ejpmr, 2024, 11(6), 175-182

SJIF Impact Factor 7.065

EUROPEAN JOURNAL OF PHARMACEUTICAL AND MEDICAL RESEARCH

www.ejpmr.com

Review Article

ISSN 2394-3211

EJPMR

DATA INTEGRITY IN PHARMA: A CRUCIAL IMPERATIVE

Rajpure Pranjal Madhukar[1]*, Devade Omkar Ashok[2], V. K. Redasani[3] and Kadam Shruti Sunil[4]

[1,4]Student, YSPM'S YTC Yashoda Technical Campus Wadhe, Satara.
[2]Department of Pharmacology, YSPM"s YTC, Satara, Maharashtra, 415011.
[3]Director of YSPM"s YTC, Satara, Maharashtra, 415011.

***Corresponding Author: Rajpure Pranjal Madhukar**

Student, YSPM'S YTC Yashoda Technical Campus Wadhe, Satara.

Article Received on 15/04/2024 **Article Revised on 05/05/2024** **Article Accepted on 26/05/2024**

ABSTRACT

Data integrity is of paramount importance in the pharmaceutical industry to ensure the safety, efficacy, and quality of products. This review article explores the challenges faced by pharmaceutical companies in maintaining data integrity throughout the product lifecycle, from research and development to manufacturing and distribution. It discusses the regulatory requirements, including guidelines from regulatory bodies such as the FDA and EMA, and highlights the consequences of data integrity breaches. Furthermore, the article examines various strategies and technologies available to mitigate these challenges, including the implementation of robust data management systems, training programs for personnel, and the use of advanced analytical techniques. By addressing these challenges proactively, pharmaceutical companies can uphold data integrity standards and safeguard public health. Terms such as ALCOA, ALCOA+ plays a major role in the integrity of data and been used by various regulatory agencies such as FDA, MHRA etc.

KEYWORDS: USFDA, Data Integrity, ALCOA, Regulatory Body.

INTRODUCTION

Data may be presented through manual recording of observations, results, or other information on paper, or by utilizing electronic records via equipment connected to a computerized system. Additionally, a hybrid approach integrating both manual and electronic systems can also be used. Maintaining data integrity (DI) involves ensuring that data records remain complete, accurate, and intact within their original context, including their connectivity to relevant data records, while also aiming to prevent any unauthorized alterations to the necessary information. The term encompasses various meanings within the realm of computing, contingent on specific contexts. Widely regarded as a proxy term for data quality, data integrity relies on data validation as a prerequisite and serves as a protective measure against data corruption.[1]

In recent years, the FDA, MHRA, European Medicines Agency (EMA), and Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-operation Scheme (PIC/S) have released several publications aimed at offering guidance on data integrity. Regulatory bodies have placed increased emphasis on data integrity concerns following the discovery of significant cGMP failures that could compromise product quality, safety, and efficacy. Taking proactive measures against data integrity issues is preferable to addressing them reactively after they have occurred.[18][7][9]

Data integrity becomes more important, as the amount of generated data and data-based decisions increase. Obviously, during the pharmaceutical data lifecycle, there are places potentially affecting data integrity. Some bad events were repeatedly 90 reported by regulatory agencies.[3][21]

The regulatory authorities have put much emphasis on data integrity in recent years because they uncovered serious cases of data integrity breaches. It is always better to proactively prevent issues, such as data integrity failures to occur, than trying to remediate and resolve inspection findings. Compliance excellence makes good business sense.[11]

According to data integrity, which is a crucial component of GMP requirements and a critical issue in any pharmaceutical health care business quality system that must guarantee that medications are of the necessary quality, data accuracy and consistency throughout the data's lifecycle are essential. As technology continues to advance the reliance on data-driven processes has increased, making it imperative for companies to adopt robust systems and practices to safeguard data integrity throughout the product lifecycle.[24]

The integrity of data collected during manufacturing activities and their used during product testing and to the confidence we can have in clinical research process.[6]

ALCOA Concept

US FDA ALCOA is the acronym for Attributable, Legible, Contemporaneous, Original, Accurate encompasses the following quality attributes for data.[7]

