WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Review: An Illustration of Data Integrity

Snehal Chandrashekhar Jale*, Nidhee Vinayak Tendulkar, Siddhi Maruti Chavan, Sayali Venkat Biradar, Jayshree Kishor Sonawane, Ishwari Prakash Narkar, Aayesha Dashrath Barge, Vaishali Jadhav, Dr Ashish Jain.

Department of Quality Assurance, Shri D. D. Vispute College of Pharmacy and Research Center, Devad-Vichumbe, Panvel 410221, Maharashtra, India.
E-mail address: snehaljale1211@gmail.com

ABSTRACT:

Data integrity is crucial for enforcing regulations and serves as the main basis for 21 CFR Part 11, which was issued in the US. FDA regulators wanted to ensure that the pharmaceutical sector gathered correct data throughout the lifecycle of the medicine. Although this data becomes one of the most precious assets of any firm, it is of little use if it lacks integrity. The likelihood of an organisation's stability and performance is increased by accuracy and original data. The degree to which all data are comprehensive, consistent, and accurate throughout the life cycle of the data is known as data integrity. It also involves good documentation practises, which help to guard against data being changed, duplicated, or moved. In terms of data integrity, data refers to all original records, including source data and metadata, whether they are kept on paper or electronically. ALCOA was suggested by various regulatory organisations, including the USFDA, Health Canada, and EMEA, to ensure the integrity of the data (Attributable, Legible, Contemporaneous, Original and Accurate).

KEYWORDS: Data integrity, ALCOA, Regulation, Data

INTRODUCTION:

Data integrity must be created, implemented, and used in every system that stores, processes, or retrieves data. It is the upkeep and guarantee of data consistency and correctness over its entire existence. The term has several uses and, depending on the context, can mean quite a few distinct things, even though it falls within the general heading of computing. [1]Data integrity requires data validation, which is sometimes used as a stand-in for data quality. Data corruption is the reverse of data integrity. The main objective of any data integrity approach is to make sure that data is captured exactly as intended (such as a database correctly rejecting mutually exclusive possibilities). [2]Additionally, make sure that when the data is accessed later, it is the same as it was when it was first recorded. In a nutshell, data integrity seeks to prevent unintentional changes to data. Data integrity should not be confused with data security, which is the discipline of keeping data safe from unauthorised parties.[3]

An observation, the results, or other facts and information can be manually recorded on paper and presented as data, or they can be electronically recorded using equipment and equipment connected to a computer system. It is also possible to utilise a mix of manual and electronic solutions.[4]The Latin adjective integer, which means whole or complete, gave rise to the English term integrity. Integrity is the quality of having upstanding moral beliefs and the ability to be honest. Holding oneself to consistent moral and ethical norms is typically a personal decision. Many people define integrity in ethics as being sincere, accurate, and honest in one's behaviour.[5]

The more morally successful a firm is likely to become, the more data integrity it has. The quality of records and evidence is compromised by weak data integrity procedures and vulnerabilities, which may eventually affect the quality of pharmaceuticals. All components of the Quality Management System must adhere to the principles of data integrity, and both electronic and paper-based systems may generate data. The manufacturer or distributor that is being inspected is accountable for effective data management and integrity practises. In order to ensure that data integrity is maintained, they have a complete responsibility and an obligation to evaluate their data management systems for any weaknesses and take action to establish and implement appropriate data governance processes.

THE VALUE OF DATA INTEGRITY:

- First and foremost, it ensures that your business is not vulnerable to data leaks or losses. To ensure the security of your internal data, you must first ensure that it is handled correctly. By implementing error checking and validation processes, sensitive data is correctly classified and stored, lowering risks.
- Data integrity ensures that your business has accurate, current, and trustworthy information recorded. Making business decisions based on inaccurate or biassed information may end up costing your company money, time, and effort. All successful data-driven decisions must be founded on reliable, consistent data. The negative effects of a corrupted or flawed database at your firm could continue for a very long time.
- Data integrity is crucial for your company's reputation in addition to enabling you to make the right business decisions. For instance, a lot of businesses gather PII (personally identifiable information) about their clients, such as complete name, address, SSN, and banking details. Let's say this data set contains an error. Your clients' personal information may be stolen or exposed due to either an innocent typing error or a hacking attempt, ending up in the wrong hands and being used maliciously.
- Lastly, businesses may save less sensitive client data, like credit card numbers, which is still incredibly important. For instance, any flaws in your data sets could result in loss of business if you improperly categorise or target your consumers if you track your customers' behaviours on your company's website or ask them for feedback.
- As a result, data integrity is significant from more than just a legal standpoint. It has far-reaching effects, including bettering your relationship with customers, upholding a positive brand image, and assisting in keeping your business resistant to outside attacks.

PRINCIPLES OF DATA INTEGRITY:

Systems shall be established and implemented to guarantee that all information gathered, processed, and recorded complies with the principles of the guidelines. Data integrity operates according to ALCOA-based principles. ALCOA is used in the pharmaceutical industry to make sure that the quality of the evidence is upheld in accordance with regulatory requirements. The use of ALCOA is advised by many regulatory agencies, including the FDA, Health Canada, and the EMEA, in order to maintain proper documentation procedures for medications. According to US FDA guidelines, ALCOA stands for Attributable, Legible, Contemporaneous, Original, and Accurate. These straightforward guidelines should be incorporated into your data lifecycle, GDP, and data integrity activities because they relate to data, whether it is paper-based or digitally. It aids in the formulation of plans for maintaining the reliability of the data in both manufacturing and research. The following has been discussed regarding ALCOA's role in pharmaceuticals:[6],[7]

- ***Attributable:*** The first term of ALCOA, all data should be attributed to the individual who generates it. This includes the individual's information as well as a timestamp of when the action was performed; this step can be completed physically or electronically. The eligible record holder's identity must be documented. For paper records, this is usually done by personal signature, and dating records with their signatures. Because the file you sign could be a legal document, the meaning of your signature must be clear. The signature must be independent of a specific person, and the tendency to sign another's name or initials is fraudulent and must be taken seriously.[8],[9]

All data recorded must be permanent and easily legible. Permanent means that the information cannot be changed or altered; the best practise is to use non-erasable ink. Recordings that cannot be read or understood are worthless and may not exist at all. All records must be created in accordance with the grammatical assemblies, which must be flawless. It is best to avoid buzzwords, groups, and abusers because they are likely to change over time and are frequently not understood in a specific location.[8],[9]

- ***Contemporaneous:*** Since all information should always be captured at the same moment an action is taken or a task is being completed, it is an exceptionally important component of the ALCOA process. Retrospective data recording undermines the reliability of the data and should be avoided. To be contemporaneous, make sure that all clocks are correctly synced during testing to remove any errors.[8],[9]
- ***Original:*** The original formats of all the data, such as protocols, databases, or notebooks should be used. Do not enter information about one entity into the official test documents. All documentation must be original, and all data must be written directly on the document. By doing this, it is less likely that transcription problems will be found when information is turned into documents. When information is printed by an instrument, that print serves as the original recording and must be accompanied by a signature and date.[8],[9]
- ***Accurate:*** The documentation must represent what actually occurred. The use of blanks or the manipulation of liquids is forbidden, and any modification must be carried out without erasing or disguising the original data. A written justification must be included with each alteration to the file, and it must be signed by the person making the change and date-stamped to show when it happened. Keep in mind that records may still be needed even after you leave the company.[8],[9]

WORLD REGULATORY RECOMMENDATIONS FOR DATA INTEGRITY:

- ***USFDA: 21-CFR:-*** The federal register is a publication used by the executive departments and agencies of the federal government to establish broad and permanent rules. which are codified in 21-CFR (Code of Federal Regulation). The Food and Drug Administration's rules are contained in Title 21 of the CFR. Every year, on or around April 1st, the CFR is amended once for each book or volume.[10],[11],[12]
- ***MHRA:-*** The MHRA's guideline on GMP data integrity requirements for the pharmaceutical sector is designed to enhance the EU's current GMP standards for active ingredients and dosage forms. The pharmaceutical quality system, which guarantees that medications are of the requisite quality, depends critically on data integrity.[10],[13],[14]
- ***TGA:-*** The Therapeutic Goods Administration (TGA), an Australian regulatory organisation, sets the standard for data integrity as a deficit. a flaw in a procedure or process that has resulted in or might lead to a considerable risk of creating a user-harmful product. Additionally, it happens when it is discovered that the manufacturer has deceived, misrepresented, or falsified goods or data.[10],[11]
- ***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 recognises the pattern of rising data integrity breaches. Records-keeping procedures that adhere to cGMPs avoid data loss or obscuration.[15],[16] 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 practise to assure that such drug meets the requirement of the act as to safety and has the identity and stringent quality controls."[10],[17],[18]
- ***Good Documentation Practices:-*** The methods that together and individually guarantee that documentation, whether paper or electronic, is accountable, readable, traceable, permanent, contemporaneously documented, original, and correct are referred to as good practises in the context of these recommendations.[10]
- ***WHO:-*** The methods that together and individually guarantee that documentation, whether paper or electronic, is accountable, readable, traceable, permanent, contemporaneously documented, original, and correct are referred to as good practises in the context of these recommendations. The reliability and correctness of the data manufacturers provide to national regulatory bodies is a crucial phase in the process, which involves many players and activities. To guarantee the calibre of research supplying requests for medications to be placed on the market, that data must be extensive, thorough, exact, and truthful. It also must comply with a number of standards, namely: good manufacturing practises (GMP), good clinical practise (GCP) and good laboratory practises (GLP). [10],[1],[19]
- ***EMA:-*** To safeguard the integrity of data generated throughout the testing, production, packaging, distribution, and monitoring of medicines, the European Medicines Agency (EMA) has published new Good Manufacturing Practice (GMP) guidelines. These statistics are used by regulators to assess the efficacy, safety, and quality of medications as well as to track the benefit-risk profile of such medications during their entire life cycle. Effective data record management enables regulatory agencies and pharmaceutical producers to make informed decisions by ensuring that the data produced are correct and consistent.[10],[20],[21]
- ***Data integrity and GDPR Compliance:-*** For data protection regulations like the GDPR to be followed, data integrity is essential. Companies may be subject to significant fines for failing to comply with these requirements. They might occasionally be utilised in addition to these high costs. Repeated compliance violations may potentially result in a company's closure.[10]

The GDPR (General Data Protection Regulation) outlines six data protection principles that summarise its many requirements.[22]

1. Integrity, fairness, and lawfulness

2. Purpose restraint

3. Data reduction

4. Accuracy

5. A storage space issue

6. Act with integrity and delicacy

7. Accountability

ADVANTAGES OF DATA INTEGRITY:[3,23]

- ***Control of data redundancy:-*** By integrating files, the database system strives to get rid of the extremes. The database system does not totally eliminate redundancy, but it does manage the level of redundancy in the database.
- ***Data consistency:-*** The database method eliminates or manages redundancy to lower the risk of consistency. It guarantees the continuous upkeep of all data copies.
- ***More information from the same amount of data:-*** It is possible to gain more information for the same data thanks to the integration of the data utilised in the database system.
- ***Sharing of data:-*** All logged-in users have access to the database, which is a component of the entire business.
- ***Improved data integrity:-*** The validity and consistency of the data that is saved are guaranteed by the database's integrity. When describing integrity, limitations are frequently used, such as the consistency rule that forbids violating a database.
- ***Improved maintenance:-*** Data freedom is granted by the database system. The application software will be impacted by changes to the database's data structure, making it easier to maintain the database application.
- ***Increased concurrency:-*** The database can efficiently control interactive data access. This ensures that there will be no user meddling, protecting against the loss of integrity or information.

