ISSN: 2231-3656

International Journal of Pharmacy and Industrial Research (IJPIR)

IJPIR |Vol.16 | Issue 2 | Apr – Jun - 2026

www.ijpir.com

DOI : https://doi.org/10.61096/ijpir.v16.iss2.2026.540-557

GMP, GCP and GDP Data Governance and Data Integrity

Shreya Thakar*[1], Dhara Patel[1], Grishma Patel[1], Dhananjay Meshram[1]

Department of Pharmaceutical Quality Assurance, Pioneer Pharmacy College, Vadodara-390019, Gujarat, India.

*Corresponding Author: Shreya Thakar
Email id: shreyathakar03@gmail.com

Published by: 16.05.2026

Abstract: Integration of data governance and data integrity within GMP, GCP, and GDP regulatory processes is a fundamental requirement for ensuring quality of products, patient safety, and regulatory compliance. GMP is a component of quality assurance which ensures the consistent production and control of products in compliance with required quality standards and marketing authorization specifications, thus establishing minimum requirements aimed at preventing risks to the consumer. Poor documentation practice often is a common issue for clinical research studies; therefore, reliable, accurate, and adequate source documentation is imperative for guaranteeing that the findings of research are based on credible and legitimate data sources. Data integrity implies the accuracy, completeness, and consistency of data during its whole lifecycle which should be preserved in the original or in true copies, as well as adherence to ALCOA principles (attributable, legible, contemporaneous, original, and accurate). Metadata is an important element providing necessary context information about data. In GDP settings, data integrity can be ensured by proper handling and distribution. The approach to ensuring data integrity based on identification of associated risks such as data manipulation, loss, and corruption can be implemented with appropriate corrective measures using quality systems. Continuous monitoring of data systems, implementation of sound governance. In summary, proper governance of the data system, document management, and risk management help create an accurate, reliable, and compliant data system. If the integrity of the data is challenged, it could result in regulatory action, recalling of product, patient harm, and loss of trust among other serious consequences, highlighting the importance of data governance within the pharma industry.

Keywords: GMPs, GCPs, GDPs, data integrity, data governance, ALCOA+, risk-based approach, data documentation practices, lifecycle data management, patient safety, audit trails and metadata, data management in clinical and manufacturing environments.

1. INTRODUCTION

1.1 Background and Regulatory Importance

In a global perspective, the pharmaceutical industry forms a key section in the health industry. This comprises pharmaceutical products that are produced, manufactured, and distributed to meet some set requirements. Every part of the world requires strict observance of GMPs so as to ensure that pharmaceutical products are produced to certain standards of quality. GMPs are policies that regulate a manufacturing process in several organizations minimizing any errors

or risks during the manufacturing process [1]. The planning, conduct, performance, monitoring, auditing, recording, analysis, and reporting of the clinical trials that are regulated by the internationally accepted ethical and scientific quality standard termed good clinical practice (GCP). GCP ensures that the rights of the participants of the clinical trials are maintained and protected; also, the data collected and reported is acceptable and trustworthy. [2] Good Documentation Practices (GDP) form a methodical process through which documents are prepared, reviewed, issued, recorded, stored and archived. Good documentation practice describes the selection for prompting and managing of documents. [3]

1.2 Scope of GMP, GCP AND GDP [4][5]

Aspect	GMP (Good Manufacturing Practice)	GDP (Good Distribution Practice)	GCP (Good Clinical Practice)
Main Objective	Implement quality, safety, and eternally of the manufactured products.	Maintaining quality and integrity during storing and distributing.	Assures ethical and scientific conduct of the clinical trials.
Stage Covered	Manufacturing stage	Post-manufacturing (distribution stage)	Pre-marketing (clinical trial stage)
Scope Area	Production facilities (pharma industries)	Warehouses, transportation, and supply chain	Hospitals, research centers, clinical sites
Key Activities	Raw material handling, manufacturing, packaging, and labeling	Storage, transportation, distribution, delivery	Clinical trial design, conduct, monitoring
Quality Control	Testing of raw materials, intermediates, finished products	Ensuring product quality during transit and storage	Ensuring accuracy and reliability of the clinical data
Personnel Requirements	Training, hygiene, qualification of staff	Training of warehouse and distribution staff	Qualified investigators and trained clinical staff
Documentation	BMR, SOPs, validation records, batch records	Distribution records, invoices, tracking data	Case Report Forms (CRFs), protocols, Trial Master File
Equipment & Facilities	Maintenance, calibration, validation of equipment	Proper storage facilities (temperature, humidity control)	Clinical trial facilities and medical equipment
Regulatory Focus	Product quality and compliance	Supply chain integrity and traceability	Patient safety and ethical standards
Risk Covered	Contamination, mix-ups, manufacturing errors	Damage, temperature excursions, counterfeit drugs	Risk to human subjects, data manipulation
End Goal	Safe and effective pharmaceutical product	Safe delivery of product to patient	Reliable clinical data and patient protection

1.3 Importance of Data Governance and Data Integrity [4]

In particular, for industries like pharma where regulations apply, data integrity and data governance play a critical role in quality management systems. It implements the correctness, defense and reliability of data generated throughout the lifecycle of the products. Data integrity makes sure that data is whole, consistent and accurate from when it is created till preserving is done. It depends on the ALCOA+ principle which states that data should be attributable, legible, contemporaneous, original, and accurate. Data integrity is important because decisions on developing drugs, manufacturing them and carrying out quality control processes are based on the collected data. It is important because if data integrity is lacking then the conclusions drawn may be incorrect causing patients harm due to the production of ineffective medicines. Non-compliance with the rules will lead to a company receiving warning letters, recalls of

products as well as legal inquiries. On top of this, it is helpful in increasing the ability to conduct traceability and auditing processes because of the audit trail.

1.4 Objectives of the review

Feature	GMP	GDP	GCP	Data Integrity	Data Governance
Purpose	Quality assurance	Quality logistics	Quality testing	Data integrity	Data integrity system
Domain	Production process	Shipping process	Patient studies	Database integrity	systemic data governance
Role of Data	Production records	Shipments logs	Test data	Essential component	Monitoring system
Feature	GMP	GDP	GCP	Data Integrity	Data Governance

2. Overview of Regulatory Frameworks

2.1 Good Manufacturing Practice (GMP) [1]

Good Manufacturing Practice (GMP) is the term used to describe those practices which ensure that any manufactured products such as foods, drugs or medical devices are produced and handled according to the quality standards associated with that particular type of product. GMPs are compulsory and thus cannot be overlooked. In America, the process of GMP is followed through cGMP which comes from 21 CFR Parts 210 and 211, under FDA. For globally accepted practices, GMP information is available through WHO and in India, through CDSCO (Schedule M).

