INTERNATIONAL JOURNAL OF PHARMACEUTICAL SCIENCES
[ISSN: 0975-4725; CODEN(USA): IJPS00]
Journal Homepage: https://www.ijpsjournal.com

OPEN ACCESS

Review Article

Data Integrity Compliance, Importance, Consequences And Strategy To Overcome Data Integrity In The Pharmaceutical Industry

Sanket Gade*[1], Prerana Jadhav[2], Pradyumana Ige[3], Pratiksha Bornare[4]

[1]*S.N.D. College of Pharmacy, Yeola, Nashik*
[2]*Asst. Professor, Sanjivani College of Pharmaceutical Education and Research, Kopargaon*
[3]*Principal, S.N.D. College of Pharmacy, Yeola, Nashik*
[4]*Sanjivani College of Pharmaceutical Education and Research, Kopargaon*

ARTICLE INFO

Received: 16 June 2024
Accepted: 23 June 2024
Published: 24 June 2024
Keywords:
Data Integrity, ALCOA, USFDA, Data, 21CFR, Audit Trail
DOI:
10.5281/zenodo.12513412

ABSTRACT

Data Integrity is an important tool that regulatory agencies use to protect public health at the same time. Data Sources: The quality and safety of medications are determined by the credibility of individuals and data. Study Selection: This article discusses the terms, concepts, principle, types, significance, advantages, drawbacks, as well as reasons, and consequences of data integrity. Results: Data integrity demonstrates the pharmaceutical industry's commitment to manufacturing safe, effective pharmaceuticals that fulfill quality standards. Conclusion: Complete, consistent, and accurate data must be traceable, legible, contemporaneously documented, original, or a true copy, and correct.

INTRODUCTION

"Data Integrity" refers to preserving and assuring the consistency and correctness of data over its whole life cycle. Data reliability and accuracy are indicators of data integrity. Although integrity is essential to the value of data, data itself is not very valuable. It is now among a company's most valuable assets. Ensuring and preserving data accuracy and consistency throughout its lifecycle is known as data integrity. This covers appropriate data management and documentation procedures, such as protecting against data alteration during copies and moves. Electronic and paper records are equally subject to data integrity requirements. The word integrity evolved from the Latin adjective integer, meaning whole or complete [1]. Business owners can only increase the quality of their production, make decisions that are best for their company, and increase their overall performance when they have access to accurate data [2].

Throughout the data life cycle, errors, omissions, and inconsistencies should be simple to find and address with an efficient system architecture and

***Corresponding Author:** Sanket Gade
Address: *S.N.D. College of Pharmacy, Yeola, Nashik*
Email : sanketgade7478@gmail.com

Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

controls. Management plays a crucial role in preventing and resolving circumstances that lead to DI issues. DI confirms the pharmaceutical industry's dedication to producing safe, effective medications that meet quality standards. DI is a vital tool that regulatory bodies employ to safeguard public health at the same time. A number of regulatory actions, including the issuing of warning letters, import warnings, and consent decrees, have been caused by DI breaches of cGMP [3].

Untrustworthy data quality can have serious consequences for the concerned organization, damaging its reputation. If suitable steps are not taken to protect the safety of data, there is a high probability of receiving results that are corrupted [4].

The maintenance of data integrity now faces additional difficulties due to electronic data and computerized systems. The criteria for data integrity are the same for both electronic and manual (paper) data. Preventing problems before they arise, such data integrity breaches, is always preferable to trying to fix and address inspection results [5]. Although data integrity has long been a delicate subject in the pharmaceutical industry, regulatory agencies' attention to it has recently led to its increased significance. Data integrity assurance refers to safeguarding the original data against any inadvertent or intentional alteration, fabrication, fraud, or even removal of data. Loss of client satisfaction and trust in the business may result from the violation [6]. Maintaining data integrity is essential to the quality of pharmaceutical goods since data errors or inconsistencies can lead to contamination, defective medicinal products, or even patient injury. For instance, improper recording of production data may result in inaccurate dosages or missing ingredients in a particular medication, which may have adverse impacts on patients who use it [7]. Data integrity is against data corruption[8].

