

# Data Engineering for GxP Compliance

**Ravi Kiran Koppichetti**

[koppichettiravikiran@gmail.com](mailto:koppichettiravikiran@gmail.com)

## Abstract

Data engineering plays a pivotal role in ensuring compliance with Good Practice (GxP) regulations, which are critical for maintaining the quality, safety, and efficacy of products in regulated industries such as pharmaceuticals, biotechnology, and healthcare. This paper explores the challenges, best practices, and technologies involved in designing and implementing GxP-compliant data engineering solutions. Key topics include data integrity, audit trails, data security, traceability, and validation, as well as the use of modern data platforms to meet regulatory requirements. Through a detailed case study, the paper illustrates the steps organizations can take to overcome challenges and achieve compliance. By adopting robust data engineering practices, organizations can ensure the integrity, security, and traceability of their data while meeting evolving regulatory expectations. This paper serves as a comprehensive guide for organizations seeking to navigate the complexities of data engineering in GxP environments.

**Keywords:** Pharmaceutical Manufacturing, Internet Of Things, Publish/Subscribe, OPC UA, Pharmaceutical Data, Data Management, Data Integrity, Artificial Intelligence (AI), Data Quality, Data Volume, Privacy, Security

## I. Introduction

GxP regulations encompass a set of guidelines and standards (e.g., Good Manufacturing Practice (GMP), Good Laboratory Practice (GLP), and Good Clinical Practice (GCP)) that ensure products are consistently produced and controlled according to quality standards. In the digital age, data has become a cornerstone of GxP compliance, as it underpins decision-making, quality control, and regulatory submissions.

Data engineering, the discipline of designing and building systems for collecting, storing, and analyzing data, is essential for meeting GxP requirements. This paper examines how data engineering practices can be aligned with GxP principles to ensure data integrity, security, and traceability.

## II. Key GxP Requirements for Data Management

The Good Practice (GxP) requirements for data management are extensive and complex, encompassing aspects such as data integrity, audit trails, security, traceability, validation, governance, retention, and electronic records. By effectively addressing these requirements through rigorous data engineering practices, organizations can guarantee compliance, sustain product quality, and prioritize patient safety. As regulatory expectations continue to evolve, an anticipatory and methodical approach to data management will remain crucial for success in regulated industries.

**A. Data Integrity:** The management of data within GxP-regulated industries, including pharmaceuticals, biotechnology, and healthcare, is governed by rigorous standards intended to ensure the integrity, security, and reliability of data. These standards are vital for upholding product quality, safeguarding patient safety, and ensuring regulatory compliance. Central to GxP data management is the principle of data integrity, which guarantees that data remains complete,

consistent, and accurate throughout its lifecycle. Regulatory authorities such as the FDA and EMA underscore the significance of the ALCOA+ framework—Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, and Available. This framework serves as a foundational element for ensuring that data is reliable and can sustain regulatory examination. For instance, data must be attributable to the individual or system that generated it, must be recorded in real-time, and must be preserved in its original format or as a certified true copy. The implementation of these principles necessitates robust systems, regular audits, and a culture of accountability [1, 2, 3].