2.2Good Clinical practice (GCP) [7]

Good Clinical Practice (GCP) can be described as an international code of conduct that aims to protect the rights of participants in human subjects research. This is a fundamental principle of international guidelines, with its regulations based on the International Conference on Harmonization (ICH) E6 guideline.

2.3 Good Documentation Practice (GDP) [8]

In order to ensure that the medicines remain safe, intact, and of the right quality throughout the entire supply chain, from the manufacturer to the consumer, good distribution practices are one element of quality assurance. To prevent imitation medicines or those of poor quality from reaching consumers, distributors and logistics and storage organizations need to comply with GDP guidelines.

2.4 Interrelationship between GMP, GCP and GDP [9]

GMP, GCP, and GDP are crucial quality management systems in pharmacy and play a very important role in guaranteeing safety and quality of the product from its manufacturing to its disposal. GMP is vital for providing standardization of manufacturing and testing processes according to the quality standards; meanwhile GCP is vital in guaranteeing the ethical conduct of clinical trials and their reliability and safety. GDP provides assurance in proper handling, storage, and distribution of pharmaceuticals. Documentation is very essential in GMP and GDP and all procedures should be documented.

3. Concept of Data Governance

3.1 Definition and principles [10]

Data governance can be understood as the governance of an organization's data property. The concept covers the effective management of the data for the purpose of checking its quality,

consistency, security, and effectiveness. Some of the codeword involved in data governance include liable, where owners who are responsible for the quality and security of the data are appointed, correspondence, who implements that the data is consistent across various platforms in terms of formatting, and security, which ensures that the data is secured and confidential.

3.2 Components of Data Governance Framework [10]

Organizational Bodies and Policies	Standard and Processes	Data Governance Technology
Governance structure	Data, Definition and standard (meta data management)	Metadata Repository
Data custodianship	Third party data extent	Data profiling tool
User group charter	Metrics development and monitoring	Data cleansing tool
Decision Rights	Data profiling	
Issue Escalation process	Data cleansing	

3.3 Roles and Responsibilities (Data Owners, Stewards, Custodians) [11]

The data governance design ensures the data is secure, and of high quality, and also comply with regulations through the provision of guidelines and policies. This structure outlines important roles such as that of the Data Governance Council, whose role is to give guidance, develop policies, and implement that governance practices support the goals of the organization. The Data Governance Lead or Chief Data Officer (CDO) will be responsible for implementing the governance structure and serve as a link between executive management and operational activities. The data owners define their respective data domain, set quality criteria, and control access to the data.

3.4 Data lifecycle management [11]

The data life cycle is everything that happens during the entire process of data creation until it is finally disposed of. These processes include data generation, processing, reporting, validation, usage, storage, and disposal. As the data progresses through each step in the data life cycle, it will be transferred among various internal and external systems and departments.

4. Understanding Data Integrity

4.1 Definition and Regulatory Expectations [12] [13]

Data integrity can be defined as the completeness, consistency, and accuracy of data. These data must be attributable, legible, contemporaneous, original or true copies, and accurate (ALCOA). The importance of data integrity is emphasized by regulatory agencies to be considered as part of the PQS, rather than just a technical issue. Under 21 CFR Part 211, record keeping must be complete, data must be protected from any kind of manipulation, and lab controls must be scientifically sound. 21 CFR Part 11 outlines the procedures on electronic signatures and records. Good Documentation Practices (GDP): Organizations need to have risk management and self-inspection processes in place to make sure data is handled in a correct manner. Backup and Archiving: To avoid loss, electronic data needs to be routinely backed up and safely preserved.

4.2 ALCOA and ALCOA+ Principles [14]

The acronym ALCOA stands for Attributable, Legible, Contemporaneous, Original, and Accurate. The concepts of Complete, Consistent, Enduring, and Available were added to ALCOA to create ALCOA Plus (ALCOA+). Integrity, Robustness, Transparency, Accountability, and Reliability are added to ALCOA++.

Fundamental ALCOA Principles

Attributable: The person or system in charge of watching or recording the data can be connected to it. Legible: Throughout its entire existence, data is legible and comprehensible. Contemporaneous: Captured in real time at the moment the activity or observation takes place.

Original: A certified true copy or the first data recording (raw data). Accurate: The information is true, accurate, and devoid of unapproved mistakes.

Expanded Principles, or ALCOA+ To satisfy contemporary data requirements, ALCOA+ (also known as ALCOA Plus) adds four more principles to the original five: Complete: All information is kept up to date, including metadata and test replications. Consistent: Information is arranged logically and according to expectations. Enduring: Rather than being recorded on transient notes, data is stored on durable media Available: Throughout its existence, data can be reviewed, audited, or inspected.

4.3 Key Elements for Data Integrity [15]

Data validation (accuracy/validation), data security (access controls/encryption), data consistency (uniformity across systems), and data backup/recovery are the essential components that ensure the accuracy, consistency, and dependability of data throughout its lifecycle. By guarding against unapproved changes and mistakes, it preserves credibility. Principles and Essential Elements of Data Integrity Ensuring that data is accurate, precise, and represents the actual status of information is known as data accuracy. Data Completeness: Ensuring that all necessary fields are present and recorded, and that no data is missing or incomplete. Ensuring that data is consistent and meets the same requirements across all tables, systems, and locations is known as data consistency. Data validation is the process of ensuring that data satisfies predetermined quality Data Security and Access Control: Adopting policies such as Role Based Access Control (RBAC), Two Factor Authentication (2FA), and encryption to guard against any unauthorized changes or manipulation.

4.4 Data Integrity Across the Product Lifecycle [13]

Product lifecycle data integrity ensures the accuracy, consistency, and reliability of data from its generation to archiving, protecting it against any unauthorized modifications. It applies to research and development, manufacturing, and distribution, complying with relevant regulations (e.g., FDA, EMA) and promoting safety, especially within pharmaceuticals. Some strategies include the use of one primary source of data, audit trails, and automated validation to eliminate errors and silos. Data integrity throughout the product lifecycle means ensuring that data remains accurate and trustworthy in all aspects of its usage. While creating and collecting data, it needs to be accurately recorded using validated tools in real time and avoiding manual means of data recording. When storing and preserving data, it must be kept safely and protected against any form of data loss or tampering. Data integrity must be ensured when data is being tracked and used within different systems such as CAD, ERP, or MES.

