivations. (17)

7. Risk Management STRATEGIES

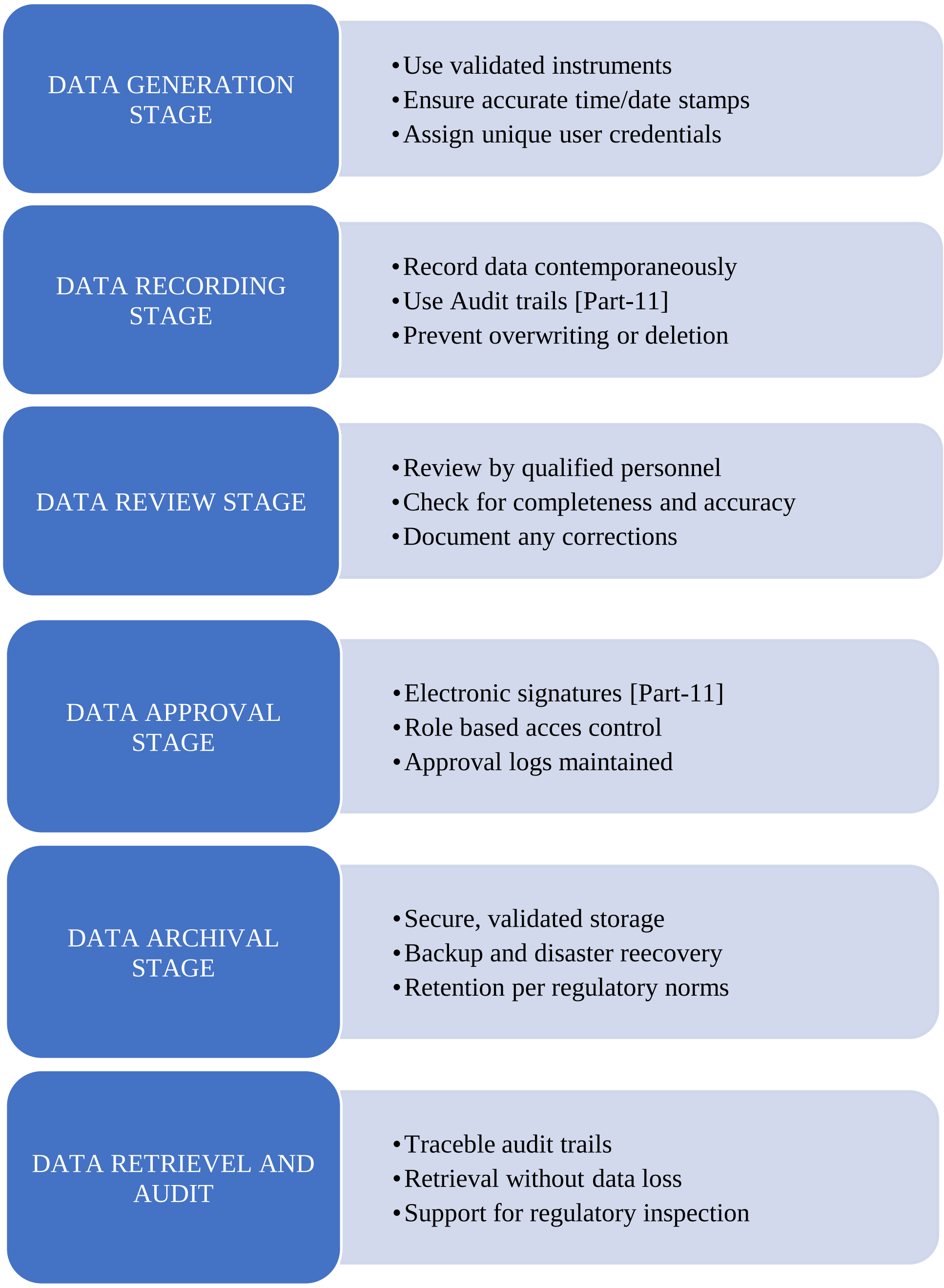
Effective risk management requires a comprehensive approach that addresses technical, procedural, and cultural aspects of data integrity throughout the entire lifecycle of computerized systems. (27)