- B. Audit Trails:** Audit trails refer to electronic or paper records that meticulously document the history of modifications to data. These records are vital for monitoring who enacted the changes, the specific alterations made, the timing of these amendments, and the underlying reasons for such changes. It is imperative that audit trails are secured and remain immutable, prohibiting any alterations or deletions. Each entry within the audit trail must be accompanied by a precise date and time stamp. Furthermore, the individual accountable for the modification must be distinctly identified. The basis for each modification must also be systematically recorded. To ensure adherence to regulations, organizations are required to activate audit trail functionality within all Good Practice (GxP) systems, routinely examine these trails for any anomalies, and preserve them for the duration mandated by regulatory guidelines, such as the FDA 21 CFR Part 11 [4, 5, 6, 7].
- C. Data Security:** Data security ensures that information is safeguarded against unauthorized access, manipulation, or loss. This is essential for preserving confidentiality, integrity, and availability. Effective data security necessitates the implementation of access controls to restrict data access based on user roles and responsibilities, encryption to safeguard data both at rest and in transit against potential breaches, and robust backup and recovery processes to avert data loss. Additionally, physical security measures are required to protect physical access to servers and data storage facilities. Organizations can further enhance their data protection strategies by employing multi-factor authentication (MFA) and conducting regular security risk assessments [4, 8, 9].
- D. Traceability:** The concept of traceability ensures that the origin and historical context of data can be monitored throughout its entire lifecycle. This is essential for investigating issues, ensuring accountability, and demonstrating compliance with relevant regulations. Achieving traceability is supported by implementing Data Lineage, which records the journey of data from its source to its destination; the use of Unique Identifiers to assign distinct identifiers to data records for efficient tracking; and Change Control to accurately document all modifications to data, including the reasons behind each change. Traceability is especially important during regulatory inspections or investigations, as it enables organizations to verify the reliability and authenticity of their data. Tools that visualize data flows and maintain essential metadata, such as timestamps and user identification numbers, are invaluable in enhancing traceability initiatives [4, 10, 11].
- E. Data Validation:** Data validation is a critical process that ensures systems and procedures consistently produce reliable and accurate results. This aspect is essential for Good Practice (GxP) compliance. The process includes System Validation, which evaluates computerized systems to confirm their proper functioning; Process Validation, which assesses processes to ensure they consistently yield quality results; and Data Verification, which checks data for accuracy and completeness. A risk-based approach, often guided by frameworks such as GAMP 5, is generally

used to improve the efficiency of validation activities. Additionally, documenting validation processes, including test scripts and results, as well as revalidating systems and processes after significant changes, is vital for demonstrating compliance [4, 10, 11, 12, 13].

**F. Data Governance:** Data governance is a comprehensive framework that includes policies, processes, and controls to ensure effective data management in compliance with Good Practices (GxP) regulations. This framework establishes clear policies regarding data management, such as data ownership, access, and retention. Furthermore, it defines roles and responsibilities related to data management. It is essential to provide training for personnel on the data governance policies and procedures. Additionally, regular monitoring and auditing of data management practices must be conducted to maintain ongoing compliance. During implementation, a data governance framework specifically tailored to GxP requirements is created, along with regular training sessions for employees. This training is vital for conducting both internal and external audits to assess compliance [9, 14, 15].

**G. Data Retention and Archiving:** Good Manufacturing Practice (GxP) regulations necessitate that organizations maintain data for designated durations to facilitate regulatory inspections and investigations. These regulations stipulate that organizations must retain data for the mandated period, as outlined by the Food and Drug Administration (FDA) or European Medicines Agency (EMA) guidelines. Data is required to be archived in a secure and accessible format, and appropriate disposal methods must be employed when data is no longer required. Organizations should establish retention periods for various types of data and utilize secure archiving systems designed to prevent any tampering with data. Furthermore, it is imperative to implement secure data disposal methods, which may include shredding or degaussing [4, 5].

**H. Electronic Records and Signatures:** For organizations using electronic records and signatures, compliance with US FDA 21 CFR Part 11 is mandatory. This regulation sets forth requirements for electronic signatures, system controls, and audit trails to ensure the authenticity, integrity, and confidentiality of electronic records. Additionally, it guarantees that electronic signatures are unique, secure, and linked to the appropriate individual. Validating electronic systems, implementing secure electronic signature solutions, and regularly assessing system controls are essential for meeting these obligations [4, 16, 17].

### III. Challenges in Data Engineering for GxP Compliance

The challenges associated with data engineering in relation to Good Practice (GxP) compliance are complex and multifaceted, encompassing technical, regulatory, organizational, and cultural dimensions. Effectively addressing these challenges necessitates a comprehensive approach that integrates advanced technology, robust processes, and a firm commitment to compliance. By thoroughly understanding and proactively addressing these challenges, organizations can develop data engineering solutions that not only fulfill GxP requirements but also foster innovation and enhance operational efficiency within regulated industries.