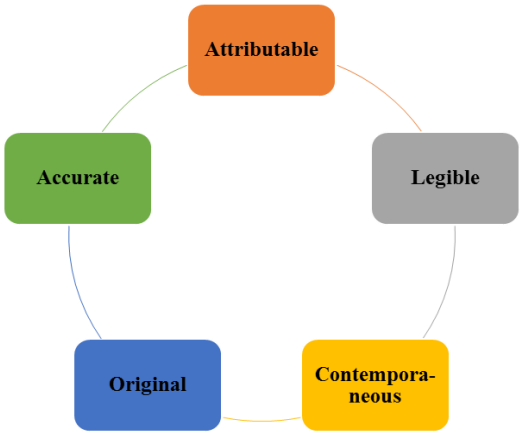

Fig No- 1.

Attributable

The identity of the person completing a record must be clear and unambiguous, ensuring data validity. Qualified individuals, with appropriate education, training, and experience, are responsible for collecting and recording data. Compliance with 21 CFR Part 11 guidelines for electronic records necessitates maintaining an audit trail, which includes registering the user, data, time of entry, and sometimes comments.[8][17][5]

Legible

The record should be easy to read and signatures should be recognizable. It can include raw data and metadata. Blank forms for manual data recordings should be controlled to stop unauthorized copying.[8][5]

Contemporaneous

Data are recorded at the time of the event / action, not transcribed at a later date. Data are not transcribed from post-it notes or scrap paper to the official documents such as batch records or laboratory notebooks.[10][8]

Original

Preserving the original record is crucial for maintaining data accuracy, completeness, content, and meaning. Metadata, which provides information about the data itself, plays a vital role in achieving this objective by facilitating the reconstruction of events.[8][5][12]

Accurate

The record is required to be free from errors or unauthorized alterations, with any changes documented through amendments or audit trail entries by authorized personnel. It must maintain accuracy, consistency, and faithfully represent the actual facts.[8][12][28]

ALCOA Plus

As a set of principles that should be followed throughout the data life cycle for achieving data integrity. ALCOA+ principles among the data generated during the process of drug manufacturing, in order to provide a quantitative measurement of data integrity compliance level.[15]

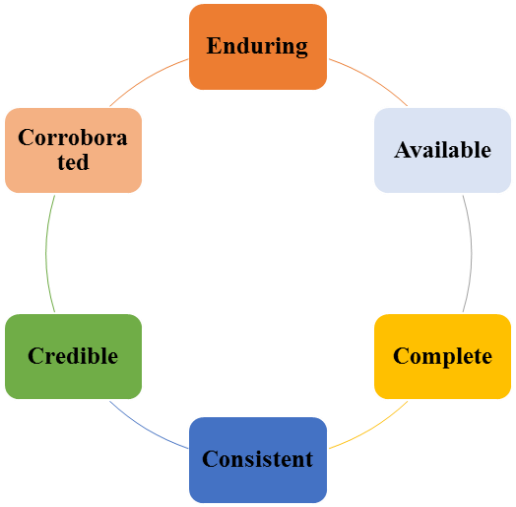

Fig No- 2.

Enduring- Maintainable and true.
Available- Easy to access.
Complete- Does not lack anything.
Consistent- Done in same sequence over time.
Credible- Convincing and effective.
Corroborated- Support or provide evidence.[2][27][28]

Data: Data is the original records and true copies of original records, including source data and metadata and all subsequent transformations and reports of these data, which are generated or recorded at the time of the GxP activity and allow full and complete reconstruction and evaluation of the GxP activity. GxP is an acronym for the group of Good Practice Guides governing the preclinical, clinical, manufacturing and post-market activities for regulated pharmaceuticals, biologics, medical devices, such as good laboratory practices, good clinical practices good manufacturing practices and good distribution practices. Data retention may be classified as archive or backup.[13][29]

Archival: The act of archiving involves keeping documents under the supervision of specialized data management staff for the duration of the mandated records retention period and safeguarding them from future alteration or deletion.[29]

Raw Data: Original records and documentation, retained in the format in which they were originally generated (i.e. paper or electronic), or as a 'true copy'. Raw data must be contemporaneously and accurately recorded by permanent means.[23]