Integrity in Daily Life

Integrity: doing the right thing when no one is watching Integrity is the “Doing the Right Thing for the Right Reason"[1]. Do it RIGHT the first time.

Terms:

1. Data:

Data means 'Facts, figures and statistics collected together for reference or analysis. Data may be contained in paper records (such as worksheets and logbooks), electronic records and audit trails, photographs, microfilm or microfiche, audio or video files or any other media whereby information related to GMP activities is recorded. Data should be accurately recorded by permanent means at the time of the activity [1].

2. Metadata

Metadata is often described as data about data. Metadata is the contextual information required to understand data. For example, the number “10” is meaningless without metadata, if unit "mL." is not mentioned.

3. Static and Dynamic records

Print out taken for Reviewed Chromatogram is Static Data. A static record, such as an electronic image or paper record, is a document with fixed data. A "dynamic record" is one in which user and record content can communicate with one other through the record format. Information that is originally captured in a dynamic state should remain available in that state [1].

4. True Copy

A true copy is an accurate, validated replica of an original data record (such as validation reports, analytical summary reports, etc) [1].

DATA LIFE CYCLE

All phases in the life of the data (including raw data) from initial generation and recording through processing (including transformation or

migration), use data retention, archive/retrieval and destruction

Generation > Processing > Use > Retention > Archival/Retrieval > Destruction

Data Integrity Definitions according to Guidelines

1. USFDA

Data integrity refers to the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA).

USFDA has published the 21 CFR Part 11 and EU has published Annex 11 to spell out the requirement with respect to computerized system. 21 CFR Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations [9][2][5].

2. MHRA

As per MHRA, GMP data integrity guidance for industry March 2018. Data integrity is the degree to which data are complete, consistent, accurate, trustworthy, reliable and that these characteristics of the data are maintained throughout the data life cycle. The data should be collected and maintained in a secure manner, so that they are attributable, legible, contemporaneously recorded, original (or a true copy) and accurate. Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles and good documentation practices [10][11].

3. EMA

The European Medicines Agency (EMA) has released new Good Manufacturing Practice (GMP) guidance to ensure the integrity of data that are generated in the process of testing, manufacturing, packaging, distribution, and monitoring of medicines. Regulators rely on these data to evaluate the quality, safety, and efficacy of medicines and to monitor their benefit-risk profile throughout their life cycle [12][1].

4. TGA

Australian regulatory body Therapeutic Goods Administration (TGA) give the requirement of data integrity in the form of deficiency. A deficiency in a practice or process that has produced, or may result in, a significant risk of producing a product that is harmful to the user. Also occurs when it is observed that the manufacturer has engaged in fraud, misrepresentation or falsification of products or data." Data Integrity is defined as "the extent to which all data are complete, consistent and accurate, throughout the data lifecycle"[13].

5. cGMP

The FDA produced guidelines on Data Integrity and Compliance with cGMP as a reflection of the significance of this issue, and within the guidance, the FDA recognizes the pattern of rising data integrity breaches. Records-keeping procedures that adhere to cGMPs avoid data loss or obscuration. The FD&C Act gives the FDA the power to regulate cGMP. Section 501 A Drugs are considered adulterated if “the methods used in, or the facilities or controls used for, its manufacture, processing, packing, or holding do not conform to, or are not operated or administered in conformity with current good manufacturing practice to assure that such drug meets the requirement of the act as to safety and has the identity and stringent quality controls" [14].

6. WHO

Essential drugs and health products, WHO is launching data integrity guidelines to protect patients around the world. It involves a number of artists and activities, a fundamental step added to the persistence and accuracy of the data submitted by manufacturers to the National Regulatory Authority. These data must be complete, complete and accurate and truthful in order to determine the quality of the studies that support drug

applications in the market. In addition, many standards must be followed, namely: good manufacturing practices (GMP), good clinical practices (GCP) and good laboratory practices (GLP)[15][8].