5. Regulatory Guidelines and Global Perspectives

5.1 WHO Guidelines on Data Integrity [16]

WHO Guideline on Data Integrity (Annex 4, Technical Report Series No. 1033, 2021) offers guidelines on the integrity of data throughout the pharmaceutical life cycle. It highlights the importance of ALCOA+ principles, data governance, and risk management for achieving data integrity attributes, which include attribution, legibility, contemporaneity, originality, and accuracy.

5.2 US Food and Drug Administration Data Integrity Guidance [17]

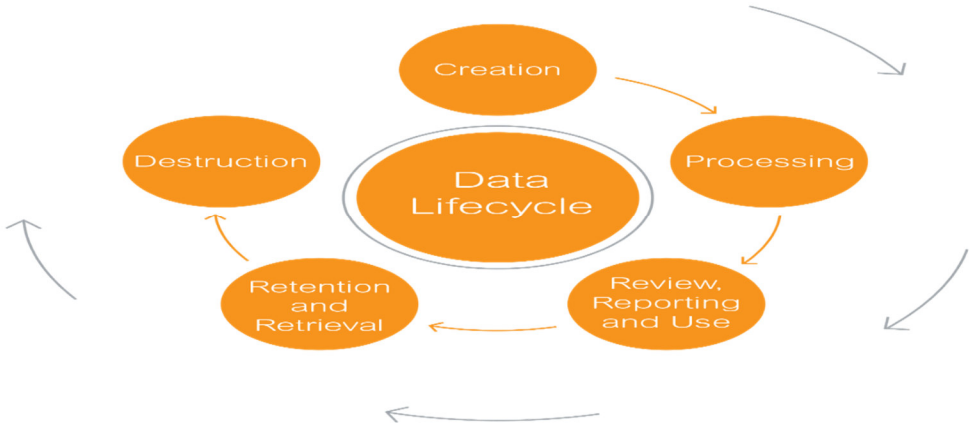
The FDA remains vigilant in their efforts to promote data integrity by mandating the need for strict compliance with ALCOA+ standards as well as 21 CFR Part 11 for electronic data and laboratory systems. The FDA will increase emphasis on the auditing of audit trails, AI-driven surveillance, and third-party contract labs. For further information, refer to FDA Data Integrity Guidance.

5.3 European medicines agency requirements [18]

The European Medicines Agency (EMA) has established an increased emphasis on data integrity as a cornerstone of pharmaceutical quality systems. This has been accompanied by increased scrutiny in regard to the role of digitized systems, Artificial Intelligence (AI), and the data life cycle. Requirements include Attributability, Legibility, Contemporaneity, Originality, and Accuracy (ALCOA+).

6. Data integrity in GMP

6.1 Manufacturing Data lifecycle [19]



6.2 Electronic vs. Paper-Based Records [20]

Factor	Paper based records	Electronic based records
Review speed	5-10 days typical for complex product	1-3 days with automated verification
Error rate	50% of batch problems from human errors	90-100% reduction in data entry error
Audit trail	Manual signatures, difficult to trace	Automatic time stamp logging of all actions
Implementation cost	Low initial cost, high ongoing labor	Lower long-term cost
Validation burden	None required	Full IQ/OQ/PQ needed, ongoing maintenance
Remote review	Impossible without physical document transport	Instant access from any approved location
System integration	Manual data transfer to other system	Automatic data flow to ERP, QMS, LIMS
Storage requirements	Physical space for years of archived records	Minimal server space, easy backup

6.3 Audit Trails and Access controls [21]

Periodic audits of the audit trail reports should be conducted for each computer system from which GMP data is obtained, such that may influence the safety, efficacy, or purity of a product. One way of reducing the effort involved in this procedure would be to target the more critical computer systems by prioritizing their audit trail reports, based on the outcome of a risk assessment on the data collected. The implementation of a routine monthly audit trail review is recommended for critical GMP systems and functions; otherwise, conduct such a review within a few days where necessary to investigate an error, security breach or other deviations. Many computer systems produce large quantities of audit trails and therefore applying risk assessment in order to prioritize the most critical computer functions for the highest risk audit trail report reviews is a good idea. High priority should be given to systems requiring the application of the electronic signature requirement (electronic batch records etc.). The most critical function for system review would include those involving the disposition of the product (e.g. release and rejection).

6.4 Validation of computerized systems [22]

Computer software has been established as an important component for the pharmaceutical industry. The pharmaceutical industry requires accurate protocols to ensure that high-quality end products are manufactured. Validation is a systematic approach that confirms the functionality of a process within certain limits, ensuring consistent and reliable results within certain limits. The pharmaceutical industry should be able to meet quality standards and regulations on a timely basis, following cGMP guidelines issued by regulatory bodies. Validation acts as a form of evidence proving that the process conforms to the set standards. Computer system software is often designed, developed, and tested using software tools.

6.5 Common GMP Data Integrity Issues [23]

In order to comply with legal obligations and ensure safety of the patients, it is important that this industry focuses on certain common integrity issues related to the data that can arise. Below are some of the common issues that the pharmaceutical industries face related to data integrity.

Common passwords: The "A" which is an abbreviation for Attributable in ALCOA is ambiguous because there is no clear identification as to who makes or changes the records if analysts use the same passwords.

User Privileges: Failure to set clear user privileges and segregation of duties within the software application setup enables users to make alterations to methods and integration without authorization.

Unauthorized access and changes: The lack of effective control of user data will result in unauthorized access and making unauthorized alterations to data.

Control of computer systems: Insufficient security mechanisms to protect data, such as encryption and data access, may cause vulnerability to data from malware infections, unauthorized access, or even data hacking.

Incomplete Data Entries: Incomplete or partial data entries in records, logs, or batch processing information may cause data gaps, making it difficult to fully understand the manufacturing process.

Non-conformity to Regulatory Guidelines: Lack of conformity to regulatory guidelines and recommendations, for instance, those offered by the United States Food and Drug Administration (US FDA) or similar organizations, may lead to significant penalties.