DISADVANTAGES OF DATA INTEGRITY: [3,23]

- ***Complexity:-*** System software for database administration is quite sophisticated. Its usefulness must be understood by all stakeholders, who must also make the most of it. As a result, administrators, designers, and users all require training.
- ***Size:-*** Database management systems require a significant quantity of main memory as well as a huge amount of disc space to function properly.
- ***Performance:-*** Instead of providing a few specialised applications, the database technique provides numerous applications, however some may not function as efficiently as before.
- ***Higher impact of a failure:-*** The vulnerability of the system is increased by centralising the database strategy. A component failure can substantially impair customer service when you must reply to all users and depend on the application database's availability.
- ***Cost of conversion:-*** The firm will have to pay extra expenses for the purchase of equipment and training fees when transitioning from a file system to a database system.

TYPES OF DATA INTEGRITY:

Data integrity can be classified as logical and physical integrity. Both are a combination of steps and approaches applied to relational and hierarchical databases to implement data integrity.

7.1 Physical integrity:- Data correctness and completeness are preserved by physical integration throughout archiving and retrieval. Natural calamities, power failures, or database processes being interfered with by hackers all endanger physical integrity. It is hard for data controllers, system programmers, and internal auditors to collect reliable data because of human mistakes, storage erosion, and many other problems[3,23].

7.2 Logical integrity:- The data does not change due to the logical integrity used differently in the relational database. Logical integrity data protects against human error and hackers, but in a different way from physical integrity. There are four types of logical integrity[23,24].

7.2.1 Entity integrity:- Entity integrity is dependent on the creation of unique values that identify the primary key or data components in order to ensure that a data entry is not listed more than once and that the fields in a table are not empty. It is a feature of relational systems in which data is stored in arrays that may be connected and utilised in many ways.

7.2.2 Referential integrity:- A collection of methods that ensure that data is saved and utilised consistently is referred to as referential integrity. The rules incorporated into the foreign key use database structure ensure that only acceptable modifications, additions, or deletions are discovered. Rules may include deleting duplicate data entries, guaranteeing data correctness, and terminating access to unauthorised data.[23]

7.2.3 Domain integrity:- Domain integrity refers to a collection of operations that assure the correctness of all data in the domain. A domain in this sense is a collection of permitted values that can be included in a column. Constraints and other measures that limit the nature, kind, and scope of the data entered may be included.[3,23]

7.2.4 User-defined integrity:- User-defined integrity refers to rules and limits that the user has developed to achieve their individual reuirements. The integrity of the entity, context, and domain is not always sufficient to secure data. Specific business concepts must also be considered and applied in data integrity projects.[23,25]

DATA INTEGRITY RISK:

A variety of circumstances can jeopardize the integrity of data contained in a database. Here are a few examples:

- ***Human error:-*** When a person inputs inaccurate information, duplicates or deletes data, fails to follow the right procedure, or makes mistakes while executing the process for information security objectives, data integrity is jeopardised.
- ***Transfer errors:-*** When data cannot be effectively transferred from one point in a database to another, a transfer error has occurred. Transfer errors occur when a piece of data exists in the destination table but not in the source table of a relational database.
- ***Bugs and viruses:-*** Spyware, malware, and viruses are software components that can invade a computer and manipulate, erase, or steal data.
- ***Compromised hardware:-*** Sudden and unexpected computer or server breakdowns, as well as issues with how a computer or other system runs, are instances of serious failures that might indicate that the hardware is faulty. Compromised hardware may produce data inaccurately or incompletely, restrict or prevent data access, or make information difficult to utilise[26,27,28].