**A. Data Complexity:** In regulated sectors such as the pharmaceutical and biotechnology industries, data is generated from a diverse array of sources, including laboratory instruments, manufacturing systems, clinical trials, and supply chain operations. This data is frequently heterogeneous, encompassing structured data (e.g., databases), semi-structured data (e.g., XML files), and unstructured data (e.g., PDF reports or handwritten notes). The integration and management of this

diverse data while ensuring compliance with Good Automated Manufacturing Practice (GxP) regulations poses a significant challenge. For instance, maintaining data integrity and traceability across multiple systems and formats necessitates sophisticated data engineering solutions. Furthermore, the substantial volume of data generated can overwhelm traditional systems, complicating the processing, storage, and analysis of data efficiently without compromising compliance [1, 18].

- B. Regulatory Evolution:** Good Manufacturing Practice (GxP) regulations are not fixed; rather, they develop in response to technological advancements, shifts in industry practices, and emerging risks. For example, regulatory agencies such as the Food and Drug Administration (FDA) and the European Medicines Agency (EMA) routinely update their guidelines to address new challenges, including the integration of artificial intelligence (AI) in drug development and the adoption of cloud-based systems. Remaining cognizant of these changes and ensuring compliance within data engineering practices can present significant challenges. Organizations must consistently monitor regulatory updates, evaluate their implications on existing systems, and implement necessary modifications, all while preserving operational continuity. This ever-evolving regulatory landscape necessitates a proactive and adaptable approach to data engineering [19, 20].
- C. Legacy Systems:** Numerous organizations within regulated industries continue to depend on legacy systems that were instituted several decades ago. These systems frequently lack the essential capabilities required to fulfill contemporary Good Practice (GxP) requirements, including robust audit trails, data validation, and secure access controls. The process of upgrading or replacing these systems is both intricate and costly, as it necessitates the migration of substantial volumes of historical data, validation of new systems, and training of personnel. Furthermore, legacy systems may exhibit poor integration with modern data engineering tools and platforms, thereby generating silos that obstruct data accessibility and traceability. Achieving a balance between the necessity for modernization and the risks associated with disrupting ongoing operations presents a considerable challenge [17].
- D. Scalability:** As organizations expand and data volumes increase, the significance of scalability becomes increasingly paramount. Data engineering solutions must adeptly manage larger datasets, more complex workflows, and elevated user requirements without compromising performance or compliance. For example, a pharmaceutical company involved in global clinical trials may need to process and store information from thousands of patients across diverse locations. It is essential to ensure that data pipelines, storage systems, and analytics platforms can scale according to these requirements while maintaining data integrity, security, and traceability, which presents a considerable challenge. While cloud-based solutions offer scalability, they also introduce new challenges, such as compliance with data residency and privacy laws [5, 21].
- E. Data Security and Privacy:** Ensuring data security is of paramount importance within Good Practice (GxP) regulated industries, as breaches may result in regulatory sanctions, loss of intellectual property, and reputational harm. Nevertheless, safeguarding data within a multifaceted and interconnected environment poses significant challenges. Data engineering solutions must integrate comprehensive security measures, including but not limited to encryption, access controls, and intrusion detection systems, to safeguard sensitive information. Furthermore, organizations are required to adhere to data privacy regulations such as the General Data Protection Regulation

(GDPR), which establishes stringent requirements for the collection, storage, and processing of personal data. Achieving a balance between security and privacy, while ensuring data accessibility and usability, constitutes a complex undertaking [4, 8, 9].