Audit Trail

The audit trail is a form of metadata containing information associated with actions that relate to the creation, modification or deletion of GxP records. An audit trail provides for a secure recording of life cycle details such as creation, additions, deletions or alterations of information in a record, either paper or electronic, without obscuring or overwriting the original record. An audit trail facilitates the reconstruction of the history of such events relating to the record regardless of its medium, including the "who, what, when and why" of the action [15].

Electronic audit trails include those that track creation, modification, or deletion of data (such as processing parameters and results) and those that track actions at the record or system level (such as attempts to access the system or rename or delete a file) [9].

Backup

A current, editable copy of the system configuration settings, metadata, and data is kept for recovery purposes, including disaster recovery. Backup to refer to a true copy of the original data that is maintained securely throughout the records retention period [9].

It's crucial to remember that backup copies of electronic documents are different from archival copies in that they are usually only kept temporarily for disaster recovery purposes and may occasionally be overwritten. It is not advisable to rely on backup copies as a means of preservation. For the duration of the records retention period, it is a genuine copy of the original data that is kept safe[1].

Principle of Data Integrity:

ALCOA is defined by US FDA guidance as Attributable, Legible, Contemporaneous, Original and Accurate. It relates to data, whether paper or electronic and these simple principles should be part of your data lifecycle, GDP, and data integrity initiatives. It helps in developing strategies so that the integrity of the evidence is maintained both in research and manufacturing [1].

ALCOA+++

- Attributable
- Legible
- Original
- Accurate
- Contemporaneous
- Complete
- Consistent
- Enduring
- Available

Attributable

The personnel's identity, actions, time, and date are documented.

revealing the accountability. The person's work or activity should be identified, along with the date and time, from the papers that are accessible. An audit trail in an electronic system or the signing and dating of a paper record can both be used to document this.

Legible

All users can clearly see the data, whether it is in the form of handwritten text, photographs, or computer formatting. clarity in both understanding and reading. The recorded information should be preserved in an electronic format, handwritten document images, scripts, graphs, etc. A document that cannot be read has no value. Keeping records legible and archival contributes to their accessibility across the course of the data lifecycle. GDP consistently encourages the use of permanent ink while writing out documentation.

Contemporaneous

Data is captured during the course of the action in real-time, or as soon as the event occurs.

Contemporaneous refers to recording the outcome, measurement, or data as soon as the task is completed—neither before nor after. For the data to be reliable, the date and time must match the order of execution. Never date data backwards.

Original

Not a duplicate. If copies are created, they need to be properly identified. A primary type or form that is produced and introduced for the first time. The media in which the data is initially captured is known as original data, commonly known as source data or primary data. This could be a worksheet, a form, an authorized protocol, or a database. To maintain the original data's meaning and content, it is crucial to know where it will be generated.

Always present the original documents related to work, activity or incident.

1. Original Documents

If copies are created, they must be distinctly labeled.

2. No Transcriptional Error

Details and information should be directly entered into the authorized documents. Steer clear of transcribing mistakes.

3. Version History

To preserve the original data in its original form, note any changes or modifications in the version history.

4. True Copy

Make sure to create a "true copy" of any handwritten original data that needs to be electronically recorded, have it checked for accuracy, and then transfer it into the electronic system.

5. Accurate

100% accurate and true to the event when it was captured. Defect-free; complies with guidelines or regulations. In order for data and records to be considered accurate, they must be free of errors, complete, truthful, and impartially proof of the actual and documented the event. Data and record corrections should never be made without an adequate explanation or reasons being documented.

6. Complete

Data is complete (no incomplete recording, change, or erasure). The data must consist of an entire set. Any generated data must be kept up to date and made available upon request from regulatory bodies.

7. Consistent

The information should to be self-explanatory and self-consistent. Logically consistent and established processes should be followed while creating, processing, and storing information. This covers guidelines or practices that support data control or standardization (e.g., date formats, units of measurement, rounding techniques, chronological sequencing, significant digits, etc).

8. Enduring

Data is preserved by storing it in a way that makes it durable.

1. sustaining the whole lifecycle of the data.