7.1 Risk Assessment

Data Integrity Risk Assessment (DIRA) identifies processes that generate data, reviews data formats and controls, and documents risks and criticality. It helps organizations understand vulnerabilities and develop strategies to protect data accuracy and reliability using a research-based, analytical approach. (17) The DIRA must be documented and regularly updated. It evaluates risks in GxP systems, personnel, training, and outsourced work. Risks should be controlled and communicated, with reviews performed throughout the data lifecycle based on risk level. (19)

7.2 Mitigation Strategies

Data processing methods must be approved, version-controlled, and protected from unauthorized changes. Even validated systems can be risky if users can choose which data to print or report. (27) Archival means protecting records from alteration or deletion and securely storing them under responsible data management staff for the required retention period. (1) Consistent monitoring, compliance with regulatory requirements, and a commitment to continuous improvement are essential components of a successful data integrity program. (17)



DATA GENERATION STAGE

- Use validated instruments
- Ensure accurate time/date stamps
- Assign unique user credentials

DATA RECORDING STAGE

- Record data contemporaneously
- Use Audit trails [Part-11]
- Prevent overwriting or deletion

DATA REVIEW STAGE

- Review by qualified personnel
- Check for completeness and accuracy
- Document any corrections

DATA APPROVAL STAGE

- Electronic signatures [Part-11]
- Role based acces control
- Approval logs maintained

DATA ARCHIVAL STAGE

- Secure, validated storage
- Backup and disaster reecovery
- Retention per regulatory norms

DATA RETRIEVEL AND AUDIT

- Traceble audit trails
- Retrieval without data loss
- Support for regulatory inspection

Figure 2. Stages involved in estimating and addressing data integrity

Data governance. Awareness of the need for strong data governance is growing. Life science companies are now investing in structured governance frameworks with clear policies, procedures, and controls to maintain data integrity. (31)

Technical Management involves ensuring computerized systems compliance with clear requirements for data integrity from a design, validation and maintenance perspective.

Human Factors Management includes implementing measures to prevent human errors and violations that could compromise data integrity. Providing training programs on data integrity and ethics is also essential. (5)

Risk Based Monitoring employs various methodologies, including Risk Based Monitoring, which helps protect human participants, improve data accuracy, and reduce costs related to drug development. (42)

Data Storage strategies involve storing data in multiple locations helps detect discrepancies by providing redundant copies that can be cross-checked.

Data Encryption protects information during data transfer and prevent unauthorized access, organizations should use encryption protocols.

8. Technological Solutions

Computer systems need strong controls to prevent unauthorized access or data changes. All edits must be logged, and critical actions restricted. Backups must be securely stored to prevent loss or tampering. (5) Cloud storage is popular for its scalability, low cost, and easy access. Archival and hybrid storage options let organizations manage data more efficiently. With advances like SSDs and emerging technologies, storage will become faster, larger, and more cost-effective. (32)

8.1 Electronic System

Biometric signatures authenticate a user's identity by measuring unique and measurable physical characteristics specific to the individual. (5) Advanced systems like Electronic Batch Records (EBRs), LIMS, and PAT have streamlined data recording and real-time process control in pharmaceutical manufacturing. Tools such as NIR and Raman spectroscopy enable continuous, non-destructive monitoring, supporting faster optimization, better quality assurance, and real-time product release. (18)

8.1.1 Laboratory information management systems - LIMS:

A Laboratory Information Management System (LIMS) is software that improves laboratory efficiency by managing workflows, tracking data, handling results, and supporting analysis. It can also integrate with Electronic Laboratory Notebooks. Its features vary by industry needs for example, QC labs focus on meeting specification requirements, while R&D labs use LIMS to manage stability and pharmacokinetic data. (14,34)

8.1.2 Electronic data capture – EDC:

Electronic Data Capture (EDC) is a computer-based system used to collect clinical trial data electronically. It replaces paper methods, making data collection faster and more efficient, and helps speed up the development of drugs and medical devices. EDC is used across all trial phases, allowing information to be entered directly into secure software via the internet.