Meta Data: Metadata is information that characterizes the properties of additional data, offering context and

significance. Typically, metadata includes details describing the organization, data components, connections, and other features of the data. It also enables data to be linked to a specific individual or source.[23]

Static Data: Static data refers to a predetermined data format, such as a static document (e.g., a paper record or an electronic image), where the content remains fixed and offers little to no interaction between the user and the record content. For instance, once chromatography records are printed or converted to a static PDF format, they lose the ability to be reprocessed or to enable more detailed examination of baselines or any concealed fields.[13]

Dynamic Data: A dynamic record format permits an interactive relationship between the user and the record content. For instance, electronic records stored in database formats offer functionalities such as tracking, trending, and querying of data. Similarly, chromatography records maintained as electronic records enable users to reprocess the data, access hidden fields with appropriate permissions, and expand baselines for clearer integration viewing.[13]

Electronic Data: This includes data from ERP software used for controlling quality systems, laboratory electronic data and records.[13]

Importance

Every day, organizations worldwide generate, capture, and leverage a growing volume of data to inform strategic business decisions. Data serves as a vital competitive advantage, given its expanding role in operations, transmission, and storage. Ensuring the reliability and relevance of this data empowers companies to gain a performance edge and effectively compete in their respective markets. However, with the proliferation of data comes an increased risk of errors, which can have significant ramifications for consumers and potentially affect a wide-ranging audience. Data integrity ensures data is discoverable, reliable, consistent, and recoverable. Protecting data's integrity can improve optimization of resources as it increases reusability. Thus, when data integrity standards are strong and vigorous, the data remains untampered and dependable, regardless of how often it is accessed, transmitted or how long it has been stored.[22]

Advantages

- Data Integrity (DI) safeguards data during end-to-end transmission via transmission mediums.
- It serves as a backup system for emergency purposes.
- Internal and external audits are conducted by regulatory bodies to ensure data integrity.
- Integrating data aids in technology transfer from pilot to large-scale manufacturing units in the pharmaceutical industry (scale-up technology).
- DI supports problem-solving and analysis by providing essential data to supervisors.
- Artificial intelligence and blockchain technology enhance data integrity and facilitate advancements in data retrieval from systems.[4]

Disadvantages

- The data integrity is susceptible to data stealing, piracy and manipulation of its content by hackers. Increases in data storage servers, globally makes the vital data prone to hacking.
- Data integrity is an old school and outdated methodology in pharmaceutical industry.
- Weak hardware quality leads to physical damage so that it reduces the chances of data retrieval and its protection.
- The artificial intelligence is more advance method when compared to the data integrity.
- The block chain technology is much more advance in its protection facility than data integrity.
- It has several kinds of limitation which prevents its usage globally.
- Data which is generated by old school handwritten method is not eligible for data storage and its integrity process in pharmaceutical industry.[4]

World Regulatory Guidance on Data Integrity

USFDA-21-CFR

The Code of Federal Regulations (CFR) comprises the enduring regulations promulgated by the executive departments and agencies of the federal government, as documented in the Federal Register. Specifically, CFR Title 21 is designated for regulations issued by the Food and Drug Administration. Notably, the content of each CFR title or volume undergoes an annual update on April 1st.[1][13]

MHRA

The guidance pertaining to data integrity expectations within the pharmaceutical industry serves as a complement to the prevailing EU Good Manufacturing Practices (GMPs) applicable to both active substances and dosage forms. Within the pharmaceutical quality system, the paramount role of data integrity is underscored, playing a central role in guaranteeing that medicinal products adhere to the stipulated quality standards.[1][26]

TGA

The TGA in Australia should focus on ensuring data integrity in the production of medicines to avoid the risk of delivering harmful products, particularly when manufacturers may mislead or distort information.[1][13]

cGMP

Recognizing the importance of data integrity, the FDA has issued guidelines on GMP compliance. The FDA identifies trends in data integrity violations and emphasizes archiving practices aligned with cGMP to prevent data loss or obfuscation. The authority for cGMP

is derived from section 1 of the FD&C Act, ensuring that drug production, processing, packaging, and administration methods comply to avoid falsification. This practice guarantees drug safety, identity, strength, and adherence to quality and purity standards**.**[1][13]

