Safeguarding Data Integrity in Pharmaceutical Manufacturing

ABSTRACT

Aims: Comprehensively analyze data integrity challenges in the pharmaceutical industry, analyze regulatory observations, and propose mitigation strategies for ensuring compliance with current good manufacturing practices (cGMP), particularly for electronic data and computerized systems.

Study design: Analysis of regulatory documents, industry-standard guides, and case studies.

Methodology: The study involved a comprehensive review of FDA guidance documents, warning letters, and Form 483 observations related to data integrity. Case studies of non-compliance were analyzed to identify common issues and consequences. Technical, organizational, and behavioral factors contributing to data integrity problems were examined. Mitigation strategies and best practices were compiled based on industry guidelines and expert recommendations.

Results: Data integrity violations often involve data falsification, poor retention, and electronic record manipulation. Non-compliant firms have faced severe penalties for non-compliance. Challenges include legacy systems, complex data management, inadequate training, and global supply chains. Mitigation strategies involve data governance, risk-based validation, access controls, comprehensive training, and advanced technologies like blockchain.

Conclusion: Data integrity remains a critical challenge in the pharmaceutical industry, requiring a holistic approach that combines technological solutions with organizational and cultural best practices. Implementing robust data governance systems, fostering a quality culture, and leveraging advanced technologies can significantly improve compliance and reduce risks associated with data integrity issues.

1. INTRODUCTION

Data integrity (DI) is critical to ensuring drug safety, efficacy, and quality in the pharmaceutical industry. It refers to data accuracy, consistency, and reliability throughout its lifecycle, from initial generation to final disposition (Charoo et al., 2023). Data integrity is essential for supporting regulatory decision-making, maintaining public trust, and protecting patient safety (Davidson, 2016). Regulatory agencies such as the United States Food and Drug Administration (FDA) and European Medicines Agency (EMA) have issued numerous guidelines to help companies maintain DI and comply with current good manufacturing practices (cGMP), good clinical practices (GCP), and good laboratory practices (GLP) (George et al., 2017). These guidelines provide a

framework for implementing robust data governance systems and ensuring data reliability in drug development, manufacturing, and distribution. However, recent FDA Form 483 observations and warning letters indicate that DI remains a significant industry challenge. Failure to comply with DI requirements can lead to invalidated results, post-marketing issues, product recalls, and severe regulatory consequences (Davidson, 2016). DI lapses can compromise the quality of drugs, leading to potential risks to patient safety and public health.

The consequences of DI non-compliance extend beyond regulatory sanctions. Companies may face significant financial losses due to delayed product approvals, lost revenue from recalled products, and the cost of remediation efforts (George et al., 2017). Reputational damage can also substantially erode public trust and investor confidence in the company and the industry. Therefore, pharmaceutical companies must stay current with DI expectations and implement robust data governance practices. This requires a comprehensive understanding of regulatory requirements, potential risks, and best practices for ensuring data reliability throughout the product's lifecycle.

This paper reviews data integrity (DI) in the pharmaceutical industry, focusing on challenges, regulatory observations, and mitigation strategies within cGMP, particularly for electronic data and computerized systems. It covers FDA guidance, common deficiencies, and case studies of non-compliance. The paper explores technical, organizational, and behavioral factors contributing to DI issues and discusses mitigation strategies, including key elements of data governance programs. By providing this comprehensive review, the paper aims to help pharmaceutical companies maintain compliance and promote a culture of quality and continuous improvement based on reliable data.

2. OVERVIEW OF FDA GUIDANCE ON DATA INTEGRITY

The FDA has published several key guidance documents outlining DI expectations for the pharmaceutical industry. These guidelines provide a framework for ensuring the reliability and integrity of data used in drug development, manufacturing, and distribution.

One of the most significant guidance documents is the "Data Integrity and Compliance With Drug CGMP" published in 2018 (Center for Drug Evaluation and Research, 2018). This guidance defines the ALCOA+ principles, which state that data should be attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and available. These principles form the foundation for assessing and mitigating DI risks throughout the data lifecycle. The ALCOA++ principles are explained in the following Table 1 (International Society for Pharmaceutical Engineering, 2017; European Medicines Agency, 2023).

Table 1: ACLOA++ Principles

Principle	**Description**
Attributable	Data should be linked to its source, including the individual who generated or recorded it and the date and time of creation.
Legible	Data must be readable and understandable, with any changes or corrections clearly documented.
Contemporaneous	Data should be recorded at the time of the activity, ensuring a complete and accurate representation of events.
Original	Data should be preserved in its original form, whether recorded on paper or electronically.
Accurate	Data should be free from errors, mistakes, and bias, reflecting the true nature of the activity or event.
Complete	Data should include all relevant information without any omissions or deletions.
Consistent	Data should be free from unexplained discrepancies or contradictions within a single record and across related records.
Enduring	Data should remain intact and accessible throughout the required retention

	period, protected from loss, damage, or alteration.
Available	Data should be readily retrievable and accessible in a timely manner for review, analysis, or inspection.
Traceable	Data should be traceable throughout its lifecycle, from creation through processing, use, retention, and disposition.