8.1.3 Share point document management system:

SharePoint, developed by Microsoft in 2001, is a web-based platform used for document management, intranet portals, search, and workflow automation. Its strong integration and content management features make it increasingly valuable for pharmaceutical companies. (14)

8.1.4 Enterprise Content Management (ECM):

Enterprise Content Management (ECM), defined by AIIM in 2000, is software that helps capture, manage, store, preserve, and deliver documents and content throughout their lifecycle. It includes tools for web content management, search, workflow, and document capture, supporting efficient handling of organizational information from creation to archival or disposal. (14,35)

8.2 Audit Trials

Regulations like EU GMP Annex 11 and US 21 CFR Part 11 require audit trail reviews. Clause 9 states that systems must record all GMP-relevant changes or deletions, with written justification for any data modification. Audit trails must be easy to access, easy to understand, and reviewed regularly. (30) Regulators require pharmaceutical companies to maintain strong audit trails in electronic systems. These trails track all changes with timestamps, ensuring accountability and transparency. (7)

System-level audit trails:

High-level audit trails operate at the system level, tracking details such as user identification, date and time of each login and logout, the device used, and tasks performed.

Application-level audit trails:

Application-level audit trails log operations performed on files and transactions, enabling auditors to verify compliance with all procedural steps.

User audit trails:

User audit trails record an individual's activities, including attempts to access specific data or functions, the commands executed, and a summary of user metrics. These audit trails are essential for detecting and identifying suspicious behavior.

Record link:

The unique ID of the corresponding record in an audit trail serves as a specific identifier that ensures traceability of that record throughout its lifecycle.

User ID operating:

Every audit trail entry must be linked to the specific record and able to trace back to the individual responsible, often through the user's unique identification.

Original and change value:

The audit trail must include all previous and updated values of a record over time to enable the reconstruction of its complete history.

Justification/Reasons for change:

A valid justification with a clear rationale for any change must sometimes be provided, and such changes should be managed through a controlled and regulated change process.

Date and time stamp:

A clear and precise date and time stamp is one of the most critical elements for ensuring trustworthy and reliable electronic records. (36)

8.3 Data Backup

Maintaining proper data retention and backup practices is an essential aspect of an effective data governance framework. Regularly performing and testing backups ensures data availability and integrity in case of system failures or disasters. (18) Inadequate backup measures and poor recovery practices can lead to permanent data loss and an inability to restore critical information. (3) Data backup and recovery plans should be established to ensure critical data remains accessible during system failures or data loss incidents. Regular backups are essential for data recovery following breaches. (7)

9. Training and cultural considerations

Data integrity relies on strong processes, secure storage, access controls, and proper training. Companies must clearly communicate policies, and all employees technical and non-technical should be trained to understand their role in protecting patient safety. (50)

9.1 Employee Training

Employees should receive training on proper data documentation and retention. They must understand regulatory requirements, best practices, and the risks of poor documentation. (3) SOPs must guide proper documentation and retention, and all GxP staff need regular, role-based data integrity training. The organization should foster a culture of accurate, complete data and ensure systems, personnel, and facilities support strong integrity controls. (7)

9.2 Organizational Culture

Organizational factors are key to maintaining data integrity. Companies must stay updated on regulatory requirements, identify risks, and apply strong data governance practices to ensure reliable data throughout the product lifecycle. (30) Companies must stay updated on DI requirements and use strong governance practices to ensure reliable data across the product lifecycle. (49) Organizational culture strongly affects data integrity, it can lead to poor practices. A strong quality culture that values data integrity at all levels is essential for lasting compliance and reduced risk. (18)

10 Audits and Inspections

Audits check compliance with FDA 21 CFR Part 11, EU Annex 11, and PIC/S. They verify system validation, access control, audit trails, documentation accuracy, and proper data review and approval.

10.1 Internal Audits

Regular internal audits check the effectiveness of data governance. Audit trails must record all changes and system events, with review frequency based on the data’s risk and impact on quality and patient safety. (18) Pharmaceutical internal quality audits check compliance with SOPs, GMP, and quality standards while promoting continuous improvement. They also assess risk management, validation, training, and document control systems. (37)

10.2 Regulatory Inspections

Regulators set record retention requirements and inspect companies for compliance. Any deficiencies found may lead to corrective actions or penalties. (3)

PIC/S Guidance: PIC/S offers data integrity guidance, and agencies like CDSCO, USFDA, and EMA conduct inspections, including Pre-Approval Inspections. These reviews assess processes, facilities, and equipment to ensure medicines are safe, effective, and consistently high quality. (39)

11. Future Trends and Innovations

Future trends in pharmaceutical data integrity will be influenced by technological advancements, changing regulatory requirements, and shifts in the pharmaceutical industry landscape.