WHO

The guidelines from WHO ensure that information provided by drug manufacturers is accurate and truthful, protecting patients worldwide and maintaining high standards in drug production. Compliance with practices like GMP, GCP, and GLP is necessary for quality studies supporting drug applications.[1][13]

EMA

The European Medicines Agency (EMA) has announced new Good Product Practices (GMP) guidelines to ensure the integrity of data produced during testing, production, packaging, distribution and medication maintenance. Good control of data records is precise and consistent with the data generated and will help make good decisions by pharmaceutical manufacturers and regulatory authorities.[26]

Types of Data Integrity

Data Integrity can be classified as logical and physical integrity as follows.

1. **Physical Integrity:** Physical integration ensures data accuracy and completeness during storage and retrieval. Physical integrity is at risk from natural disasters, power outages, and hacker-inflicted database procedures. The collection of trustworthy data is a challenge for data controllers, system programmers, and internal auditors due to human error, storage degradation, and numerous other issues.[1]
2. **Logical Integrity:** The data remains constant despite variations in the application of logical integrity within relational databases. Logical integrity safeguards data from both human error and hackers, albeit in a manner distinct from physical integrity.[4]

I. **Entity Integrity:** Entity integrity relies on the establishment of unique identifiers for primary keys or data elements to prevent duplicate entries and ensure that table fields are not left empty. This feature is integral to relational systems, where data is stored in arrays that can be interconnected and utilized in various ways.[16]

II. **Referential Integrity:** Referential integrity encompasses a set of techniques aimed at maintaining consistent storage and utilization of data. Embedded within the database structure, the rules governing foreign key usage ensure that only valid modifications, additions, or deletions are permitted. These rules may encompass actions such as removing duplicate data entries, ensuring data accuracy, and restricting access to unauthorized data.[1]

III. **Domain Integrity:** Domain integrity involves a series of procedures aimed at ensuring the accuracy of all data within a domain. In this context, a domain refers to a set of allowable values that can be assigned to a column. Measures such as constraints are implemented to control the characteristics, types, and range of data that can be entered.[4]

IV. **User-defined Integrity:** User-defined integrity encompasses regulations and boundaries established by users to meet their specific needs. While the integrity of entities, contexts, and domains is crucial, it may not always suffice to ensure data security. Therefore, it's imperative to consider and implement specific business concepts in data integrity initiatives.[16][1]

Regulatory Requirements for Data Integrity

21 CFR 211 and 212: These regulations outline several key requirements pertaining to data integrity, including:

Ensuring backup data are accurate, complete, and safeguarded against alteration or loss.

Storing data in a manner that prevents deterioration or loss.

Documenting certain activities at the time of performance and ensuring laboratory controls are scientifically sound.

Retaining records as original records, true copies, or accurate reproductions.

Maintaining complete information and records of all tests performed.

Electronic Signature and Record-Keeping Requirements: Additional regulations govern electronic signature and record-keeping practices to ensure data integrity and compliance with regulatory standards.

FDA Draft Guidance, Data Integrity and Compliance with cGMP - April 2016: This guidance offers insights into best practices for creating and handling data in alignment with CGMP requirements, reflecting the FDA's current perspective on data integrity.

MHRA GMP Data Integrity Definitions and Guidance for Industry - March 2015: The MHRA provides definitions and guidance to assist the industry in understanding and implementing data integrity standards in compliance with GMP regulations.