Failing to meet these ALCOA++ principles can compromise data quality and regulatory non-compliance (Center for Drug Evaluation and Research, 2018). The regulations and guidance documents provide recommendations for ensuring the DI of both paper and electronic data, emphasizing the need for robust data governance systems, standard operating procedures (SOPs), and regular training and audits.

Another critical guidance is "Part 11 - Electronic Records; Electronic Signatures – Scope and Application," published in 2003 (U.S. Food and Drug Administration, 2003). This guidance specifies the criteria for electronic records and signatures to be considered trustworthy and equivalent to paper records. It requires the implementation of controls such as limited system access, computer system validation, audit trails, and data backup. 21 CFR Part 11 compliance is essential for ensuring the integrity of electronic data, which is increasingly prevalent in modern pharmaceutical operations. The guidance requires that electronic records are protected from unauthorized access, modification, or deletion and that any changes are captured securely and traceably.

The FDA guidance documents on DI provide a comprehensive framework for ensuring the reliability and trustworthiness of data in the pharmaceutical industry. By adhering to the ALCOA++ principles and implementing robust controls for electronic records and signatures, companies can mitigate DI risks and maintain compliance with regulatory requirements (Alosert et al., 2022). However, it is important to recognize that DI is not a one-time effort but an ongoing process that requires continuous monitoring, assessment, and improvement. Companies must stay current with evolving regulatory expectations and industry best practices and regularly review and update their data governance systems to ensure ongoing effectiveness (International Society for Pharmaceutical Engineering, 2017).

3. REGULATORY OBSERVATIONS AND CONSEQUENCES OF NON-COMPLIANCE

A review of recent FDA Form 483s and warning letters reveals several recurring themes related to DI deficiencies in the pharmaceutical industry. These observations highlight the challenges companies face in maintaining compliance with regulatory requirements and the potential consequences of non-compliance (Jaiswal et al., 2020).

Commonly found data integrity violations are (Perez, 2017)

- Falsifying dates on documents or records
- Manipulating or modifying original information and documentation
- Fabricating favorable test outcomes without conducting actual tests
- Preemptively recording procedures or actions before they occur
- Supplementing quality assurance data packages with removable adhesive notes

Inadequate data retention and missing raw data and metadata are other frequently cited DI deficiencies (Perez, 2017). Companies must retain complete and accurate records of GMP activities, including raw data and metadata, for a specified period. Failure to properly retain and protect this data can lead to gaps in the documentation and make it difficult to reconstruct events or investigate discrepancies (George et al., 2017). The consequences of these DI lapses can be severe, including costly delays, rejected batches, product recalls, import alerts, injunctions, and even criminal prosecution. In addition to the direct financial impact, companies may also face significant reputational damage, eroding public trust and investor confidence.

Several case studies illustrate the far-reaching consequences of DI non-compliance.

3.1 Ranbaxy Laboratories

Ranbaxy faced a major data integrity scandal in the early 2000s. The company was found to have systematically falsified drug data and test results for years, compromising the quality and safety of its products. Investigations revealed widespread issues, including fabricated stability data, altered test parameters, and using raw materials from unapproved sources (Center for Drug Evaluation and Research, 2023a).

In 2013, Ranbaxy pleaded guilty to seven federal criminal counts in the U.S., including falsifying data to FDA regulators. The company paid $500 million in fines and settlements (U.S Department of Justice, 2013). This case highlighted the critical importance of data integrity in pharmaceutical manufacturing and led to increased scrutiny of global drug supply chains, particularly those involving manufacturers in developing countries.

3.2 Intas Pharmaceuticals

Intas Pharmaceuticals faced significant data integrity issues in 2023. The U.S. FDA inspection of their facility revealed severe violations, including data manipulation and poor documentation practices. Investigators found evidence of deleted data, backdated records, and unauthorized changes to electronic files. The company was accused of retesting samples until passing results were obtained and failing to maintain complete records of all tests performed. These practices raised concerns about the reliability of their quality control processes and the safety of their products (Center for Drug Evaluation and Research, 2023b). As a result, the FDA issued a warning letter and import alert, effectively banning Intas products from entering the U.S. market (U.S. Food and Drug Administration, 2023). This case underscores the ongoing challenges in maintaining data integrity in the pharmaceutical industry and the severe consequences of non-compliance.

3.3. Synchron Research Services

Synchron Research Services faced severe data integrity issues in 2020. The U.S. FDA and European Medicines Agency (EMA) inspections uncovered widespread data manipulation and fraudulent practices in bioequivalence studies conducted by the company. Investigators found evidence of data falsification, including the fabrication of subject participation in trials and manipulation of analytical results. The company was accused of selectively reporting data and altering chromatograms to achieve desired outcomes. As a result, the U.S. FDA adjudicated that the results for studies conducted at Synchron is unacceptable and advised companies to repeat bioequivalence studies conducted by Synchron at other facilities (Center for Drug Evaluation and Research, 2021).