11.1 Automation and Artificial Intelligence

Low-code automation streamlines compliance, improves data integrity, and boosts efficiency, helping companies meet evolving regulatory requirements. (40) AI uncovers patterns humans may miss, speeds up analysis, reduces experiments, and improves process consistency while lowering validation time and costs. (51) AI supports continuous validation by monitoring system performance in real time and updating validation status after changes. In cleaning validation, AI uses image recognition and sensor data to detect residual contaminants accurately. Figure 3 shows its applications in the pharmaceutical sector. (41)

Artificial Intelligence (AI): AI strengthens data integrity by reducing human error and processing large data sets with high accuracy. Its advanced algorithms improve the reliability and quality of data analysis. (42)

Automation and Machine Learning: Emerging technologies like artificial intelligence (AI), machine learning (ML), and blockchain are set to transform data management throughout its lifecycle, from creation to destruction. (32) These technologies help reduce errors because manual data entry is prone to mistakes, while automation greatly minimizes them. (10)

11.2 Blockchain Technology

Blockchain improves data integrity and traceability in the pharmaceutical supply chain by providing secure, transparent, and tamper-proof records of all transactions. (18) Integrating blockchain with Enterprise Resource Planning (ERP) systems marks a significant advancement in the management of supply chains and data integrity. (44) It is a promising technology in the pharmaceutical industry due to its core features of security, authenticity, immutability, and transparency, which ensure end-to-end verification. (48) Blockchain secures data with tamper-evident records, protects sensitive health information, and ensures transparent, traceable drug and vaccine distribution to verify product authenticity. (45) Blockchain stores data in linked blocks, forming a chain where data cannot be deleted or altered without appropriate network permissions. Its key advantage is decentralized storage, avoiding reliance on a single central repository. (10)

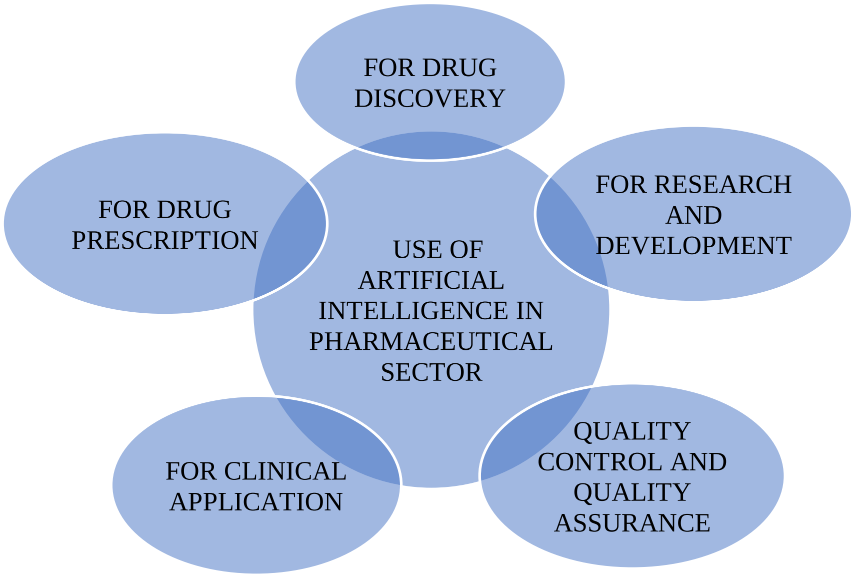

FOR DRUG DISCOVERY
FOR DRUG PRESCRIPTION
FOR RESEARCH AND DEVELOPMENT
USE OF ARTIFICIAL INTELLIGENCE IN PHARMACEUTICAL SECTOR
FOR CLINICAL APPLICATION
QUALITY CONTROL AND QUALITY ASSURANCE

Figure 3. Use of artificial intelligence in pharmaceutical sector

Compliant with DSCSA, blockchain improves supply chain transparency and traceability, reducing counterfeit risks. Digital Ledger Technology assigns each drug a unique identifier and records its full history. Authorized stakeholders can verify a product's authenticity at any stage, and the transparent audit trail simplifies regulatory inspections. (46) Infosys' Blockchain Pharma Supply Chain Solution offers end-to-end traceability from source to shelf. Its tamper-proof records share key product milestones with all partners, helping prevent counterfeits and enabling faster, targeted recalls. (47)

12. Conclusion

Data integrity is not just a regulatory requirement it is the foundation of patient safety, product quality, and overall organizational success. As regulations tighten and supply chains become more complex, strong data integrity practices are essential for long-term efficiency and sustainability.