- F. Validation of Data Engineering Systems:** Validation constitutes a fundamental requirement for GxP compliance, guaranteeing that systems and processes reliably yield accurate outcomes. Nevertheless, the validation of data engineering systems—encompassing data pipelines, ETL (Extract, Transform, Load) processes, and analytics platforms—presents a complex and resource-intensive endeavor. This process necessitates the establishment of validation protocols, execution of rigorous testing, and thorough documentation of results to substantiate compliance. For instance, the validation of a machine learning model utilized in drug discovery necessitates not only the evaluation of the model's accuracy but also the assurance that the data employed for training the model is both accurate and complete, as well as traceable. The sophistication inherent in contemporary data engineering systems renders validation a considerable challenge [4, 10, 11, 12, 13].
- G. Interoperability and Integration:** Within numerous organizations, data is maintained across various disparate systems that lack effective communication with one another. For instance, laboratory data may be retained within one system, while manufacturing data is stored in another, and clinical trial data resides in yet another. The integration of these systems to establish a unified and compliant data environment presents a significant challenge. Data engineering solutions must facilitate interoperability among systems, while simultaneously preserving data integrity, security, and traceability. This often necessitates the utilization of middleware, Application Programming Interfaces (APIs), and data integration platforms, all of which must themselves be validated and compliant with Good Practice (GxP) regulations [22, 23].
- H. Cultural and Organizational Challenges:** Achieving Good Practice (GxP) compliance is not just a technical challenge; it also requires a cultural transformation within the organization. Employees at every level must understand the importance of data integrity and compliance, as well as follow established policies and procedures. However, fostering a culture of compliance can be difficult, especially in organizations with entrenched practices or resistance to change. Training and change management are essential yet often overlooked aspects of data engineering for GxP compliance. In addition, collaboration between Information Technology (IT), quality assurance, and business units is critical; however, it may be hindered by siloed structures and conflicting priorities.
- I. Cost and Resource Constraints:** The implementation and maintenance of Good Practice (GxP)-compliant data engineering solutions require a significant investment in technology, personnel, and training. Many organizations, especially smaller ones, face budget constraints that limit their ability to adopt advanced data engineering tools and methods. For example, deploying a cloud-based data platform with built-in compliance features may be financially challenging for some organizations. Additionally, hiring skilled data engineers and validation specialists poses considerable difficulties in a competitive job market. Achieving a balance between the need for compliance and the constraints of available resources remains an ongoing challenge.
- J. Global Regulatory Variations:** Organizations operating in multiple regions must navigate the discrepancies in Good Practice (GxP) regulations across various jurisdictions. For instance, the

requirements outlined in the FDA's 21 CFR Part 11 regarding electronic records and signatures may differ significantly from the guidelines provided by the European Medicines Agency (EMA) in the European Union. Such variations can create complexities in designing and implementing data engineering solutions that must comply with standards across all regions. Therefore, organizations are encouraged to adopt a flexible and adaptable strategy to ensure global compliance while minimizing duplication of efforts.

#### IV. Best Practices for Data Engineering in GxP Environments

Data engineering in Good Practice (GxP) environments poses unique challenges. However, by adopting optimal practices, organizations can ensure compliance while also maintaining data integrity, security, and traceability. From implementing rigorous validation processes to fostering a culture of compliance, these practices provide a comprehensive framework for managing data in regulated sectors. As GxP regulations evolve, organizations must stay adaptable and proactive, leveraging modern technologies and continuous improvement to stay ahead of regulatory requirements.