This case highlighted the critical importance of data integrity in clinical research and the potential far-reaching consequences of fraudulent practices in CROs.

3.4. Quest Life Sciences

The World Health Organization (WHO) inspected the Quest Life Sciences facility and uncovered severe violations in their clinical trial practices. Investigators found evidence of data fabrication and manipulation in a bioequivalence study for an HIV/AIDS medication. The issues included falsified electrocardiogram (ECG) reports and fabricated patient participation records. Some patients' ECG results were identical, suggesting copying and pasting of data (World Health Organization, 2015). As a result, the WHO issued a notice of concern, recommending that medicines tested by Quest should not be approved for use based on these studies (World Health Organization, 2015). This case underscored the critical importance of data integrity in clinical trials and the potential impact on global public health.

These examples underscore the critical importance of DI in the pharmaceutical industry and the severe consequences of non-compliance. Companies must prioritize DI in their quality systems, implement robust controls and governance measures, and foster a culture of quality and compliance at all levels of the organization.

4. CHALLENGES AND CONTRIBUTING FACTORS

4.1. Technical Challenges in Data Management and Systems

The pharmaceutical industry faces significant technical hurdles in maintaining data integrity. Many companies still rely on legacy computer systems that lack proper controls and audit trail capabilities. These outdated systems often fail to align with current data integrity regulations and may not have necessary security features, access controls, or data management capabilities. Upgrading or replacing these systems is a costly and time-consuming process, requiring careful planning to avoid disruptions to ongoing operations (Ullagaddi, 2024a). Modern analytical technologies, such as process analytical technology (PAT) and various "omics" techniques (genomics, proteomics, etc.), generate large volumes of complex, high-dimensional data. Ensuring the integrity and traceability of this data throughout its lifecycle is challenging, particularly when dealing with multiple data sources and formats. This requires sophisticated data management systems and expertise in handling big data in a compliant manner (Steinwandter & Herwig, 2019). The lack of standardization in data formats and structures across different instruments and systems further complicates data integrity efforts. When data is generated and stored in disparate formats, it becomes difficult to integrate, compare, and analyze, potentially leading to errors and discrepancies (Ullagaddi, 2024b). The development and adoption of standardized data formats and protocols, such as the Allotrope Foundation's Allotrope Data Format (ADF), can help address this challenge by facilitating data interoperability and integrity across different platforms and processes (Ullagaddi, 2024c).

4.2. Organizational Factors Impacting Data Integrity

Organizational issues significantly impact data integrity compliance. Implementing effective data governance systems and processes requires substantial investments in technology, personnel, and training. Without sufficient resources and management commitment, data integrity initiatives may not receive the attention and priority they require, leading to gaps in compliance and increased risk of data integrity issues (Osvaldo, 2017). The complexity of the pharmaceutical supply chain, involving numerous third-party suppliers, contract manufacturers, and service providers, creates additional data integrity challenges (Parmar et al., 2020). Ensuring the integrity and reliability of data generated by external partners requires robust due diligence, clear contractual agreements, and ongoing oversight and monitoring. Failure to adequately assess and manage the data integrity risks associated with third-party relationships can lead to compliance issues and potential liability for the sponsor company (Perez, 2017).

The organizational culture plays a crucial role in maintaining data integrity. A culture that prioritizes production speed or cost-cutting over quality and compliance can inadvertently encourage practices that compromise data integrity. Establishing a strong quality culture that values data integrity at all levels of the organization is essential for long-term compliance and risk mitigation (Manzano & Langer, n.d.).

4.3. Human and Behavioral Factors Affecting Data Integrity Compliance

Inadequate training on data integrity principles, regulations, and best practices can contribute to human errors and compliance failures. When employees do not have a clear understanding of their roles and responsibilities in maintaining data integrity or lack the necessary skills and knowledge to properly manage and protect data, the risk of data integrity issues increases (Ullagaddi, 2024c). Regular and effective training on data integrity, tailored to the specific needs and responsibilities of different roles, is essential for promoting a culture of quality and compliance. Behavioral factors, such as complacency, shortcuts, and workarounds, can also undermine data integrity efforts. This can include failing to follow standard operating procedures (SOPs), skipping required documentation steps, or manipulating data to avoid additional work or delays (Jaiswal et al., 2020).

4.4. Oversight and Monitoring Mechanisms for Ensuring Data Integrity

Lack of effective oversight and monitoring is a significant barrier to maintaining data integrity. Without adequate checks and balances in place to detect and prevent data integrity issues, such as regular audits and

reviews of data and records, non-compliant practices can go unnoticed and become entrenched (Isaak Kavasidis et al., 2022). Establishing robust monitoring and audit programs, with clear roles and responsibilities for data review and verification, is essential for identifying and addressing data integrity risks in a timely manner (James et al., 2021).