2. Important documents must be protected in order to guarantee the durability of all documents, including those in electronic form, in accordance with legal obligations.

9. Available

Data is available for viewing (in a suitable time window). Easily accessible for examination or inspection Within a fair timescale, make the data accessible or available for review or inspection. There should be a process in place for retrieving the records after they have been archived in safe locations.

TYPES OF DATA INTEGRITY

A. Physical Integrity

Physical integrity is jeopardized when natural disasters happen, power outages occur, or hackers disturb database operations. Human errors, storage erosion, and other difficulties make it impossible for data controllers, system programmers, seas

application programmers, and internal auditors to access accurate data [8].

B. Logical Integrity

It protects against hackers and manual errors. When creating a database, ensuring data integrity should be a priority. For this reason, wherever possible, a proper database will enforce data integrity [16].

1. Entity Integrity

It is based on providing unique values that highlight the data component to ensure that the data record is not mentioned more than once. It is ensured that each row in the table is distinctive and that no two rows have the same identifier.

2. Referential Integrity

It refers to a series of procedures that ensure that information is secure and usable. Referential integrity prevents users from linking records to connected records and changing values that result in an orphaned record.

3. Domain Integrity

A collection of procedures known as "domain integrity" guarantee the accuracy of every piece of data within the domain[16].

4. End user defined integrity

Rules and limitations that the user has established to suit their own requirements are included in user-defined integrity. It gives the user permission to apply rules that are not covered by the other three types of data integrity safeguards in the database[16].

Importance of Data Integrity

The importance of precise and trustworthy data in guaranteeing the security and quality of drugs. The FDA and other international authorities stress the data integrity, as the regulator has done for many years[8].

1. Safety & Effectiveness [2]

The safe use of medications is ensured by data integrity. It also shows that taking medication will cause them to function. This is because all knowledge pertaining to manufacturing is protected. Adequate data integrity is essential for effective treatment.

2. Accuracy [2]

The safe use of medications is ensured by data integrity. It also shows that taking medication will cause them to function. This is because all knowledge pertaining to manufacturing is protected. Adequate data integrity is essential for effective treatment.

3. Effective Production and Distribution [2]

Adhering to data integrity protocols facilitates the distribution and manufacturing of pharmaceuticals. Data integrity is used by pharmaceutical companies to develop the finest possible drugs. In the same way, it helps them give these medications to the right patients.

4. Trust Building [2]

It is difficult for consumers to trust pharmaceutical companies if their data is compromised. Furthermore, other companies would reject any kind of association. Building and sustaining trust is achieved through maintaining data integrity.

Advantages and Disadvantages

1. Advantages [16]

- It guarantees standards for both goods and services.
- It guarantees clients' privacy and protection.
- Create a data security substructure.
- Redundant data control.
- Greater details from the same quantity of data.
- It is accurate, comprehensive, retrievable, corroborated, and true.
- Enhanced upkeep and integrity of data.
- A higher level of concurrency

2. Disadvantage [16]

- The data management system is extremely complex.
- System memory and storage space requirements are higher.

- The database method offers certain applications that might not operate quickly.
- By accident, malicious insider or outsider attacks have altered data.
- Greater impact from failing.

Reasons for Data Integrity to Occurs [1]

1. Absence of raw data to back up records or data loss during system modifications.
2. Producing incomplete and improper documentation.
3. One batch's test finding are used to release subsequent batches.
4. Eliminating data from recurrent trials, sample runs, and trial runs (checking for compliance).
5. Modifying the chromatographic data's integration parameters to get passable results.
6. Data fabrication or the deletion/manipulation of electronic records.
7. Disabling audit trail.
8. Password sharing.
9. Insufficient restrictions on powers of access.
10. Inadequate or without computer validation.
11. Actions that were not immediately documented.
12. Employees who sign off on finishing manufacturing steps even though they weren't present when the stages were finished.
13. Manpower shortage
14. Quantity rather than quality
15. Ignorance
16. Training's efficacy
17. Falsifying information
18. Wrong data recording
19. When to date: in forward or backward
20. Falsifying, misrepresenting, leaving out information, or making a claim without providing proof of a real occurrence
21. Providing erroneous information.
22. Doubling up on current data to create new data
23. Maintaining Two Sets of Documents
24. Ignoring facts, whether in hard copy or electronic form.
25. Neglecting unjustified failed test results
26. Process changes that are not warranted should be notified.
27. Signing analyst or operator work without first examining the raw data gives supervisor approval.
28. Time and Pressure at Work
29. Inadequate understanding and awareness
30. Fear of Making Errors
31. Pressure to perform
32. A given authorization to carry out the action that is against cGMP procedures by a manager or leader.