7. Data Integrity in GCP

7.1 Clinical Trail Data Management [24]

Data integrity in the context of clinical trials is an important concern not only for the pharmaceutical industry but also for researchers. There can be serious implications of lacking data integrity, including the rejection of data for use in marketing applications, the need to carry out additional studies, and even tarnishing the organization's reputation. Furthermore, there are ethical concerns about putting participants in the clinical trial at risk of being subjected to investigational medicines in cases where clinical trial data will not be useful in the end. Data integrity has been vital for new drug development programs and all research work in general. Data collected during a clinical trial serves as a basis for decision making when regulating medicines. One of the main goals of GCP inspections carried out within the regulatory process is the reconstruction of the study based on its data to make sure about the data integrity. The introduction of new technological advances, including mobile technology, telemedicine, adaptive and other novel trial methods, and more widespread use of data contracting and outsourcing creates new challenges for regulatory authorities regarding their approach to assessment of data integrity and calls for their continual optimization in the review of data.

7.2 Source Data Verification (SDV) [25]

The importance of Source Data Verification (SDV) is an oft-recurring topic in the practical Clinical Translational Science literature. However, there are relatively few publications that assess the quality of SDV, although such assessment is important in developing risk-based or reduced monitoring strategies. This review was done with the intent of looking for articles discussing SDV quality. Definitive and comprehensive definitions of SDV accuracy were not identified. To implement a reduction in SDV without considering the risk of critical findings not being discovered, i.e., SDV sensitivity, runs contrary to the tenets of GCP and QbD methodology. It is required that reference estimates (or procedures to determine estimates) of SDV accuracy be provided to effectively implement risk-based SDV reduction strategies.

7.3 Electronic Data Capture (EDC) Systems [26]

The study focuses on the innovative nature of the Electronic Data Capture (EDC) system used in clinical trials. In particular, the importance of the technology will be analyzed within the context of its contribution to data integrity, regulatory compliance, and process improvement. Therefore, the aim of the study is to critically analyze how EDC systems comply with the requirements of FDA and ICH/GCP regulations in light of the complexities involved in contemporary clinical trials. The methodology includes an extensive literature review in order to examine the opportunities and drawbacks associated with the use of the technology, alongside recent advancements. Among the main conclusions, there is an emphasis on the substantial potential of EDC systems when it comes to increasing data accuracy, timely monitoring, and regulatory compliance through proper data management and tracking. Nevertheless, the use of the system also involves numerous difficulties, ranging from significant expenses related to implementation to privacy issues and compatibility problems with other digital trial technologies. Finally, technological advancements related to artificial intelligence, blockchain, and decentralized trial models are presented as possible ways to address these drawbacks.

7.4 Patient Safety and Data Reliability [27]

Good Clinical Practice (GCP) refers to the globally accepted ethical and scientific quality standard that guarantees the safety, rights, and accuracy of data collected during the clinical

trial process. This practice requires proper monitoring, obtaining of informed consent from participants, and proper documentation of the study's results to verify their credibility.

7.5 Inspection and Compliance Challenges [28]

Challenges in GCP inspection and compliance are related to the need for ensuring data integrity, documentation, and safety in complicated multi-site clinical trials. Poor management of Trial Master Files (TMFs), ineffective informed consent, and failure to follow protocols are some common problems in GCP inspections.

8. Data Integrity in GDP

8.1 Principles of Good Documentation Practice [23]

Good Documentation Practices (GDP) Data Integrity make sures that pharmaceutical, clinical, and laboratory documentation maintain its accuracy and consistency throughout its entire life cycle in compliance to ALCOA+. This includes ensuring that the information is attributable, legible, contemporaneous, original, and accurate, among others. ALCOA (Attributable, Legible, Contemporaneous, Original, and Accurate) refers to the framework that is in compulsion for the application of Good Documentation Practice (GDPs) and is adapted by regulated organizations for maintaining the data integrity. Both electronic and paper data are covered under ALCOA. The principles of ALCOA are crucial for driving data integrity efforts, maintaining GDPs, complying with GMPs, and maintaining electronic and paper data management process throughout its lifecycle according to specifications. ALCOA, an acronym, was first introduced in the 1990s by Stan W. Woollen, a member of the FDA's Office of Enforcement. ALCOA+CCEA (Complete, Consistent, Enduring, and Available) was highlighted in 2010. ALCOA+CCEA is often called ALCOA-C or ALCOA+.

8.2 Documentation Errors and risks [28]

- The use of scratch paper or non-official documentation forms.
- Failure to retain the original documentation (data).
- Obliteration and/or corrections over writing.
- Failure to make corrections or too many corrections.
- Failure to initial and date the procedures performed on the study form.
- Failure to fill out the study documentation.
- Inadequate explanations about the modifications to the data entry and confirmation of the data entry.

8.3 Best Practices for Documentation control [29]

The documentation control system in Good Distribution Practice ensures data integrity, traceability, and regulatory compliance in all pharmaceutical transactions. The company must have a robust documentation system with all the documents and records approved, signed, and dated appropriately under a strict versioning system, which would make sure that the latest and most up-to-date documentation system is being used. The documentation should be in compliance to ALCOA+ criteria, which ensures the data is attributable, legible, contemporary, original, accurate, complete, consistent, durable, and readily accessible. The company should maintain adequate recordkeeping for storage and distribution activities and equipment maintenance, which are readily available for review during inspection. In the event of mistakes in documentation, the errors should be corrected using an approved procedure. For example, one can strike off the erroneous document with a single line, enter the updated information, and provide the reason, date, and signature. The original data should remain visible, and no

correction should be made by erasing any part of the document. There should be adequate documentation retention policies to store and protect the documents from destruction, theft, loss, or misuse. With increasing technology, there is the need for e-documentation, which must be secured in a validated system with access.

8.4 Data Recording and archiving [30]

In Good Distribution Practice (GDP), effective record keeping of information plays an essential role in ensuring accountability and traceability. All information about pharmaceutical products, which includes the storage condition, transport information, receipt and dispatch documentation, and the use of equipment, should be recorded according to ALCOA+ principles. The acronym stands for attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, and readily available. Records should be created at the same time when the action is performed, and they should be clear, durable, and resistant to any changes that may distort their initial meaning. If any correction is necessary, it should be done using appropriate methods and should not affect the original record. Archiving information should be done properly and with all necessary measures being taken to protect its availability and safety. Both paper and electronic documents need to be stored for a specified period of time and in places where they cannot be damaged, stolen, or being exposed to any breach of confidentiality. Electronic data should be archived in validated computer systems equipped with audit trails, controlled access, and backup procedures.