Effective oversight requires a multi-layered approach, including automated system checks, regular internal audits, and periodic external assessments. Implementing electronic systems with built-in data integrity controls, such as audit trails, time-stamped records, and user access controls, can help prevent and detect many common data integrity issues (Kulkarni & Kothari, 2024). However, human oversight and review processes must complement these technical solutions to ensure their effectiveness and to catch more subtle or complex data integrity problems. Developing key performance indicators (KPIs) for data integrity and regularly monitoring these metrics can help organizations identify trends and potential issues before they escalate into serious compliance problems. This proactive approach to data integrity management can save significant time and resources in the long run by preventing costly remediation efforts and regulatory actions (Parmar et al., 2020).

4.5. Global Regulatory Challenges in Data Integrity Compliance

The increasing globalization of the pharmaceutical industry presents unique challenges for data integrity compliance. Companies must navigate and comply with multiple regulatory requirements across different jurisdictions, each with its own specific expectations and standards for data integrity (Rattan, 2017). Differences in regulations, standards, and expectations across countries can make it difficult to establish consistent and harmonized data integrity practices throughout the global supply chain.

Ensuring compliance with diverse regulatory requirements demands a thorough understanding of the specific data integrity expectations and requirements in each jurisdiction, as well as effective communication and coordination among different sites and functions (Ronolo, 2023). This may require developing flexible yet robust data integrity systems and processes that can adapt to varying regulatory landscapes while maintaining a consistent level of quality and compliance. Moreover, regulatory agencies worldwide increasingly focus on data integrity in their inspections and enforcement actions. Companies must stay abreast of evolving regulatory expectations and be prepared to demonstrate the integrity and reliability of their data to multiple regulatory bodies (Khin et al., 2020). This often requires investing in advanced data management systems, conducting regular internal and external audits, and fostering a culture of transparency and continuous improvement in data integrity practices. Addressing these multifaceted challenges requires a comprehensive and systematic approach to data integrity management (Leal et al., 2021). Organizations must conduct thorough risk assessments that consider technical, organizational, human, and regulatory factors to identify and prioritize their most significant data integrity vulnerabilities.

Ultimately, maintaining data integrity in the pharmaceutical industry is an ongoing process that requires continuous attention, resources, and adaptation to evolving technologies and regulatory expectations (Pedro et al., 2023). By taking a holistic and proactive approach to data integrity, pharmaceutical companies can ensure regulatory compliance and enhance the quality, safety, and efficacy of their products, thereby protecting patient safety and maintaining public trust in the pharmaceutical industry (Rogers et al., 2020).

5. MITIGATION STRATEGIES AND BEST PRACTICIES

Establishing a robust data governance program integrated with the pharmaceutical quality system is fundamental to addressing DI issues and ensuring compliance with regulatory requirements. An effective data governance program should be risk-based, scalable, and flexible, considering the specific needs and characteristics of the organization and its products (Steinwandter & Herwig, 2019; Manzano & Langer, n.d.).

5.1 Management Commitment and Leadership

One of the critical elements of a successful data governance program is management commitment and leadership (Leal et al., 2021). Senior management must set the tone for quality and DI, communicating their expectations clearly and consistently throughout the organization. This includes providing adequate resources,

support, and oversight for DI initiatives and fostering a culture of transparency, accountability, and continuous improvement (Hock et al., 2020).

5.2 Risk-Based GxP Validations

Another critical component of data governance is the risk-based validation of GxP computerized systems. This involves a systematic approach to assessing the potential impact of computerized systems on product quality and patient safety and establishing appropriate controls and testing requirements based on the level of risk. The validation process should cover the entire lifecycle of the system, from design and development through operation and retirement, and should be regularly reviewed and updated as needed (Ullagaddi, 2024b; Ullagaddi, 2024e).

5.3 Access Controls and User Management

Access controls and user management establish firm governance and prevent unauthorized access in computerized systems (George et al., 2017). This includes establishing clear roles and responsibilities for system users, with well-defined access privileges based on job function and need-to-know principles. User access should be regularly reviewed and updated, with prompt removal of access for terminated or transferred employees. Strong authentication mechanisms, such as unique user IDs and passwords, should be in place to prevent unauthorized access and ensure traceability of actions (Ullagaddi, 2024c).

5.4 Audit Trails and Review

Audit trails are another key component for ensuring DI in computerized systems (Huy, 2023). Audit trails should capture a complete and accurate record of all GxP-relevant actions, including data creation, modification, and deletion, as well as system configuration changes and security events. Audit trails should be secure, tamper-evident, and regularly reviewed as part of data review and approval processes. The frequency and extent of audit trail review should be based on a risk assessment, considering the criticality of the data and the potential impact on product quality and patient safety (Ullagaddi, 2024d).