Data Integrity Risk due to Human errors

a) Unintentional Human Errors

1. Something that unconsciously happens to us: without realizing it.
   Example: Error due to attention failures, error due malfunctioning of instrument.
2. Processing treatment of data isn't optimized or contains errors
3. Fundamental GDP mistakes lapses (e.g. forgot to record, sign, check etc. a data entry at the time of the original event

b) Intentional Human Errors (Fraud)

1. Intentionally changing falsifying, deleting, alteration, manipulation & hiding of data
2. Lying to or misleading an inspector or auditor.
3. Favorable data selection from the set of the data [15]

Data Integrity Consequences

Data integrity problems can have a wide range of effects on different stakeholders, including customers, patients, and regulators, both directly and indirectly. The worst case scenario involves harm to patient security and fatalities.

1. Warning Letters, Statement of Non-Compliance and Consent Decrees

Following the discovery of data integrity problems, the regulatory bodies have sent pharmaceutical manufacturing facilities several warning letters, notifications of non-compliance,

and consent decrees. The company's ability to obtain permission for a new drug product for sale will be impacted, and regulatory bodies may lose faith in it if they take these kinds of actions.

2. Import Alert, Product Recalls and Seizure of Products

Adulterated drug products are those that contain data integrity problems. The US FDA will impose restrictions on their ability to sell these contaminated pharmaceutical items in the US. FDA field employees and the general public are notified by import alerts that the agency has sufficient proof to mandate the detention of products that seem to be in violation of FDA laws and regulations without a physical examination.

3. Need to appoint Third Party Consultants for Data Integrity

Following the issuance of a warning letter by the US FDA to the pharmaceutical facility, the FDA recommends that the firm engage the services of a third-party consultant with expertise in identifying data integrity issues to help with the evaluation process and to support the company's overall CGMP compliance.

4. Loss of Regulatory Trust

The loss of regulatory trust is likely to occur when problems with data integrity surface. This will make it more difficult for a corporation to obtain approval for the common issues they may wish to do and lead to more regular inspections of the facility in the hopes of finding more evidence to support allegations.

5. Debarment and Imprisonment (for Individuals involved in data integrity issue)

A case study provides a thorough understanding of the impact that data integrity issues can have on those who are involved in them [8].

Data Integrity Remedies

1. Personnel preparation

The personnel involving in generating, reviewing and approving data must have adequate knowledge and skills to generate GMP environment and keep up to the data integrity expectations [4].

2. Being proactive

Being proactive in detecting the potential data integrity issues and upholds the civilizing elements supports data integrity in the organization. Frequent audits on data integrity should be performed and issues in potential or questionable practices should be identified4].

3. Training

Employees and new hires should be made aware of the company's data integrity policy through regularly scheduled training sessions provided by knowledgeable staff members.

Make sure employees know how to handle data in order to minimize mistakes and maintain accuracy. Furthermore, training maintains workers' dedication to overall quality, which is beneficial to the company [6].

4. Quality Culture

In order to maintain data integrity throughout the organization, management should train staff members on the significance of their role in maintaining data integrity as well as the effects of their actions on patient safety and product quality. It is the goal of management to promote a culture of quality where employees feel comfortable to discuss mistakes and failures so that appropriate preventive and remedial measures can be implemented [6].