Achieving this requires committed leadership, trained employees, and investment in technology and culture. When done well, it improves decision-making, reduces risks, increases efficiency, and builds trust.

Ultimately, strong data integrity ensures patients receive safe, effective medicines backed by reliable data. Organizations that prioritize this will be best positioned to support global health and maintain high-quality pharmaceutical standards.

Acknowledgements

I would like to express my gratitude to International Journal of Drug Regulatory Affairs who gave me the opportunity to publish the article.

Conflict of Interest

The authors declare that they have no competing interests related to this work.

Financial Disclosure statement:

The authors have no relevant affiliations or financial involvement with any organization or entity with a financial interest in or financial conflict with the subject matter or materials discussed in the manuscript. This includes employment, consultancies, honoraria, stock ownership or options, expert testimony, grants or patents received or pending, or royalties.

Reference

1. Ahmad S, Kumar A, Hafeez A. Importance of data integrity & its regulation in pharmaceutical industry. Authorea Preprints. 2022 Sep 8;8(1):306-313.
2. Vignesh M, Ganesh GN. Current status, challenges and preventive strategies to overcome data integrity issues in the pharmaceutical industry. Int J Appl Pharm. 2020 Nov 7;12(6):19-23.
3. Ingale MH, Tayade MC, Patil YP, Salunkhe R. Data Integrity Violations in the Pharmaceutical Industry and Regulatory Measures. International Journal of Pharmaceutical Quality Assurance. 2023;14(2):416-420.
4. Kavasidis I, Lallas E, Leligkou HC, Oikonomidis G, Karydas D, Gerogiannis VC, Karageorgos A. Deep transformers for computing and predicting ALCOA+ data integrity compliance in the pharmaceutical industry. Applied Sciences. 2023 Jun 28;13(13):7616.
5. James R, Das S, Kumari A, Rekdal M, Kulyadi GP, Sathyanarayana MB. A recent regulatory update on consequences of data integrity issues and its management in pharmaceutical scenario. Indian Journal of Pharmaceutical Education and Research. 2021 Apr 1;55(2):S616-S622.
6. Gupta KR. Ensuring data integrity in the pharmaceutical sector. International Journal of Pharmaceutical Chemistry and Analysis. 2023 Dec 8;10(4):218–219.
7. Shelke A, Shinde A, Shinde S, Shinde K, Shinde S, Mankar SD. Data Integrity in Pharmaceutical Sciences. International Journal of Pharmaceutical Sciences. 2025 Apr 9;3(4):1142-1148.
8. Singh S, Punjabi N, Shah D. Importance of Data Integrity in Pharmaceutical Industry. EPRA. International Journal of Economics, Business and Management Studies (EBMS). 2023;10(2):100-6.