- A. Implement Strong Data Validation and Verification:** Data validation is a crucial aspect of Good Practice (GxP) compliance, ensuring that the data is accurate, complete, and trustworthy. Data engineering pipelines must integrate automated validation checks to detect and flag errors, inconsistencies, or missing data. For example, validation rules can be applied to ensure that data falls within expected ranges, follows established formats, or matches reference datasets. Additionally, regular manual reviews and audits should be conducted to confirm the accuracy of essential data. A risk-based approach to validation, as outlined in the GAMP 5 guidelines, can help prioritize validation efforts and ensure that high-risk data and systems receive the necessary attention [4, 10, 11, 12, 13].
- B. Establish Comprehensive Audit Trails:** Audit trails are pivotal for monitoring alterations to data and ensuring accountability. In Good x Practice (GxP) environments, it is imperative that audit trails are tamper-proof, time-stamped, and encompass details pertaining to the individual who effectuated the change, the nature of the modification, and the rationale behind it. Data engineering solutions should be designed to automatically generate and securely store audit trails for all alterations to data, irrespective of their occurrence in databases, data pipelines, or analytics platforms. Periodic review of audit trails is essential for identifying anomalies, conducting investigations into incidents, and demonstrating compliance during regulatory inspections. Technologies such as blockchain can further enhance the integrity and immutability of audit trails [4, 5, 6, 7].
- C. Adopt a Strong Data Governance Framework:** Data governance forms the essential foundation for managing data in compliance with regulatory standards while ensuring consistency. An effective data governance framework includes a comprehensive set of policies, procedures, and controls concerning data ownership, access, quality, and lifecycle management. The key components of data governance within Good Practice (GxP) environments are critical to maintaining integrity and reliability in data handling, including:
  - Defining roles and responsibilities associated with data management.
  - Establishing explicit policies governing data access, retention, and disposal.
  - Implementing data quality standards accompanied by monitoring mechanisms.
  - Conducting regular training sessions to ensure that employees comprehend and comply with data governance policies [9, 14, 15].

**D. Ensure Secure Data Storage and Transmission:** Data security is of paramount importance in Good Practice (GxP) environments, where breaches may result in significant regulatory and reputational repercussions. Consequently, data engineering solutions should integrate comprehensive security measures to safeguard data both at rest and during transit. This includes:

- Protecting sensitive data through encryption to stop unauthorized access.
- Establishing access controls that limit data availability according to user roles and responsibilities.
- Utilizing secure protocols like HTTPS and SFTP for safe data transmission.
- Conducting routine tests of backup and recovery procedures to guarantee data accessibility in the event of a breach or system failure [4, 24].

**E. Leverage Modern Data Platforms:** Modern data platforms, particularly cloud-based solutions, offer scalability, flexibility, and integrated compliance features that can greatly enhance data engineering in Good Practice (GxP) environments. For example, cloud platforms enable automated backups, encryption, and access controls, reducing the burden on internal IT departments. However, organizations must confirm that these platforms comply with GxP regulations, especially regarding data residency, privacy, and security. When adopting modern data platforms, it is crucial to assess their operational capabilities and ensure they meet regulatory requirements [5].

## V. Case Study: Implementing a GxP-Compliant Data Engineering Solution

Implementing a Good Practice (GxP)- compliant data engineering solution is an essential measure for organizations operating within regulated sectors, including pharmaceuticals, biotechnology, and healthcare. This guide presents a systematic approach to designing, deploying, and maintaining a data engineering system that adheres to GxP standards, thereby ensuring data integrity, traceability, and security. By adhering to the outlined steps, organizations can attain compliance while simultaneously enhancing operational efficiency and facilitating regulatory success.

**A. Step 1: Assess Current Systems and Identify Gaps:** Begin by conducting a thorough assessment of your existing data systems and processes. This step is crucial for understanding the current state and identifying gaps in compliance.

- **Inventory Data Sources:** Catalog all data sources, including laboratory instruments, clinical trial management systems (CTMS), manufacturing execution systems (MES), and any other relevant systems.
- **Perform a Gap Analysis:** Compare your current data management practices against GxP requirements. Identify gaps such as missing audit trails, inadequate data validation, or insufficient security controls.
- **Engage Stakeholders:** Interview key stakeholders, including IT, quality assurance (QA), and R&D teams, to understand pain points and gather input on requirements.

This assessment will provide a clear roadmap for addressing compliance gaps and designing a solution tailored to your organization's needs.

**B. Step 2: Create a GxP-Compliant Data Engineering Pipeline:** Develop a contemporary data engineering pipeline that addresses the identified gaps and guarantees compliance with GxP regulations.

- **Centralize Data Storage:** Use a cloud-based data lake or warehouse to consolidate data from disparate sources, creating a single source of truth.
- **Implement Data Validation:** Incorporate automated validation checks to ensure data accuracy, completeness, and consistency.
- **Enable Audit Trails:** Design systems to generate immutable logs that track all data changes, including user IDs, timestamps, and reasons for changes.
- **Enhance Data Security:** Use encryption, access controls, and secure protocols to protect sensitive data.
- **Track Data Lineage:** Integrate tools to document the flow of data from source to destination, ensuring traceability.