5. Computerized Systems

Enough and appropriate controls should be present in computer systems to stop and identify illegal access or data modifications. Any changes made, along with the information about who made them and when, should be documented. User privileges and access to the installation of folder deletion software should be restricted [17][6].

6. Electronic Systems

Using a measurement of a person's unique and measurable physically characteristics, biometric signatures are a way to confirm an employee's

identity. Comply 21 CFR Part 11, EUGMP Annex 11, and additional regulatory requirements; verified [6].

7. Protect Your Documents

You can secure the records by imposing restrictions on the files.

You can use a password to encrypt PDFs and documents [8].

8. Data encryption

Another helpful option is encryption, which is especially helpful for managing communication over the internet or between devices. Before it can be used by others, stolen data needs to be decrypted, allowing producers ample time to identify an attack and take the necessary countermeasures. Since data integrity also depends on data uniqueness, keeping track of user IDs and passwords can help prevent unauthorized access [8].

9. Introduce Access Controls

Data can be seriously harmed by someone with bad intent and no formal access. One extremely common method of access control is to implement a minimum privilege model, where access is granted to users who need to view the data [8].

10. Leverage Audit Trails

An audit trail created by a computer that is time-stamped keeps track of the names, dates, and timestamps of all data additions, changes, and deletions. Audit trails give the breadcrumbs that lead to the problem source in the event that data is compromised [8].

11. Passwords

To stop illegal access to any storage device where data is kept, use passwords. Never save the passwords on sticky notes or your computer [8].

RECOMMENDATIONS

1. Organizations should prioritize long-term sustainability over short-term gains
2. They should concentrate on systems and procedures
3. They should emphasize QBD, or quality by design, and RFT, or right first time concepts
4. They should emphasize better process understanding over the traditional trial-and-error method
5. They should involve SME, or subject matter experts, and outside DI consultants
6. They should avoid placing undue pressure on output or yield improvement, as this could push employees to engage in DI issues.
7. Strengthen internal audit oversight, including cross-functional specialists in self-inspections, and make sure the purpose of the inspections is improvement
8. Provide the necessary and sufficient resource-based management support.
9. Develop knowledge-sharing procedures, provide a suitable forum, and disseminate the lessons learned among the company's several manufacturing locations.
10. Acquire lessons from both your own and other businesses' failures.
11. Keep an eye on industry developments and update the fundamental personnel's skills and expertise.
12. Pay attention to training that is effective and assess it to gauge its impact [4].

CONCLUSION

The pharmaceutical industry depends heavily on data integrity, and companies should be able to prove it in regulatory audits. The company's trust in using correct information to comply with regulatory standards is based on the use of quality data. After all, your company's growth potential increases with the amount of data you have. Data integrity issues like developing and upholding a quality culture, control by design, control by process, cGMP training, and other techniques can be resolved with good strategic planning. Companies who violate data integrity suffer penalties include warning letters, consent decrees, product recalls, imprisonment, decreased market

value, and decreased consumer trust. We discussed data integrity, its benefits and drawbacks, problems with data integration that the pharmaceutical industry faces, the causes of improper data management, a warning letter on this issue, and the solution in the review article mentioned above.

ABBREVIATION

1. DI – Data Integrity
2. MHRA – Medicine and Healthcare Products Regulatory Agency
3. USFDA – United State Food and Drug Administration
4. WHO – World Health Organization
5. TGA – Therapeutic Goods Administration
6. EMA – European Medicines Agency
7. GDP – Good Documentation Practice
8. CFR – Code of Federal Regulations
9. HPLC – High performance Liquid Chromatography
10. cGMP – Current Good Manufacturing Practices
11. GMP – Good Manufacturing Practices
12. QbD – Quality by Design