9. Integration of Data Governance Across GxP

9.1 Unified Data Governance Models [31]

The implementation of data governance practices has been gaining momentum in order to facilitate successful achievement of objectives by public sector organizations. The importance of implementation of data governance in the decision-making process of the public sector lies in meeting the needs of public administration in an increasingly complicated and rapidly changing environment (Rijal, 2023; Nisar et al., 2021). The contribution made by this study is in developing a more comprehensive framework through determining the current implementation of data governance in public sector decision-making, as well as aspects that facilitate decision-making based on which further developments may be introduced in relation to the role of data governance. Similar to the situation in any other sectors, the amount and complexity of data available in decision-making of the public sector organizations are growing, owing to new sources of data as well as increased capabilities. Consequently, access to proper data has turned into an essential element of efficient decision-making (Nadal et al., 2022). At the same time, paradoxically, the growth in both number and complexity of data collected has drawn attention to the importance of ensuring proper management and accuracy of such data. Data governance refers to measures required for maintaining the accuracy.

9.2 Risk-Based Approach [31, 32]

Risk Based Approach, the risk assessment includes the systematic identification, evaluation, and mitigation of risks associated with data integrity. The ICH Q9 quality risk management principles, 6M (Man, Machine, Material, Method, Measurement, Milieu), and Failure Mode Effects Analysis (FMEA) are some of the key methodologies in this regard. These methodologies involve prioritizing controls based on their severity, likelihood, and detectability, often in line with Good Manufacturing Practices. Identifying elements of computer system configurations that may impact patient safety, product quality, and data integrity is the main objective within the risk assessment process.

9.3 Cross-Functional Coordination [33]

Cross-functional teams are key in implementing and sustaining a collaborative data governance approach. Such teams comprise experts in data governance as well as representatives from all departments, who work together to solve data problems and practice best data management policies. The main responsibility of cross-functional teams is to act as an intermediary between various business units to communicate data governance policies. Cross-functional teams help to foster a collaborative spirit by providing a space where interaction among various departments happens frequently. These teams assist in solving any potential problem related to data, making data governance policy consistent with business requirements, and encouraging data-driven decision making. Having representatives from several business lines ensures a better approach towards data governance.

9.4 Quality Culture and Leadership [34]

A robust data governance program needs good executive buy-in, where senior management will champion the implementation of the data governance program, resource allocation, and the hiring of key personnel, such as a Chief Data/Digital Officer. A culture change is necessary to ensure that data becomes viewed as an organizational asset, through the development of programs that increase data literacy among employees, allowing them to effectively leverage data. IT-Business cooperation ensures effective data governance and accountability, while proper assignment of responsibilities and the designation of data owners/stewards guarantee high-quality data.

10. Digital Transformation and Data Integrity

10.1 Impact of Digital Systems and Automation [35]

Accuracy and efficiency are some of the factors that play a vital role in motivating automation and digitalization in laboratory analysis. Through consistency in carrying out the tasks, the automation system minimizes errors and maintains accuracy in their results. Besides, they can work nonstop without challenges like fatigue. Automation also increases efficiency since it eliminates the manual activity of recording data, mixing solutions, and preparing samples.

10.2 Cloud Computing and Data Security [36]

In the last couple of years, cloud computing technology has been used to replace conventional systems of storage and management of data since cloud computing offers benefits such as cost-effectiveness, scalable and flexible among others. With enterprise being moved to a cloud setting, some issues regarding data security have to be addressed. Data security, loss of data control and regulatory compliance are the primary challenges of cloud computing technology as far as data security is concerned. This paper discusses different avenues of attack such as malicious access, internal attacks and data leakage among other things. The paper also looks at some of the security solutions currently used, such as data encryption, multi-factor authentication and good data access policies among others. In addition, we discuss how different cloud service providers should offer security in cloud computing technology.

10.3 Use of artificial intelligence and machine learning [37]

Artificial intelligence (AI) and machine learning (ML) are revolutionary industries. These technologies often simulate human intelligence, enabling machines to learn from data and make decisions. From healthcare to finance, AI and Machine learning are transforming how we work and live. AI and ML come in various forms, including supervised, unsupervised and reinforcement learning. Each type has unique applications, from predicting outcomes to finding patterns in the given data. As these technologies advance, they bring both exciting possibilities and ethical challenges to consider.

10.4 Cybersecurity considerations [38]

Digital transformation is fast changing the way organizations operate, while shopping, working, and communicating have become part of daily routine thanks to e-commerce and cloud computing. Besides personal and organizational use, critical infrastructure, including pipeline distribution and electric grids, is also being managed via online systems that can be easily hacked. With increasing reliance on digital platforms by both organizations and individuals, cybersecurity measures become more important than ever. They help protect not only the information stored within the systems but also services that provide basic utility functions for millions of people every day.

11. Risk Management in Data Integrity

11.1 Risk Assessment Tools [40]

Failure Modes and Effects Analysis (FMEA): This is a technique that tries to determine any possible failures in the process or design to avoid them before they happen.

Bow-Tie Diagram: This is a graphical method for analyzing the risks in terms of their causes and effects.

Risk Matrix: This is a graphical tool that is employed to evaluate the probability and consequences of any risk, and it can be used to prioritize risks.

Root Cause Analysis (Fishbone/5 Whys): These techniques are applied to determine the underlying cause of a particular problem.

Fault Tree Analysis (FTA): This is an analysis technique that is applied in a deductive manner to ascertain the causes of a particular adverse effect.

11.2 Preventive action and corrective Action (CAPA) [41]

CAPA in risk assessment refers to the process where an issue that is either current or likely to arise is identified, analyzed, and eliminated through the identification of its root cause. The process links reactive problem solving to preventive risk management to ensure that such issues do not recur in future. There must be a SOP that defines how corrective action and preventive action provisions will be defined for every company. There should be guidelines on how such procedures should be executed in the company in cases when the product may have issues, customer complaints, or measures taken to ensure that the cause of detected nonconformity or incident. Efficient corrective action and preventive action programs (CAPA) are crucial parts of continual improvement processes. This article offers a detailed insight into various aspects of conducting corrective action and preventive action including mechanisms used for taking such action, their impact on the quality management system and application of CAPA system during the entire lifecycle of a pharmaceutical product, as well as the importance of establishing the change management system following the CAPA.