5.5 Data Review and Approval Procedures

Data review and approval procedures are critical for ensuring the accuracy, completeness, and consistency of GxP records (James et al., 2021). This includes establishing clear roles and responsibilities for data review and approval and appropriately segregating duties to prevent conflicts of interest or undue influence. Data should be reviewed in a timely manner, with any discrepancies or errors promptly investigated and resolved. The review process should include a comparison of source data with reported results, as well as a check for completeness and consistency across different records and systems (Pravin Ullagaddi, 2024).

5.6 Data Retention and Backup

Data retention and backup are also essential elements of a robust data governance program (George et al., 2017). GxP records should be retained for a minimum period of time, as specified by regulatory requirements and company policies. Records should be stored in a secure and accessible manner, protected from unauthorized access, alteration, or destruction. Regular backups should be performed and tested to ensure the availability and integrity of data in the event of a system failure or disaster (International Society for Pharmaceutical Engineering, 2017). Procedures should be in place for the secure and controlled destruction of records once the retention period has expired.

5.7 Training and Awareness

Training and awareness are critical for promoting a culture of quality and DI (Bunn, 2019). All employees involved in GxP activities should receive regular training on DI principles, regulations, and best practices, tailored to their specific roles and responsibilities. Training should cover data management, record-keeping, system use, and error detection and correction (Alosert et al., 2022). Employees should also be trained in the importance of DI, the consequences of non-compliance, and their individual roles and responsibilities in maintaining data integrity.

5.8 Periodic Audits and Assessments

Periodic internal audits and assessments are essential for monitoring the effectiveness of data governance programs and identifying areas for improvement (Charoo et al., 2023). Audits should be risk-based, focusing on the areas of greatest vulnerability or criticality, and should cover all aspects of data management and integrity, including policies, procedures, systems, and records (Durá et al., 2022). Audit findings should be documented and communicated to management, with corrective and preventive actions (CAPAs) developed and

implemented promptly. The effectiveness of CAPAs should be monitored and assessed through follow-up audits or reviews (Durà-Hernández et al., 2023).

5.9 Automation and Technology Solutions

In addition to these core elements of data governance, several best practices can help organizations strengthen their DI programs and reduce the risk of compliance issues (Durá et al., 2022). One such practice is the use of electronic batch records (EBRs) and laboratory information management systems (LIMS) for automated data capture and processing (Ullagaddi, 2024e). These systems can help reduce the risk of human error and data manipulation by automating data entry, calculations, and reporting. They can also provide a complete and accurate record of all actions and events, with secure audit trails and access controls. However, implementing EBRs and LIMS requires careful planning, validation, and training to ensure they are fit for purpose and compliant with regulatory requirements. Another best practice is using process analytical technology (PAT) for real-time monitoring and control of manufacturing processes (George et al., 2017). PAT tools, such as near-infrared and Raman spectroscopy, can provide continuous, non-destructive measurements of critical quality attributes, enabling faster and more efficient process optimization and quality control. PAT data can also support continuous process verification and real-time release testing, reducing the reliance on end-product testing and increasing manufacturing operations' overall quality and efficiency.

Blockchain technology is also emerging as a promising tool for enhancing DI and traceability in the pharmaceutical supply chain (Isaak Kavasidis et al., 2022). Blockchain provides a secure, transparent, and immutable record of transactions and data, enabling the creation of a tamper-proof audit trail. This can help prevent data falsification and manipulation and improve the visibility and accountability of supply chain activities. However, implementing blockchain requires significant technical expertise and infrastructure, as well as careful consideration of data privacy and security issues. Cloud computing can help organizations improve data management and integrity while reducing costs and increasing scalability (Parmar et al., 2020). Cloud-based solutions can provide secure, reliable, and accessible storage and processing of GxP data, with built-in backup and disaster recovery capabilities. They can also enable real-time data sharing and collaboration across different sites and functions, improving data management and analysis efficiency and effectiveness. Using cloud computing requires careful assessment of data privacy, security, and compliance risks, as well as the establishment of clear service level agreements and monitoring mechanisms (Ullagaddi, 2024c).

5.10 Organizational and Cultural Best Practices

While these technological solutions can significantly benefit DI and compliance, it is essential to recognize that they are not a panacea. These tools' practical implementation and use require a robust data governance foundation, including policies, procedures, training, and oversight (Huy, 2023). Organizations must also be prepared to invest in the necessary infrastructure, expertise, and resources to ensure these systems' ongoing maintenance and validation. In addition to technological solutions, several organizational and cultural best practices can help promote DI and compliance (George et al., 2017). One such practice is establishing a cross-functional DI team or council, with representation from different departments and levels of the organization. This team can help coordinate and oversee DI initiatives, provide guidance and support to different functions, and ensure the consistent application of policies and procedures across the organization. The team should have clear roles and responsibilities and the authority and resources to carry out its mandate effectively (Hock et al., 2020).