9. The role of data integrity in implementing QMS in pharmaceutical manufacturing [Internet]. Pharma GMP; 2025 [cited 2025 Nov 30]. Available from: https://www.pharmagmp.in/the-role-of-data-integrity-in-implementing-qms-in-pharmaceutical-manufacturing/
10. Avchar C M. Ensuring Data Integrity in the Pharmaceutical Industry: Challenges and Best Practices. International Journal of Pharmaceutical Sciences. 2025 Mar 31; 3(3):3238-3250.
11. Jale S C, Tendulkar N V, Chavan S M, Biradar S V, Sonawane J K, Narkar I P, Barge A D, Jadhav. An Illustration of Data Integrity. International Journal of Research Publication and Reviews. 2023 May ;4(5):5620-5629.
12. Solanki D, Patel D, Meshram D. Data Integrity: A cornerstone for compliance signature. 2022 Apr 12;3(2): 594-602.
13. Rattan AK. Data integrity: history, issues, and remediation of issues. PDA Journal of Pharmaceutical Science and Technology. 2018 Mar 1;72(2):105-116.
14. Raviteja M N, Gupta N V. A review on electronic data management in pharmaceutical industry. Asian J Pharm Clin Res. 2013 Apr 1;6(2):38-42.
15. Rupani ZM. Clinical trial master file migration: A preordained step for a centralized electronic trial master file. Perspectives in Clinical Research. 2020 Oct 1;11(4):139-143.
16. Durá M, Sánchez-García A, Sáez C, Leal F, Chis AE, González-Vélez H, García-Gómez JM. Towards a computational approach for the assessment of compliance of ALCOA+ Principles in pharma industry. Studies in health technology and informatics. 2022 May 25;294:755-759.
17. Gokulakrishnan D, Venkataraman S. Ensuring data integrity: Best practices and strategies in pharmaceutical industry. Intelligent Pharmacy. 2024 Sep 26;3(4):296-303.
18. Ullagaddi P. Safeguarding data integrity in pharmaceutical manufacturing. Journal of Advances in Medical and Pharmaceutical Sciences. 2024 Aug 17;26(8):64-75.
19. World Health Organization [Internet]. Expert Committee on Specifications for Pharmaceutical Preparations. Geneva, Switzerland: WHO; 2025 [cited 2025 Nov 30]. Available from: https://www.who.int/teams/health-product-policy-and-standards/standards-and-specifications/norms-and-standards-for-pharmaceuticals/expert-committee-on-specifications-for-pharmaceutical-preparations
20. ChemXpert [Internet]. Exploration of data types in the pharmaceutical industry. ChemXpert Blog. [cited 2025 Nov 30]. Available from: https://chemxpert.com/blog/exploration-of-data-types-in-the-pharmaceutical-industry
21. Oronsky B, Burbano E, Stirn M, Brechlin J, Abrouk N, Caroen S, Coyle A, Williams J, Cabrales P, Reid TR. Data Management 101 for drug developers: A peek behind the curtain. Clinical and Translational Science. 2023 Jun 20;16(9):1497-1509.
22. Pharmaceutical Journal [Internet]. How to understand and interpret clinical data. The Pharmaceutical Journal [cited 2025 Nov 30]. Available from: https://pharmaceutical-journal.com/article/ld/how-to-understand-and-interpret-clinical-data
23. Žagar J, Mihelič J. Big data collection in pharmaceutical manufacturing and its use for product quality predictions. Scientific data. 2022 Mar 23;9(1):1-11.
24. Handoo S, Arora V, Khera D, Nandi PK, Sahu SK. A comprehensive study on regulatory requirements for development and filing of generic drugs globally. International journal of pharmaceutical investigation. 2012 Jul;2(3):99-105.
25. Ahluwalia K, Abernathy MJ, Algorri M, Cauchon NS, Perico-Norred NM, Youssef RY. The future of regulatory filings: digitalization. AAPS Open. 2025 Apr 18;11(1):1-12.
26. Charoo NA, Khan MA, Rahman Z. Data integrity issues in pharmaceutical industry: Common observations, challenges and mitigations strategies. International journal of pharmaceutics. 2023 Jan 25;631:122503.
27. Jain SK. Strategy to avoid data integrity issues in pharmaceutical industry. The Pharma Innovation. 2017 Feb 1;6(2, Part B):110.
28. World Health Organization. Annex 4: TRS 1033 [Internet]. Geneva, Switzerland: WHO; 2025 [cited 2025 Nov 30]. Available from: https://www.who.int/publications/m/item/annex-4-trs-1033
29. Ajiga D, Okeleke PA, Folorunsho SO, Ezeigweneme C. Designing cybersecurity measures for enterprise software applications to protect data integrity. Computer Science & IT Research Journal. 2024 Aug 23;5(8):1920-1941.
30. Kantilal P D, Patil N A, Dhankani M, Pawar P S. Data Integrity Best Practices in Pharmaceutical Quality Assurance: A Thorough Review. Research & Reviews: A Journal of Pharmaceutical Science. 2024 Mar 30;15(1):22-30.
31. Boakai J. European Pharmaceutical Review [Internet]. Data integrity considerations in pharma and life sciences. European Pharmaceutical Review; 2024 Mar 12. [cited 2025 Nov 30]. Available from: https://www.europeanpharmaceuticalreview.com/article/219686/data-integrity-considerations-in-pharma-and-life-sciences/
32. Ige AB, Chukwurah N, Idemudia C, Adebayo VI. Managing data lifecycle effectively: Best practices for data retention and archival processes. International Journal of Engineering Research and Development. 2024 Jul 31;20(8):199-207.
33. Duggineni S. Data integrity and risk. Open Journal of Optimization. 2023 Jun 6;12(2):25-33.
34. Faunce TA. Global Clinical Trials: Effective Implementation and Management. JAMA. 2012 May 16;307(19):2105.
35. Svärd P. Enterprise Content Management and the Records Continuum Model as strategies for long-term preservation of digital information. Records Management Journal. 2013 Nov 25;23(3):159-176.
36. Saxena A. Audit Trail in Pharma: A Review. Asian Journal of Pharmaceutical Research. 2022;12(4):359-363.
37. Qualityze [Internet]. Internal quality audit pharmaceutical industry. Qualityze.com. 2025 [cited 2025 Nov 30]. Available from: https://www.qualityze.com/blogs/internal-quality-audit-pharmaceutical-industry
38. JAF Consulting. Good documentation practices for beginners: a step-by-step introduction [Internet]. JAF Consulting; 2025 [cited 2025 Nov 30]. Available from: https://jafconsulting.com/good-documentation-practices-for-beginners-a-step-by-step-introduction/
39. Knors Pharma. Regulatory inspections in pharmaceutical industry [Internet]. Knors Pharma Blog; 2025 Aug 21 [cited 2025 Nov 30]. Available from: https://www.knorspharma.com/blog/regulatory-inspections-in-pharmaceutical-industry/
40. IDBS. Data integrity in pharma industry [Internet]. IDBS Knowledge Base; 2024 Oct 21 [cited 2025 Nov 30]. Available from: https://www.idbs.com/knowledge-base/data-integrity-in-pharma-industry/
41. Adhao V, Ambhore J, Chaudhari S. Transforming pharmaceutical quality assurance and validation through artificial intelligence. Artificial Intelligence in Health. 2025 Aug 13:025160032.