PDA Code of Conduct: The Parenteral Drug Association's code of conduct likely outlines principles and guidelines for maintaining data integrity within the pharmaceutical industry, aligning with regulatory expectations and industry standards.[20]

Reasons for Occurance of Data Integrity[19]

- Lack of Integrity culture
- Lack of training
- Lack of supervisory controls
- Lack of awareness
- Lack of review mechanisms

Regulatory challenges due to Data Integrity issues

In recent years, large firms have encountered numerous challenges, including receiving warning letters, grappling with compliance issues, managing product imports and recalls, and facing the erosion of regulatory trust. These issues not only result in significant capital losses but also tarnish the firm's reputation. To address these challenges effectively, companies must prioritize data integrity. The USFDA reports that a staggering 95% of data integrity issues stem from poor data integrity and management practices.[15]

Major issues of Data Integtrity

Backup Data: Many companies neglect to maintain data backups, leading to potential inspection failures. Regulatory guidelines stipulate that data should be retained for a minimum of five years for pharmaceutical products, with paper records meticulously preserved and electronic data adequately backed up.[11]

Sharing Login Crendentials: In many analytical laboratories, colleagues often share login IDs and passwords. However, this practice undermines individual accountability and complicates the analysis of process changes. Sharing login credentials compromises the "A" in ALCOA principles, as it hinders the ability to attribute actions to specific individuals.[15]

Audit Trials: Numerous instruments feature audit trails, but sometimes they are disabled or inadequately maintained. It is the responsibility of management or the laboratory in charge to ensure that instruments have properly functioning audit trails.[11],[13]

User Access: Certain analysts may have access to documents that they can edit or delete. However, user access should be restricted to higher officials, and any changes made should be documented.[15]

Copying of Data: Regulatory bodies provide comprehensive guidance on data copying. Copies of data sourced from original documents must be clearly labeled as "COPY" to ensure clear differentiation between originals and copies.[15]

Strategies to prevent data integrity issues Quality Control Management within Organization

We commonly attribute data integrity lapses to fraudulent data, but most issues stem from inadequate quality practices within the organization. Implementing robust quality management systems can address these concerns. Ethical conduct, comprehensive training, and core values contribute to optimal performance. Additionally, implementing data governance ensures sustained data integrity across its lifecycle, regardless of the data format.

Control By design

Various design approaches can be implemented within the organization to uphold data integrity. These measures can be tailored to suit the organization's needs. Below are some examples of control through design:

- **System Validation:** This is a crucial element of control through design. Inadequate validation of computer systems can lead to inconsistent results. System validation ensures both technical and procedural control throughout the process.[15]
- **Personnel:** Documents pertaining to GMPs may only be added, modified, or deleted by authorized persons. All staff who are relevant, including qualified individuals, IT personnel, process owners, and system owners, should work closely together. It is imperative that all people possess the necessary qualifications, access levels, and clearly defined responsibilities to effectively perform their assigned duties.[30]
- **Audit Trails:** Audit trails consist of computer-generated records documenting the date, time, and sequence of workflow activities. Many data integrity issues stem from inadequate audit trails, leading to warning letters. It's imperative for the organization to enable audit trails in systems such as chromatography and HPLC to facilitate workflow authorization.[14]
- **Security:** Another strategy to manage problems with data integrity is to have strong computer security. Robust computer security measures guarantee that access to GMP data is restricted to authorized individuals only. Additionally, it will confirm that no attempts have been made by unauthorized persons to access the computer system or data storage devices. Computer security must also cover protocols for regular electronic data archiving, migration, and backup.[30]

Control by Monitoring

Implementing proper monitoring procedures throughout the process can positively impact data integrity. This includes internal audits conducted by the internal auditing committee and third-party audits carried out by hired review teams to assess the accuracy, authenticity, and traceability of data and provide reports. In today's digital age, electronic auditing is common, focusing on electronic records within systems. During auditing, several considerations include prioritizing electronic records over paper, configuring ER/ES software, inspecting audit trail entries, and emphasizing electronic signatures within documents.[14][15]

Improving Data Integrity in Pharma Industries Training

Creating awareness about the company’s data integrity policy to the employees and new employees is to be

made clear through scheduled training programmes conducted by experienced personnel. To make it easier to understand, it is to be oriented in various languages. This is vital since most of the errors or data integrity issues at the workplace are originated due to humans. These human errors can be prevented by appropriate training and by making the employees believe that these changes do make a huge impact on the quality of the medicines manufactured at the facility. They should understand that the impact of carelessness or fraud will ultimately affect the patients' lives. Training should be given to technical and non-technical operating staff. Data integrity culture should be followed through data integrity policies and Standard Operating Procedure.[18]