Another best practice is promoting a culture of quality and compliance, where DI is seen as a shared responsibility of all employees rather than just a regulatory requirement. This requires leadership commitment and engagement, as well as ongoing communication and reinforcement of DI principles and expectations. Organizations should encourage open dialogue and reporting of DI issues without fear of retaliation or punishment (Perez, 2017). The mitigation strategies are summarized in Figure 1.

Figure 1: Mitigation Strategies and Best Practices for Effective Data Governance and Data Integrity in the Pharmaceutical Industry.

6. Conclusion

Data integrity is a critical foundation of the pharmaceutical quality system, underpinning the industry's ability to consistently deliver safe, effective, and high-quality medicines to patients. As the pharmaceutical landscape becomes increasingly complex and data-driven, the importance of effective data governance and DI practices has never been greater. The FDA's guidance on DI, including the ALCOA+ principles and Part 11 requirements for electronic records and signatures, provides a clear and comprehensive framework for data governance and compliance. However, the effective implementation of this guidance requires a risk-based and holistic approach, considering each organization's specific needs, capabilities, and constraints. Organizations that prioritize DI as a core value and that invest in the necessary resources, expertise, and oversight to support data governance are more likely to achieve and sustain compliance with regulatory expectations. The increasing adoption of advanced technologies, such as process analytical technology, blockchain, and cloud computing, offers significant opportunities for enhancing DI and efficiency in pharmaceutical operations. However, implementing these technologies must be carefully planned and validated, with appropriate controls and safeguards in place to ensure data reliability, security, and privacy.

Ultimately, the key to success in DI is to develop a proactive, collaborative, and agile approach to data governance that can adapt to the evolving regulatory landscape and technological innovations. This requires ongoing investment in people, processes, and technology and a willingness to learn from mistakes and continuously improve. By embracing DI as a core element of the pharmaceutical quality system and by implementing the best practices and recommendations outlined in this paper, organizations can significantly reduce the risk of compliance issues and ensure the continued delivery of safe and effective medicines to patients. This is not only a regulatory imperative but also a moral and ethical responsibility of the industry, one that requires the commitment and engagement of all stakeholders, from senior leadership to front-line employees. As the pharmaceutical industry continues to evolve and innovate, the importance of DI will only continue to grow. By staying abreast of regulatory expectations, investing in robust data governance systems, and fostering a culture of quality and compliance, organizations can position themselves for success in this data-driven future and continue to play a vital role in promoting and protecting public health.

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc) and text-to-image generators have been used during writing or editing of manuscripts.

REFERENCES

1. Alosert, H., Savery, J., Rheaume, J., Cheeks, M., Turner, R., Spencer, C., S. Farid, S., & Goldrick, S. (2022). Data integrity within the biopharmaceutical sector in the era of Industry 4.0. *Biotechnology Journal*, *17*(6), 2100609. https://doi.org/10.1002/biot.202100609
2. Bunn, G. P. (2019). *Good manufacturing practices for pharmaceuticals*. Crc Press, Taylor & Francis Group.
3. Center for Drug Evaluation and Research. (2018). *Data Integrity and Compliance With Drug CGMP: Questions and Answers*. U.S. Food and Drug Administration. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-integrity-and-compliance-drug-cgmp-questions-and-answers
4. Center for Drug Evaluation and Research. (2021). *Notification to Pharmaceutical Companies: Clinical and Bioanalytical Studies Conducted by Panexcell Clinical Lab or Synchron Research Services Are Unacceptable*. https://www.fda.gov/drugs/drug-safety-and-availability/notification-pharmaceutical-companies-clinical-and-bioanalytical-studies-conducted-panexcell
5. Center for Drug Evaluation and Research. (2023a). Regulatory Actions Against Ranbaxy and Sun Pharma. *FDA*. https://www.fda.gov/drugs/enforcement-activities-fda/regulatory-actions-against-ranbaxy-and-sun-pharma
6. Center for Drug Evaluation and Research. (2023b, November 28). *Intas Pharmaceuticals Limited - 662868 - 11/21/2023*. FDA. https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/intas-pharmaceuticals-limited-662868-11212023
7. Charoo, N. A., Khan, M. A., & Rahman, Z. (2023). Data integrity issues in pharmaceutical industry: Common observations, challenges and mitigations strategies. *International Journal of Pharmaceutics*, *631*, 122503. https://doi.org/10.1016/j.ijpharm.2022.122503
8. Davidson, J. (2016). The Real Cost of Poor Data Integrity in Pharmaceutical Manufacturing. In *lachmanconsultants.com*. https://www.lachmanconsultants.com/wp-content/uploads/2016/08/Pharmaceutical-Engineering-July-Aug-2016.pdf
9. Durá, M., Sánchez-García, Á., Sáez, C., Leal, F., Chis, A. E., González-Vélez, H., & García-Gómez, J. M. (2022). Towards a Computational Approach for the Assessment of Compliance of ALCOA+ Principles in Pharma Industry. *Studies in Health Technology and Informatics*, *294*. https://doi.org/10.3233/shti220578
10. Durà-Hernández, M., Leal, F., Angel Sánchez García, Sáez, C., Juan Miguel García-Gómez, Chis, A. E., & González-Vélez, H. (2023). Blockchain for Data Originality in Pharma Manufacturing. *Journal of Pharmaceutical Innovation*, *18*. https://doi.org/10.1007/s12247-023-09748-z
11. European Medicines Agency . (2023). *Guideline on computerised systems and electronic data in clinical trials*. https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-computerised-systems-and-electronic-data-clinical-trials_en.pdf
12. George, R., Truong, T., & Davidson, J. (2017). Establishing an Effective Data Governance System: Data governance is necessary for compliance with current regulatory expectations or data integrity in pharmaceutical R&D and manufacturing organizations. *Pharmaceutical Technology Europe*, *29*(11), 40–44. https://link.gale.com/apps/doc/A551975175/AONE?u=anon~12cf7ffd&sid=googleScholar&xid=f0e45a9d