11.3 Continuous monitoring [42]

Continuous risk monitoring represents a modern method of risk assessment that has replaced the conventional way of conducting periodic risk assessments through continuous, automated monitoring of risk factors, risks, and threats. This is because the risk analysis process involves continuous analysis using available data to identify cybersecurity risk, compliance risk, and operational risks as they occur. Continuous risk monitoring allows organizations to capture information from different sources in real time, detect potential risks and fraud, and continuously modify their risk management strategy based on emerging risk. Automated risk alerts help the stakeholders take appropriate actions where there are deviations. Some essential

elements of continuous risk monitoring are identifying key risk indicators, adopting automation tools, and developing risk awareness.

12. Common Challenges and Deficiencies

12.1 Human Errors and Training Gaps [43]

Another common issue that is often encountered during investigations related to data integrity and data quality issues is human error or lack of training. These issues are commonly experienced due to the absence of knowledge regarding SOPs, ignorance regarding the importance of data integrity principles (ALCOA+), and lack of training on how to properly handle analytical tools and systems. Some examples of human error include data entry mistakes, failure to document results in a timely manner, failure to properly document information, and even intentional omission and manipulation of results. In some cases, there might be insufficient training, as well as lack of evaluation and assessment of personnel's ability to determine if they have been trained adequately. Additionally, high workload, pressure from deadlines, and poor supervision also contribute to human error.

12.2 System Limitations [44]

The system problems are those associated with ineffective requirements gathering, insufficient scalability, security concerns, and high costs of maintenance. Some of the common problems facing IT departments today include poor performance resulting from aged infrastructure, poor compatibility with the latest technologies, and lack of consistency with the data within the systems.

12.3 Regulatory Non-Compliance Trends [45]

There are various challenges arise that have led to increasingly complicated compliance and regulatory environments. Executives are now being held personally responsible for any misconduct of their organizations', especially concerning issues like frauds and money laundering. Besides, technology has been evolving rapidly in recent years, making old regulatory methods insufficient. The growing number of cybersecurity and data privacy threats is another factor contributing to compliance problems; the cost associated with non-compliance is estimated to be around $4.61 million. ESG reporting has also become a center point for regulatory authorities, especially where companies make misleading sustainability statements. Lastly, proactive real-time monitoring is gaining prominence through AI applications.

12.4 Case examples of warning letters [46]

The warning letters issued by the FDA are formal communications to manufacturing companies, clinical investigators, and establishments in violation of government rules and procedures, especially Good Manufacturing Practices (cGMP). Some common violations include a lack of proper investigation for quality complaints, non-compliance with SOPs, and unsatisfactory aseptic practices in drug, food, and medical device industries.

13. Best Practices for Ensuring Data Integrity

13.1 Implementation of ALCOA+ [23]

Change management, independent data review methodologies, and the use of modern technologies like electronic signatures and audit trail systems in pharmaceutical companies. The article also mentions the significance of data backup and recovery procedures, along with continuous improvements, in ensuring data integrity and encouraging accountability. procedures in the pharmaceutical industry that ensure data integrity in every stage of a product's lifecycle in order to promote safety, efficiency, and excellence in pharmaceutical products. It

emphasizes the need to overcome a difficult regulatory environment while underscoring the commitment of the sector to ensuring data integrity.

13.2 Training and Awareness Programs [47]

Data integrity education and training programs are necessary activities aimed for training staff members on data integrity concepts to achieve consistent, accurate, and reliable data. Such activities will decrease the likelihood of mistakes and data breaches. Moreover, these activities will ensure that the organization adhere with legal requirements such as the GDPR and HIPAA. Successful training programs will includes educational elements, phishing simulations, and open communication.

13.3 Periodic Audits and Self-Inspections [23]

Routine audits and inspections play a vital risk management role in the pharma and regulated industry to ensure accuracy, completeness, and consistency in data across its entire life cycle. The audit process carried out by competent internal staff ensures adherence to Good Manufacturing Practices and Standard Operating Procedures.

13.4 Strong Documentation System [23]

Data management requires a number of important controls for effectiveness. Document control and versioning will help to use the up-to-date documents only, thus avoiding any possible mistakes because of outdated information. Audit trails will ensure that all data management processes are secure and have time stamps attached to each action taken within the system. EDMS is an effective tool for ensuring centralized storage of documents and more convenient management as compared to paper-based systems. Access control helps to prevent unauthorized access to the system and make sure only relevant people are allowed to use it.

13.5 Vendor and Third-Party Management [48]

The risk management of vendors or third parties is becoming crucial for developing successful data privacy strategies. As companies continue to establish connections with different external actors, the threat of data privacy breaches through third-party collaboration becomes much higher and harder to control. Thus, this article will discuss the complexities and nuances of effective vendor and third-party risk management with particular attention to such aspects as conducting thorough data privacy risk assessment, performing due diligence checks and monitoring, and complying with regulations like GDPR, CCPA, and HIPAA. To begin with, it would be reasonable to consider the regulatory framework governing the handling of personal information by third parties. Companies must protect their private data from any kind of misuse; at the same time, vendors must also follow all the applicable laws. Therefore, there should be strict requirements for contracts with third-party entities, such as data privacy clauses and audit plans. Moreover, special attention should be paid to managing risks while interacting with vendors. In addition to regular data privacy risk assessments and due diligence, organizations have to address some difficulties, for example, dealing with cross-border data transfer. Finally, this article touches upon new technology-based methods for vendor risk management and mentions.

14. Case Studies and Practical Applications

14.1 Pharmaceutical Manufacturing [49]

Illustrations in case studies and practical applications in pharmaceutical production stress the need to ensure data integrity and compliance in real-life situations. For example, events including data tampering, insufficient record keeping, and the inability of quality assurance systems to deliver results in actions such as warning letters and recalling of products from the

market. From this example, one can see that poor GMPs and insufficient training may affect product quality and consumer's safety. In a positive light, putting into place strict quality management systems, validated electronic documents, and audit trails has helped companies achieve better performance levels.

14.2 Quality Control Laboratories [50]

Laboratories have the essential function of assuring quality in the pharmaceutical manufacturing process through the assessment of raw material and final product according to USP guidelines before the latter is released into the market. The appearance of an unknown impurity in a tablet being tested using HPLC analysis will call for a failure investigation. Mass spectrometry will be applied to determine the identity of the impurity, which will prompt changes in the manufacturing process to decrease any further degradation. In FDA audits of pharmaceutical companies, emphasis is placed on proper laboratory procedures, calibration of equipment, and OOS investigations.