CONFLICT OF INTEREST

The authors have no conflicts of interest regarding this investigation**.**

REFERENCE

1. Ahmad S, Kumar A, Hafeez A. Importance of data integrity & its regulation in pharmaceutical industry. Authorea Preprints. 2022 Sep 8.
2. Singh S, Punjabi N, Shah D. IMPORTANCE OF DATA INTEGRITY IN PHARMACEUTICAL INDUSTRY. EPRA International Journal of Economics, Business and Management Studies (EBMS). 2023 Feb 27;10(2):100-6.
3. Vignesh M, Ganesh GN. Current status, challenges and preventive strategies to overcome data integrity issues in the pharmaceutical industry. International Journal of Applied Pharmaceutics. 2020 Nov 7:19-23.
4. Kumar JS. Strategy to avoid data integrity issues in pharmaceutical industry. The Pharma Innovation Journal. 2017;6(2):110-5.
5. James R, Das S, Kumari A, Rekdal M, Kulyadi GP, Sathyanarayana MB. A recent regulatory update on consequences of data integrity issues and its management in pharmaceutical scenario. Indian Journal of Pharmaceutical Education and Research. 2021 Apr 1;55(2):S616-22.
6. Kavasidis I, Lallas E, Leligkou HC, Oikonomidis G, Karydas D, Gerogiannis VC, Karageorgos A. Deep Transformers for Computing and Predicting ALCOA+ Data Integrity Compliance in the Pharmaceutical Industry. Applied Sciences. 2023 Jun 28;13(13):7616.
7. Nikam NR, Patil PR, Vakhariya RR, Mohite SK, Magdum CS. Data Integrity: An Overview. International Journal of Recent Scientific Research. 2020;11(6):38762-7.
8. Snehal Chandrashekhar Jale, Nidhee Vinayak Tendulkar, Siddhi Maruti Chavan, Sayali Venkat Bir adar, Jayshree Kishor Sonawane, Ishwari Prakash Narkar, Aayesha Dashrath Barge, Vaishali Jadhav, Dr Ashish Jain. A Review: An Illustration of Data Integrity. International Journal of Research Publication and Reviews.2023; Vol 4, no 5, pp 5620-5629
9. http://www.fda.gov/ (Guidance for Industry - FDA)
10. Medicines & Healthcare Products Regulatory Agency (MHRA) GXP Data Integrity Guidance and Definitions -March-2018
11. Guidance on good manufacturing practice and good distribution practice: Questions and answers (MHRA)
12. EMA EudraLex Vol. 4 (Chapter 4: Documentation)

13. Department of Health and Aged Care Therapeutic Goods Administration (TGA) : Data Management and Data Integrity : Australian Government – 2017
14. Data Integrity and Compliance With CGMP Guidance for Industry: U.S. Department of Health and Human Services Food and Drug Administration – 2016
15. WHO guidance on DATA INTEGRITY (WHO Technical Report Series, No. 1033, 2021) Annex 4
16. Charoo NA, Khan MA, Rahman Z. Data integrity issues in pharmaceutical industry: Common observations, challenges and mitigations strategies. International Journal of Pharmaceutics. 2023 Jan 25;631:122503.
17. EMA EudraLex Vol. 4 (Annex 11: Computerized System)
18. Rattan AK. Data integrity: history, issues, and remediation of issues. PDA Journal of Pharmaceutical Science and Technology. 2018 Mar 1;72(2):105-16.
19. Brooks JL, Albon KI, Davis D. A risk-based approach to Data Integrity. Pharmaceutical Technology. 2015 Jul 2;39(7):46-50.
20. Dharnish.R , Jeyaprakash M.R. An Approach Of Data Integrity In Pharmaceutical Industries, Eur. Chem. Bull. 2023,12(1),30-36
21. Bhadrashette MS. Overview of Data Integrity issues in the Pharmaceutical industry. International Journal of Pharmaceutical Sciences Review and Research. 2018 Jun ;14:95-101.
22. ICH Q10 Pharmaceutical Quality System
23. PIC/S guideline on Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments -2021.

HOW TO CITE: Sanket Gade*, Prerana Jadhav, Pradyumana Ige, Pratiksha Bornare, Data Integrity Compliance, Importance, Consequences And Strategy To Overcome Data Integrity In The Pharmaceutical Industry, Int. J. of Pharm. Sci., 2024, Vol 2, Issue 6, 1122-1132. https://doi.org/10.5281/zenodo.12513412