Quality Culture: For maintaining data integrity in the company, the management should make personnel create awareness about the importance of their role in safeguarding data integrity and the impact of their activities on the quality of product and patient safety. The Standard Operating Procedure for data integrity should be followed efficiently by all personnel working in the company. A code of ethics should be strictly followed and it should reflect the management's attitude towards quality. Management should try to create a quality culture in which personnel are encouraged to freely communicate about failures and errors, so that corrective and preventive actions can be taken care of accordingly. The flow of information between all levels of the organization should be permitted.[19]

Computerized Systems: Computer systems should have enough and suitable controls to prevent and detect unauthorized access or changes to data. Record should be maintained of any change made as to by whom and when the change was made. Access to folder deletion software installation and user privileges should be controlled. Computer system validation checks should be done in order to discern invalid or altered records. Computerized systems which are connected to other systems and are responsible for exchange of data electronically, should have a suitable number of checks for the secure entry of data to minimize the risks. A secure location should be allotted for backups of all data to prevent intentional or unintentional damage. In case of data review, there must be regular internal and external audits and verification of the attendance, log books and presence of the person. The frequency of data review should also be increased.[18],[27]

Electronic Systems: Biometric signatures are a method to verify an operative's identity based on measurement of an individual's physical features which are unique and measurable to that individual. For example, voice prints, hand prints and retinal scans. These signatures must consist of two distinctive components and must be used by the genuine owner. The system ensures that no two individuals have the same combination of identification codes and it should be periodically checked, recalled or revised, which is a necessary step in maintaining data integrity within electronic systems.[13]

Better Communication: Communication is a critical to reduce data integrity challenges within organizations. Making workflows simpler and following the best ways of doing things in the industry will make things less complicated. Using modern tools like LIMS, ELN, and LES means the industry needs to find a good balance between using computers and doing lab work. Making it easier to connect instruments will help a lot in reducing data problems in labs.[19]

Breach of Data Integrity[2]

Breach of data integrity refers to the violation of the integrity of the data. This shows that reality and truth are not reflected in the records and documents. This applies to the entire drug discovery and development process, which includes:

- Research and development
- Quality control
- Quality assurance
- Manufacturing
- Clinical trials
- Inspection
- Post-inspection activities

Data Integrity in research

As per the National Institutes of Health (NIH), maintaining meticulous records is imperative for the advancement of science. Accurate record-keeping not only upholds research integrity but also ensures accountability. The data collected from instruments play a pivotal role in identifying target chemicals, refining potential medications, and demonstrating efficacy, prerequisites for initiating preclinical studies. However, negligence in data integrity and records management can precipitate various challenges. These may include difficulties in collaboration and project transitions between research teams, complications in patent filings resulting in delays or failures, suboptimal decision-making regarding investments in preclinical studies, and potential rejection by regulatory agencies of Investigational New Drug (IND), New Drug Application (NDA), or Biologics Licensing Agreement submissions.[24]

Data integrity in clinical studies

It encompasses the comprehensive management of data generated by bioanalytical laboratories, which contributes significantly to Phase 1-4 clinical studies as well as Biologics License Application (BLA) and New Drug Application (NDA) submissions. Beyond the collection of clinical and non-clinical data, a multitude of critical steps must be diligently executed. These include ensuring the transportation and stability of samples and analytes, validating techniques and instruments, managing samples and studies, maintaining thorough documentation, and providing adequate training. Regulatory bodies in each jurisdiction where sponsors intend to market their products continuously update

guidelines, imposing stringent requirements for laboratory compliance.[24][25]

Data Integrity in Pharmaceutical Manufacturing

Ensuring data integrity in pharmaceutical manufacturing is critical for regulatory compliance and product safety. Implementing robust data management systems, maintaining documentation accuracy, and employing secure electronic records help safeguard the integrity of manufacturing data. Regular audits and adherence to Good Manufacturing Practice (GMP) guidelines are essential components of a comprehensive data integrity strategy in the pharmaceutical industry. Additionally, pharmaceutical companies often establish procedural controls, access restrictions, and user training programs to prevent data manipulation or unauthorized changes. Utilizing validated software systems, implementing version control mechanisms, and maintaining a secure data backup strategy contribute to data reliability. Regular validation of equipment and analytical methods further ensures the accuracy and consistency of data generated throughout the manufacturing process. Continuous monitoring, periodic reviews, and a strong quality management system play pivotal roles in upholding data integrity standards in pharmaceutical manufacturing.[17]