14.3 Lessons learned with regulatory actions [51]

Insights gained from various regulatory investigations into violations related to pharmaceuticals and data integrity point to the necessity for having effective quality systems and a culture geared toward ensuring compliance. Most regulatory findings have found out that ineffective documentation procedures, lack of training, and absence of data integrity controls may be the root causes of regulatory non-compliance. From experience, it is crucial for any organization to have complete, accurate, and timely documentation, conduct proper investigations of deviation and out-of-specifications (OOS), and implement audit trails to track any changes. Other issues which are identified from regulatory findings include management oversight, conducting internal audits, and validating computer systems.

15. Future Trends and Innovations

15.1 Blockchain in Data Integrity [52]

Data integrity involves ensuring that data accuracy and consistency remain intact throughout the entire life cycle of the data. Data integrity is facilitated by blockchain technology owing to several attributes inherent in it. First, due to its immutability, once the data is entered into the blockchain, it cannot be tampered with or altered. It also maintains transparency in transactions such that any history of data can easily be verified. Timestamping of blocks is yet another feature of blockchain technology that enables authentication of data.

15.2 Advanced Analytics for Compliance [53]

Advanced analytics is revolutionizing compliance management by automating it through the use of artificial intelligence (AI). With advanced analytics, organizations will be able to manage risks promptly using technologies such as machine learning, NLP, and graph analytics among others. Predictive monitoring can be used to anticipate any risk that an organization faces while anomaly detection helps in detecting abnormal behaviour of transactions. On the other hand, AI investigations are important in analysis of communications and documents. Graph analytics, which uses social network analysis to expose any fraudulent activities, and automated reporting are other key areas where AI can be applied.

15.3 Real-Time Data Monitoring [54]

Real-time or dynamic monitoring is key in improving industrial system performance. It involves the collection of live data which is very essential when it comes to planning purposes and the early detection of problems before they trigger unplanned system downtime and losses in the form of income. As the technology of monitoring, especially sensors and Internet of

Things (IoT), advances and grows exponentially, there could be great sources of data that are available. This same information can serve as inputs in a dynamic life cycle assessment (LCA) to measure and evaluate its potential environmental impacts. Nonetheless, while the growth of monitoring technology opens up great opportunities, it also poses some environmental concerns, such as increased energy consumption through the use of batteries. This article highlights the application of real-time monitoring technologies in LCA studies as a basis for measuring and quantifying real-time environmental impact of the systems in different fields. In this paper, a systematic literature review was carried out where academic publications in the area of LCA studies were sought. Specifically, 34 journal articles discussing how real-time data is handled in LCA studies were collected. The results of the review show that the combination of LCA and real-time sensors.

15.4 Global Harmonization Efforts [55]

International harmonization activities in the field of pharmaceutical products mean international attempts made to bring about harmony among different countries concerning regulation standards. It is mainly due to the efforts of bodies like the ICH. The other agencies which supports international harmonization include WHO, FDA, and EMA, among others. Harmonization facilitates drug development processes, saves time, minimize costs, and enables efficient access to drugs globally without compromising on their safety standards.

16. Conclusion

Data Governance (DG) and Data Integrity (DI) are the two pillars that assure GMP, GCP, and GDP operations of their reliability, security, and adherence to the laws. The effective implementation of DG that is incorporated in the QMS helps maintain DI in data generation and management, thus allowing the compliance with the principles of Attributability, Legibility, Contemporaneousness, Originality, Accuracy, and Availability (ALCOA+). ALCOA+ can be achieved only when data is complete, consistent, available, durable, and traceable regardless of whether it was generated in paper or electronic systems. In GMP, DG ensures the proper creation, review, and retention of data concerning manufacturing operations and testing, performed using validated laboratory information management systems (LIMS), manufacturing execution systems (MES), and other similar tools. In GCP, data governance provides for the integrity of clinical trial processes, assuring the accuracy of source data, EDC validation, subject traceability, and confidentiality of personal data of study subjects. Finally, in GDP, DG is concerned with medicinal product distribution record integrity, providing for data traceability and falsification prevention, as well as the documentation of transport and storage conditions.

17. References

1. Kumar A, Yadav DK, Kumar M, Alam T, Subramanyam S. Good manufacturing practices (GMP) and regulatory challenges in the pharmaceutical industry: a comprehensive review. *Int J Creat Res Thoughts (IJCRT).* ISSN: 2320-2882.
2. Vijay Ananthan A, Nawawi O. The importance of good clinical practice guidelines and its role in clinical trials. *Biomed Imaging Interv J.* **2008** Jan 1;4(1):5.
3. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=58
4. World Health Organization. WHO good manufacturing practices for pharmaceutical products: main principles. WHO Technical Report Series, No. 986, Annex 2. Geneva: WHO; **2014**.
5. Central Drugs Standard Control Organization (CDSCO). Good Clinical Practices for Clinical Research in India. New Delhi: CDSCO; **2001.**
6. Arnold JE, Camus MS, Freeman KP, et al. ASVCP guidelines: principles of quality assurance. Vet Clin Pathol. **2019**;48(4):542–618.