A well-structured pipeline emphasizes scalability, compliance, and user-friendliness, allowing your organization to address both current and future needs.

**C. Step 3: Migrate Data to the New Platform:** Data migration is a critical phase that requires careful planning to ensure data integrity and compliance.

- **Clean and Standardize Data:** Remove duplicates, correct errors, and standardize formats to ensure data quality.
- **Validate Migrated Data:** Verify that data is accurately transferred and meets GxP requirements.
- **Migrate Incrementally:** Move data in phases to minimize disruption to ongoing operations.
- **Establish Backup and Rollback Plans:** Prepare contingency plans to address any issues during migration.

A successful migration will create a unified and compliant data environment, prepared for operational use.

**D. Step 4: Validate the System:** Validation is essential to ensure the new system meets GxP requirements and functions as intended.

- **Develop a Validation Plan:** Define the scope, objectives, and acceptance criteria for validation.
- **Conduct Rigorous Testing:**
  1. Perform unit testing to verify individual components of the data pipeline.
  2. Conduct integration testing to ensure seamless interaction between systems.
  3. Complete user acceptance testing (UAT) to confirm the system meets user needs and regulatory requirements.
- **Document Validation Activities:** Record all validation activities, including test scripts, results, and approvals.

Successful validation will demonstrate compliance with GxP regulations and readiness for operational use.

**E. Step 5: Monitor and Continuously Improve:** After deployment, create systems to continuously monitor and enhance the system.

- **Track Data Quality Metrics:** Monitor key performance indicators (KPIs), such as data accuracy, completeness, and processing times.
- **Conduct Regular Audits:** Perform internal audits to assess compliance with GxP regulations.



- **Collect Feedback:** Gather input from users to identify areas for improvement.
- **Implement Updates:** Make enhancements based on audit findings and user feedback.

Continuous monitoring and improvement will ensure the system remains compliant, effective, and aligned with evolving business needs.

## VI. Conclusion

Data engineering acts as a vital facilitator of Good Practice (GxP) compliance in regulated industries. By effectively tackling challenges like data complexity, regulatory changes, legacy systems, and scalability, organizations can design and implement data engineering solutions that meet strict GxP requirements. Best practices, including rigorous data validation, comprehensive audit trails, strong data governance, and the use of modern data platforms, provide a framework to ensure data integrity, security, and traceability. The case study presented in this paper demonstrates how a structured and collaborative approach can lead to successful implementation, resulting in benefits such as enhanced data quality, improved compliance, and increased operational efficiency.

As GxP regulations continue to evolve, it is crucial for organizations to remain proactive and adaptable, utilizing advanced technologies and committing to continuous improvement to meet regulatory demands. By fostering a culture of compliance and investing in strong data engineering practices, organizations can not only meet GxP standards but also promote innovation and operational excellence. This paper highlights the importance of data engineering in achieving regulatory success and provides a strategic roadmap for organizations aiming to navigate the complexities of GxP compliance in the digital age.