DISCUSSION

Data assures the quality and efficiency of innovation in the pharmaceutical organization. Data integrity is applicable for both electronic as well as manual records. Absence of data integrity may impact the organization and result in the statement of non-compliance, warning letters, importation ban, fines and penalties, reputation damage, safety alerts, share price reduction, business damage, product recalls market withdrawals and sometimes closure of companies losing thousands of jobs.[2] Regulatory challenges presented in this article will continue to attract increased international focus over the coming years. Pharmaceutical companies should plan for remediation of these challenges by establishing effective quality systems and ethics programs that allow all employees supporting GxP activities to clearly understand data integrity and its impact on patient safety, product quality, and product supply. Employees must understand their role within a GxP context and feel empowered to ensure data integrity.[14]

CONCLUSION

Ensuring data integrity in the pharmaceutical industry is paramount for maintaining product quality, patient safety, and regulatory compliance. By implementing robust systems, procedures, and training, pharmaceutical companies can safeguard against data manipulation, errors, and fraud. Collaboration between stakeholders, adherence to regulatory guidelines, and continuous monitoring are essential for upholding data integrity throughout the product lifecycle. By following the ALCOA & ALCOA+, integrity of data can be maintained. In addition to implementing robust systems and technologies, fostering a culture of integrity and accountability within the organization is crucial. This involves regular training and education for employees at all levels, emphasizing the importance of accurate data recording and reporting. Furthermore, establishing clear policies and procedures, conducting regular audits, and embracing emerging technologies such as blockchain and artificial intelligence can further strengthen data integrity efforts. Ultimately, by taking a proactive and comprehensive approach to data integrity, pharmaceutical companies can build trust with regulators, healthcare professionals, and patients, ensuring the continued delivery of safe and effective medicines.

REFERENCES

1. Nikita R. Nikam1, Priyanka R. Patil, Mr. Rohan R.Vakhariya. Data Integrity :An Overview, International Journal of Recent Scientific Research, June, 2020; 11(06(A)): 38762-38767.
2. Himani Jaiswal, Muddukrishna B. S.Girish Pai Kulyad, Data Integrity Violations: A Challenge to the Pharmaceutical Industry, INTERNATIONAL JOURNAL OF PHARMACEUTICAL QUALITY ASSURANCE, 25th Mar, 2020; 11(01).
3. Valentin Steinwandter and Christoph Herwig, Provable Data Integrity in the Pharmaceutical Industry based on Version Control Systems and the Blockchain, PDA Journal of Pharmaceutical Science and Technology, February 26, 2019.
4. Dharnish.R, Jeyaprakash M.R An Approach Of Data Integrity In Pharmaceutical Industries, Eur. Chem. Bull., 2023; 12(1): 30-36.
5. B. S. Rao and B. S. Reddy, Understanding USFDA Guidance on Data Integrity – ALCOA Plus-An Overview Article in Pharma Times, March 2022; 54(03).
6. Nader Shafiei, Regis De Montardy and Edwin Rivera-Martinez, Data Integrity—A Study of Current Regulatory Thinking and Action, PDA Journal of Pharmaceutical Science and Technology, December 22, 2015.
7. Dr. Sushmita Singh, Nikhil Punjabi, Drashti Shah, Importance Of Data Integrity In Pharmaceutical Industry, EPRA International Journal of Economics, Business and Management Studies (EBMS), February 2023; 10(2).
8. Anil K. Rattan, Data Integrity: History, Issues, and Remediation of Issues, PDA Journal of Pharmaceutical Science and Technology, March 25, 2018.
9. Barbara W. Unger, Data Integrity and Data Management for GxP regulated firms, 2014–2016.
10. DURÁa, and Ángel SÁNCHEZ-GARCÍAa, Carlos SÁEZa,Towards a Computational Approach for the Assessment of Compliance of ALCOA+ Principles in Pharma Industry, doi:10.3233/SHTI220578
11. Sasidhar Duggineni, Impact of Controls on Data Integrity and Information Systems, Science and Technology, 2023, 13(2): 29-35.