7. https://www.ema.europa.eu/en/human-regulatory-overview/research-development/compliance-research-development/good-clinical-practice
8. https://www.gmp-journal.com/current-articles/details/gdp-update-for-2024-2025.
9. Kumar N, Jha A. Pharmaceutical 'good manufacturing practices' and 'good distribution practices': a comparative review of diligence in regulatory standards. *Indo Am J Pharm Res.* **2016**; ISSN: 2231-6876.
10. Paul Brous, Marijn Janssen, Riikka Vilminko-Heikkinen. Coordinating Decision-Making in Data Management Activities: A Systematic Review of Data Governance Principles. 5th International Conference on Electronic Government and the Information Systems Perspective (EGOV), Sep **2016**, Porto, Portugal. pp.115-125.
11. https://www.actian.com/blog/data-governance/data-governance-roles-and-responsibilities
12. **Kamaraj A, Puranik S.** Data integrity and meeting the regulatory expectations. *Int J Sci Res Methodol.* **2023** May;24(3).
13. Ahmad S, Kumar A, Hafeez A. Importance of data integrity & its regulation in pharmaceutical industry. Pharma Research. **2019**;8(1):306–313.
14. Choudhary Ankur. ALCOA, ALCOA+ and ALCOA++ Principles | Ensuring Data Integrity. Pharma guideline; **2026** Feb 16.
15. https://www.coursera.org/in/articles/what-is-data-integrity
16. Dakhole MR, Thombre KR, Gupta KR, Umekar MJ. Ensuring data integrity in the pharmaceutical lifecycle: Challenges, principles, and global implications. *Ann Pharm Fr.* **2026**;84(2):175–191.
17. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/data-integrity-and-compliance-drug-cgmp-questions-and-answers
18. https://www.mavenrs.com/blog/ema-gmp-guidelines-2026-eu-gmp-updates-annex-revisions-compliance-strategy
19. https://www.eurotherm.com/life-sciences-cpg/data-integrity-life-sciences/data-life-cycle/
20. Jessica R. *Paper vs Electronic Batch Records: Compliance, Costs & What to Choose*, **2025** Dec 24
21. Brandt C. *Audit trails and access control* [Internet]. GMP Compliance Consulting, NNE Pharma plan; **2014** Sep 8.
22. Raja JR, Kella A, Narayanaswamy D. *The essential guide to computer system validation in the pharmaceutical industry*. Cureus. **2024** Aug 23;16(8)
23. Gokul Krishnan D, Venkataraman S. *Ensuring data integrity: best practices and strategies in pharmaceutical industry*. Intelligent Pharmacy. **2025** Aug;3(4):296–303.
24. Hamidi M, Eisenstein EL, Garza MY, Torres Morales KJ, Edwards EM, Rocca M, Cramer A, Singh G, Stephenson-Miles KA, Syed M, Wang Z, Lanham H, Facile R, Pierson JM, Collins C, Wei H, Zozus M. *Source data verification (SDV) quality in clinical research: A scoping review*. Clin Transl Sci. **2024** May 21;8(1).
25. Ehidiamen AJ, Oladapo OO. *The role of electronic data capture systems in clinical trials: Streamlining data integrity and improving compliance with FDA and ICH/GCP guidelines*. World J Biol Pharm Health Sci. **2024** Oct;20(1):321–334.
26. Franchetti J. *Why GCP matters for patient safety and data integrity* [Internet]. JAF Consulting; **2025** Jan 16
27. https://www.fda.gov/media/185615/download
28. World Health Organization. *WHO good distribution practices for pharmaceutical products* Geneva: WHO; **2026** May 6
29. JAF Consulting. *Mastering good documentation practices (GDP): A comprehensive guide for pharmaceutical professionals*, **2024** Aug 6
30. **Osakw J.** Integrating data governance into public sector decision-making processes. **2025 Jul.**
31. International Society for Pharmaceutical Engineering (ISPE). *GAMP good practice guide: a risk-based approach to GxP compliant laboratory computerized systems*. 2nd ed.**2012**. 978

32. **Jain SK.** Strategy to avoid data integrity issues in pharmaceutical industry. *The Pharma Innovation.* **2017** Feb 1;6(2 Pt B):110.
33. Legheno IM, Segun-Falade OD, Odionu CS, Azubuike C. A collaborative model for data governance: enhancing integration across multi-line businesses. *Gulf Journal of Advance Business Research*. **2025**;3(1):47–63.
34. DAMA International. *The DAMA Guide to the Data Management Body of Knowledge (DAMA-DMBOK2)*. 2nd ed. Basking Ridge (NJ): Technics Publications; **2017**.
35. **Alzahrani ASA, Alharbi HAA, Alkhawlani HAA, Orepi AA, Alamri AA, Alzahrani AA, et al.** Automation and digitalization in laboratory testing: revolutionizing accuracy and efficiency. *Review of Contemporary Philosophy*. **2023**;22(1):2252–2266.
36. Neoaz N. Cloud computing and data security. Wilmington (DE): Wilmington University; **2023** Mar.
37. https://fiveable.me/information-systems/unit-10/artificial-intelligence-machine-learning/study-guide/8SaCGBFlYYTSFicC
38. https://www.fortinet.com/resources/cyberglossary/what-is-cybersecurity
39. https://safetyculture.com/topics/risk-assessment
40. Tashi T, Mbuya VB, Gangadharappa HV. Corrective action and preventive actions and its importance in quality management system: a review. *Int J Pharm Sci Rev Res*. **2016** Jan 1.
41. Morales P. Elevating risk management: the imperative of continuous monitoring, **2024** Dec 20.
42. Tayade MC, Ingale MH, Patil YP, Salunkhe R. Data integrity violations in the pharmaceutical industry and regulatory measures. Int J Pharm Qual Assur. **2023**;14(2):416–420.
43. Dakhole MR, Thombre KR, Gupta KR, Umekar MJ. Ensuring data integrity in the pharmaceutical lifecycle: challenges, principles, and global implications. Ann Pharm Fr. **2025**.
44. https://www.geeksforgeeks.org/common-challenges-in-system-analysis-and-how-to-overcome-them/
45. https://www.researchgate.net
46. Rathore AS, Li Y, Chhabra H, Lohiya A. FDA warning letters: a retrospective analysis of letters issued to pharmaceutical companies from 2010–2020. *J Pharm Innov.* **2022** Aug 15;1–10.
47. https://www.learngxp.com/elearning/data-integrity-awareness-introduction
48. **Anny D.** Vendor and third-party risk management in the context of data privacy,**2022** Apr
49. Rathore AS, Li Y, Chhabra H, Lohiya A. FDA warning letters: a retrospective analysis of letters issued to pharmaceutical companies from 2010–2020. *J Pharm Innov.* **2022**;1–10.
50. https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/inspection-guides/pharmaceutical-quality-control-labs-793
51. https://www.pharmaceuticalonline.com/doc/an-analysis-of-fda-warning-letters-on-data-governance-data-integrity-0001
52. https://cmitsolutions.com/tribeca-ny-1166/blog/the-role-of-blockchain-in-data-security-and-integrity
53. Ekeh AH, Apeh CE, Odionu CS, Austin-Gabriel B. Automating legal compliance and contract management: advances in data analytics for risk assessment, regulatory adherence, and negotiation optimization. *Engineering and Technology Journal* [Internet]. **2025**;10(1)
54. Da Costa TPC, da Costa DMB, Murphy F. A systematic review of real-time data monitoring and its potential application to support dynamic life cycle inventories. *Environmental Impact Assessment Review* **2024** Mar; 105:107416.
55. Lakkis MM. Global and regional drug regulatory harmonization initiatives. Regul Aff J **2010**;44(3).