13. Hock, S. C., Tay, V., Sachdeva, V., & Wah, C. L. (2020). Pharmaceutical Data Integrity: issues, challenges and proposed solutions for manufacturers and inspectors. *Generics and Biosimilars Initiative Journal*, *9*(4), 171–183. https://link.gale.com/apps/doc/A677574409/AONE?u=anon~d991cc42&sid=googleScholar&xid=570480b5
14. Huy, H. V. (2023). Ensuring Data Integrity in Quality Control: Completeness, Consistency, and Accuracy in Pharmaceutical Processes. *Emerging Trends in Machine Intelligence and Big Data*, *15*(11), 43–55. https://orientreview.com/index.php/etmibd-journal/article/view/66
15. International Society for Pharmaceutical Engineering. (2017). *ISPE GAMP Records and Data Integrity Guide*. International Society for Pharmaceutical Engineering.
16. Isaak Kavasidis, Lallas, E. N., Gerogiannis, V. C., & Karageorgos, A. (2022). Analytics and Blockchain for Data Integrity in the Pharmaceuticals Industry. *2022 4th International Conference on Advances in Computer Technology, Information Science and Communications (CTISC)*. https://doi.org/10.1109/ctisc54888.2022.9849776
17. Jaiswal, H., S., M. B., & Kulyadi, G. P. (2020). Data Integrity Violations: A Challenge to the Pharmaceutical Industry. *International Journal of Pharmaceutical Quality Assurance*, *11*(01), 196–198. https://doi.org/10.25258/ijpqa.11.1.30
18. James, R., Das, S., Kumari, A., Rekdal, M., Kulyadi, G. P., & Sathyanarayana, M. B. (2021). A Recent Regulatory Update on Consequences of Data Integrity Issues and its Management in Pharmaceutical Scenario. *Indian Journal of Pharmaceutical Education and Research*, *55*(2s), s616–s622. https://doi.org/10.5530/ijper.55.2s.134
19. Khin, N. A., Francis, G., Mulinde, J., Grandinetti, C., Skeete, R., Yu, B., Ayalew, K., Cho, S., Fisher, A., Kleppinger, C., Ayala, R., Bonapace, C., Dasgupta, A., Kronstein, P. D., & Vinter, S. (2020). Data Integrity in Global Clinical Trials: Discussions From Joint US Food and Drug Administration and UK Medicines and Healthcare Products Regulatory Agency Good Clinical Practice Workshop. *Clinical Pharmacology & Therapeutics*, *108*(5), 949–963. https://doi.org/10.1002/cpt.1794
20. Kulkarni, P., & Kothari, C. (2024). Documentation and Data Integrity in Pharmaceutical Industry. *Modern Aspects of Pharmaceutical Quality Assurance*, 381–403. https://doi.org/10.1007/978-981-99-9271-3_11
21. 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., Lallas, E., Ntounas, T., Vasileiou, E., Mountzouris, G., Otti, B., Pucci, P., Papini, R., Cerrai, D., & Mier, M. (2021). Smart Pharmaceutical Manufacturing: Ensuring End-to-End Traceability and Data Integrity in Medicine Production. *Big Data Research*, *24*, 100172. https://doi.org/10.1016/j.bdr.2020.100172
22. M., V., & G. N. K., G. (2020). CURRENT STATUS, CHALLENGES AND PREVENTIVE STRATEGIES TO OVERCOME DATA INTEGRITY ISSUES IN THE PHARMACEUTICAL INDUSTRY. *International Journal of Applied Pharmaceutics*, *12*(6), 19–23. https://doi.org/10.22159/ijap.2020v12i6.38987
23. Manzano, T., & Langer, G. (n.d.). *GETTING READY FOR PHARMA 4.0 Data integrity in cloud and big data applications*. Retrieved November 20, 2021, from https://www.ispe.gr.jp/ISPE/02_katsudou/pdf/201812_en.pdf
24. Osvaldo. (2017). Data Integrity Implementation Strategy for Pharma Industry. *Handle.net*. http://hdl.handle.net/20.500.12475/399
25. Parmar, J., Mehta, P., Patel, R., Shah, M., & Kothari, C. (2020). Raw Data Management and Data Integrity in Pharmaceutical Product development. *Applied Clinical Research, Clinical Trials and Regulatory Affairs*, *7*(3). https://doi.org/10.2174/2213476x07999200901110354
26. Pedro, F., Veiga, F., & Filipa Mascarenhas-Melo. (2023). Impact of GAMP 5, data integrity and QbD on quality assurance in the pharmaceutical industry: How obvious is it? *Drug Discovery Today*, *28*(11), 103759–103759. https://doi.org/10.1016/j.drudis.2023.103759