12. Patil RA, Patil SN; Data Integrity and Worldwide Regulatory Guidance; PharmaTutor., 2016; 4(5): 20-24.
13. Shmmon Ahmad, Ashok Kumar and Dr. Abdul Hafeez, Importance of data integrity & its regulation in pharmaceutical industry, The Pharma Innovation Journal, 2019; 8(1): 306-313.
14. Jain Sanjay Kumar, Strategy to avoid data integrity issues in pharmaceutical industry, The Pharma Innovation Journal, 2017; 6(2): 110-115.
15. Pralesha sahoo, Kamaraj R, Review of Data Integrity in Pharmaceutical industry, International Journal of Research in Pharmaceutical Sciences, 2020; 11(SPL4): 1323-1328.
16. Snehal Chandrashekhar Jale, Nidhee Vinayak Tendulkar, Siddhi Maruti Chavan, A Review: An Illustration of Data Integrity, International Journal of Research Publication and Reviews, May 2023; 4(5): 5620-5629.
17. Fátima Leal a,c, Adriana E. Chis a, Simon Caton, Smart Pharmaceutical Manufacturing: Ensuring End-to-End Traceability and Data Integrity in Medicine Production, Big Data Research, 2021; 24: 100172.
18. Remya James,Srija Das,Anjali Kumari.A Recent Regulatory Update on Consequences of Data Integrity Issues and its Management in Pharmaceutical Scenario, Indian Journal of Pharmaceutical Education and Research, Apr-Jun, 2021; 55(2).
19. P. Kiruba Rachel, N. Vishal Gupta, Data Integrity – Regulations and Current Scenario, International Journal of Pharmaceutical Sciences Review and Research, March - April 2017; 43(1),05: 16-22.
20. Kamaraj A, Sangamesh Puranik, Data Integrity and Meeting the Regulatory Expectations, International Journal of Science and Research Methodology, 2023; 24(3): 18-29.
21. Vignesh M, Ganesh G. N. K. Current Status, Challenges and preventive strategies to overcome data, Integrity issues in the Pharmaceutical Industry, International journal of applied Pharmaceutics, ISSN- 0975-7058, 2020; 12(6).
22. Duggineni, S. Data Integrity and Risk. Open Journal of Optimization, 2023; 12: 25-33.
23. R.D. McDowall, Ph.D. Review and Critique of the MRHA Data Integrity Guidance for Industry — Part 4: System Design, Definitions and Overall Assessment,Fri, 05/29/2015 - 1:56pm
24. Gupta KR. Ensuring data integrity in thepharmaceutical sector. Int J Pharm Chem Anal, 2023; 10(4): 218-219.
25. Saima Shahida,Evaluating The Role of Data Integrity as a Code in Regulatory Compliance for Clinical Trials, August 2023.
26. Ni A. Khin1, Gail Francis, Jean Mulinde, Cheryl Grandinetti, Rachel Skeete, Data Integrity in Global Clinical Trials: Discussions From Joint US Food and Drug Administration and UK Medicines and Healthcare Products Regulatory Agency Good Clinical Practice Workshop, Clinical pharmacology & Therapeutics, 00(0): 2020.
27. MHRA 2018. GXP Data Integrity in Pharmaceutical Industry. Medicines and Healthcare products Regulatory Agency.
28. Sia Chong Hock, Chan Lai Wah, Generics and Biosimilars Initiative Journal, Pharmaceutical Data Integrity: Issues, challenges and proposed solutions for manufactures and inspectors, 2020; 9(4): 171-82.
29. World Health Organization, Guidance on good data and record management practices, 2015.
30. Manojkumar Suryakant Bhadrashette, Overview of Data Integrity issues in the Pharmaceutical industry, Int. J. Pharm. Sci. Rev. Res., May - June 2018; 50(2): 14: 95-101. ISSN 0976 – 044X