42. Sembiring M H, Novagusda F N. Enhancing Data Security Resilience in AI-Driven Digital Transformation: Exploring Industry Challenges and Solutions Through ALCOA+ Principles. Acta Informatica Medica. 2024;32(1):65-70.
43. GxP-CC. How automating processes can simplify pharma data integrity compliance [Internet]. GxP-CC Insights Blog; 2022 Aug 24 [cited 2025 Nov 30]. Available from: https://www.gxp-cc.com/insights/blog/how-automating-processes-can-simplify-pharma-data-integrity-compliance/
44. Polu V S. Blockchain in Enterprise Resource Planning: Revolutionizing Supply Chain Transparency and Data Integrity.International Journal of Management Technology. 2025 Apr 16;12(1),48-57.
45. Lengston V. Blockchain for Public Health: Securing Data and Empowering Communities. European Journal of Medical and Health Research. 2025 May 1;3(3):4-10.
46. Sim C, Zhang H, Chang ML. Improving end-to-end traceability and pharma supply chain resilience using blockchain. Blockchain in Healthcare Today. 2022 Aug 12;5(31):1-10.
47. Padma A, Ramaiah M. Blockchain based solution for secure information sharing in pharma supply chain management. Heliyon. 2024 Nov 30;10(22): e40273.
48. Leal F, Chis A E, Caton S, 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 Research. 2021 May 15;24:100172.
49. 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 Nov 1;28(11):1-9.
50. Sridhar D. Leveraging blockchain technology for test data integrity in regulated industries. International journal. 2025 Feb 18;11(1):2927-2937.
51. Compliance Quest. Future trends in regulatory compliance for the pharmaceutical industry [Internet]. Compliance Quest: AI-powered PLM, QMS, EHS & SRM Platform. [cited 2025 Nov 30]. Available from: https://www.compliancequest.com/cq-guide/regulatory-compliance-future-trends/
52. GMP Compliance. FDA warning letter on missing audit trails and raw data review [Internet]. GMP Compliance News; 2025 Feb 24 [cited 2025 Nov 30]. Available from: https://www.gmp-compliance.org/gmp-news/fda-warning-letter-on-missing-audit-trails-and-raw-data-review