27. Perez, J. (2017). Maintaining data integrity. *In Quality Progress*, *50*(3), 14–16. https://bec-global.com/wp-content/uploads/2017/10/Article-Data-Integrity.pdf.
28. Pravin Ullagaddi. (2024). Digital Transformation Strategies to Strengthen Quality and Data Integrity in Pharma. *International Journal of Business and Management*, *19*(5), 16–16. https://doi.org/10.5539/ijbm.v19n5p16
29. Rattan, A. K. (2017). Data Integrity: History, Issues, and Remediation of Issues. *PDA Journal of Pharmaceutical Science and Technology*, *72*(2), 105–116. https://doi.org/10.5731/pdajpst.2017.007765
30. Rogers, C. A., Ahearn, J. D., & Bartlett, M. G. (2020). Data Integrity in the Pharmaceutical Industry: Analysis of Inspections and Warning Letters Issued by the Bioresearch Monitoring Program Between Fiscal Years 2007–2018. *Therapeutic Innovation & Regulatory Science*, *54*(5), 1123–1133. https://doi.org/10.1007/s43441-020-00129-z
31. Ronolo, S. C. (2023). *Assuring Data Integrity towards Regulatory Compliance: A Study on Process Improvement in Data Integrity Compliance of Computerized Systems*. Www.theseus.fi. https://urn.fi/URN:NBN:fi:amk-2023052614535
32. Steinwandter, V., & Herwig, C. (2019). Provable Data Integrity in the Pharmaceutical Industry based on Version Control Systems and the Blockchain. *PDA Journal of Pharmaceutical Science and Technology*, *73*(4), pdajpst.2018.009407. https://doi.org/10.5731/pdajpst.2018.009407
33. U.S Department of Justice. (2013, May 13). *Generic Drug Manufacturer Ranbaxy Pleads Guilty and Agrees to Pay $500 Million to Resolve False Claims Allegations, cGMP Violations and False Statements to the FDA*. Justice.gov. https://www.justice.gov/opa/pr/generic-drug-manufacturer-ranbaxy-pleads-guilty-and-agrees-pay-500-million-resolve-false
34. U.S. Food and Drug Administration. (2003). *Guidance for Industry Part 11, Electronic Records; Electronic Signatures -Scope and Application Pharmaceutical CGMPs*. https://www.fda.gov/media/75414/download
35. U.S. Food and Drug Administration. (2023). *Import Alert 66-40*. Www.accessdata.fda.gov. https://www.accessdata.fda.gov/cms_ia/importalert_189.html
36. Ullagaddi, P. (2024a). Digital Transformation in the Pharmaceutical Industry: Enhancing Quality Management Systems and Regulatory Compliance. *International Journal of Health Sciences*, *12*(1), 31–43. https://doi.org/10.15640/ijhs.v12n1a4
37. Ullagaddi, P. (2024b). GDPR: Reshaping the Landscape of Digital Transformation and Business Strategy. *Www.ijbmm.com International Journal of Business Marketing and Management*, *9*(2), 29–35. https://ijbmm.com/paper/Mar2024/8340436609.pdf
38. Ullagaddi, P. (2024c). Digital Transformation in the Pharmaceutical Industry: Ensuring Data Integrity and Regulatory Compliance. *International Journal of Business & Management*. https://doi.org/10.24940/theijbm/2024/v12/i3/bm2403-013
39. Ullagaddi, P. (2024d). Leveraging Digital Transformation for Enhanced Risk Mitigation and Compliance in Pharma Manufacturing. *Journal of Advances in Medical and Pharmaceutical Sciences*, *26*(6), 75–86. https://doi.org/10.9734/jamps/2024/v26i6697
40. Ullagaddi, P. (2024e). Digital Transformation Strategies to Strengthen Quality and Data Integrity in Pharma. *International Journal of Business and Management*, *19*(5), 16–26. https://doi.org/10.5539/ijbm.v19n5p16
41. World Health Organization. (2015, June 30). *Prequalification Team - Inspection Services Notice of Concern*. https://rx-360.org/wp-content/uploads/2018/08/Notice-of-Concern-Quest-Life-Sciences_2015.pdf