## References

- [1] H. Alosert et al., "Data integrity within the biopharmaceutical sector in the era of Industry 4.0," *Biotechnol. J.*, vol. 17, no. 6, p. 2100609, 2022.
- [2] S. C. Hock, V. Tay, V. Sachdeva, and C. L. Wah, "Pharmaceutical Data Integrity: Issues, challenges and proposed solutions for manufacturers and inspectors," *Generics Biosimilars Initiative J.*, vol. 9, no. 4, pp. 171–183, 2020.
- [3] D. Solanki, D. Patel, and D. Meshram, "Data Integrity: A cornerstone for compliance," *Signature*, vol. 1, p. 2, 2022.
- [4] S. C. Ronolo, "Assuring Data Integrity towards Regulatory Compliance: A Study on Process Improvement in Data Integrity Compliance of Computerized Systems," 2023.
- [5] S. Davis et al., "Cloud solutions for GxP laboratories: Considerations for data storage," *Bioanalysis*, vol. 13, no. 17, pp. 1313–1321, 2021.
- [6] R. Hattemer-Apostel, "Quality assurance, quality control and audit," in *Principles and Practice of Pharmaceutical Medicine*, pp. 163–181, 2010.
- [7] J. Avellanet, "FDA 21 CFR Part 11 Revisited," *BioProcess Int.*, 2009.
- [8] L. Robert, "Integrating AI and IAM for Comprehensive Cybersecurity in GxP-Regulated Healthcare Environments," 2023.
- [9] T. Truong, R. George, and J. Davidson, "Establishing an effective data governance system," 2017.
- [10] G. Wingate, *Demonstrating GxP Compliance. Validating Corporate Computer Systems: Good IT Practice for Pharmaceutical Manufacturers*, p. 119, 2000.
- [11] S. Rönninger, S. Schmitt, V. Rangavajhula, E. Hough, and J. Lyda, "Considerations on auditing and GXP requirements along the product lifecycle," *PDA J. Pharm. Sci. Technol.*, vol. 66, no. 5, pp. 396–402, 2012.
- [12] K. de Jong, *Maintenance and Support of Validated IT Systems*, p. 351, 2000.

- [13] T. Morgan and T. Carey, "Computer Validation: A Compliance Focus," in *Compliance Handbook for Pharmaceuticals, Medical Devices, and Biologics*, CRC Press, pp. 220–243, 2003.
- [14] A. R. Carter, E. Meinert, and D. A. Brindley, "Data and corporate governance in pharma and digital health: A necessary regulatory convergence," *Rejuvenation Res.*, vol. 21, no. 4, pp. 291–293, 2018.
- [15] R. George, T. Truong, and J. Davidson, "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," *Pharm. Technol. Eur.*, vol. 29, no. 11, pp. 40–44, 2017.
- [16] G. Wingate, "Electronic records and electronic signatures," in *Pharmaceutical Computer Systems Validation*, CRC Press, pp. 280–307, 2016.
- [17] G. Wingate, *Demonstrating GxP Compliance. Validating Corporate Computer Systems: Good IT Practice for Pharmaceutical Manufacturers*, p. 119, 2000.
- [18] S. Goriparthi, "Implementing robust data governance frameworks: The role of AI/ML in ensuring data integrity and compliance," *Int. J. Artif. Intell. Mach. Learn.*, vol. 1, no. 1, pp. 83–91, 2022.
- [19] B. W. Unger, "Data integrity and data management for GxP regulated firms," [Online]. Available: <https://ungerconsulting.net/wp-content/uploads/2016/01/Data-Integrity-White-Paper-BLOG.pdf>. [Accessed: 27-Apr-2017].
- [20] S. C. Hock, S. M. Kian, and C. L. Wah, "Global challenges in the manufacture, regulation and international harmonization of GMP and quality standards for biopharmaceuticals," *Generics Biosimilars Initiative J.*, vol. 9, no. 2, pp. 52–64, 2020.
- [21] N. Jain, S. Katre, and A. Vinukonda, "Importance of qualification, computer system validation and its regulatory compliance in pharmaceutical industry," *Int. J. Drug Regul. Aff.*, vol. 8, no. 3, pp. 70–77, 2020.
- [22] M. Pestronk et al., "Electronic data capture-selecting an EDC system," *J. Soc. Clin. Data Manage.*, vol. 1, no. 1, 2021.
- [23] D. Della Corte, W. Colsman, H. Fessenmayr, A. S. da Silva, and D. E. Vanderwall, "Self-reporting data assets and their representation in the pharmaceutical industry," *Drug Discov. Today*, vol. 27, no. 1, pp. 207–214, 2022.
- [24] T. Sandle, "Application of wireless technology in the pharmaceuticals sector: Maintaining data integrity, security and privacy."