VARIOUS METHODS TO MINIMIZE DATA INTEGRITY RISK:-

- ***Add redundancy:-*** Data can be stored simultaneously in two or more locations and then checked for discrepancies. This method necessitates more resources, but it significantly minimises the likelihood that an improper update would go undetected.
- ***Data encryption:-*** Encryption is another useful option, particularly for controlling communication between devices or over the internet. Decryption must be applied to stolen data before it can be utilised by anyone else, giving producers enough time to detect an attack and respond appropriately. Data uniqueness is also important for data integrity, thus keeping track of user IDs and passwords can assist prevent illegal access.
- ***Data privacy:-*** Reduce the risk of data integrity by keeping data private and secret. Data access can be limited to certain users, with rights granted per user.
- ***Data loss minimization:-*** This can be accomplished by preventing data from being shared across numerous sources. Keeping the data in one location decreases the risk of malicious or unintentional intervention. Data backups are also essential in the event of hardware or software failure. In the event of an attack or incursion, organisations must build fail-safe measures; firewalls and data loss prevention (DLP) solutions are required to prevent data breach after an attacker has access.
- ***Consistent update of data:-*** A company's overall security depends on thorough data integrity management. When necessary, data should be updated to reflect the state of the world. Before being implemented, all data modifications must undergo thorough testing. The prevention of further issues on top of the first problem is strengthened by error detection. To check for these problems, which may impact the key data points, schedule data reviews.
- ***Employee training :-*** Assure your staff members understand how to work with data to reduce errors and preserve accuracy. Additionally, training keeps employees committed to overall quality, which is great for company
- ***Protect Your Documents :-*** You may encrypt the records by placing restrictions on the files. The actions that may be conducted on documents can be restricted by vendors like Adobe and Microsoft, ranging from read-only access to making just certain modifications. Additionally, you may password-protect your PDFs and papers.
- ***Introduce Access Controls:-*** Personal can seriously harm data if they have bad intentions and no formal access. One of the most common methods of access control is the implementation of a minimal privilege model, in which only people who actually require access to the data are granted access.

- ***Implement Backup and Recovery Procedures:-*** To maintain data integrity and prevent important data loss, regular data backups are essential. In the event of a breach, data that is routinely backed up can be recovered in its original state.
- ***Leverage Audit Trails:-*** The name, date, and time of data additions, revisions, and deletions are tracked via a time-stamped, computer-generated audit trail. Audit trails offer the breadcrumbs that point to the problem source in the event that data is compromised.
- ***Passwords:-*** Use passwords to prevent unauthorized access to all storage devices where data is stored. Do not place the passwords on your computer or post-it notes.
- ***Ensure Security:-*** File encryption is one cyber-security solution that can lessen the loss of data integrity. To prevent harmful assaults and files from reaching your computer and modifying your data, anti-malware software is also advised. [29,30,31,32]

DATA INTEGRITY ISSUES:

- ***User privilege's:-*** Users have access to improper programme rights such method modification and integration because the system setup for the software does not properly identify or segregate user levels.
- ***Common passwords:-*** The A in ALCOA is unclear when analysts share passwords since it is impossible to tell who makes modifications to documents.
- ***Computer system control:-*** The file may not be original, accurate, or complete because laboratories have not implemented proper data control measures that would prevent unauthorised access to edit, destroy, or not save electronic information.
- ***Audit Trial capture:-*** FDA advises reviewing audit trails documenting modifications to crucial data with each record and prior to the record's final approval.
- ***Warning Letters, Statement of Non-Compliance and Consent Decrees:-*** After detecting data integrity problems, the regulatory authorities delivered several warning letters, notices of non-compliance, and consent decrees to pharmaceutical production plants. If the regulatory bodies respond in this way, it will be difficult for the firm to obtain authorisation for the sale of new medicinal products and the regulatory bodies may lose faith in the company. Additionally, a circumstance might arise where the business has to reduce manufacturing or retain the items on-site. This will result in a shortage of pharmaceutical items and a decline in customer confidence.
- ***Import Alert, Product Recalls and Seizure of Products :-*** Drug items that lack data integrity are referred to as adulterated drug products. The US FDA will impose restrictions on their ability to sell these contaminated drug items on the US market. Import warnings let the public and FDA field personnel know that the agency has enough proof to demand that products that seem to be breaking FDA laws and regulations be held without a physical examination. These infractions could relate to the goods, the distributor, the shipper, or other specifics. The best approach to safeguard consumers against faulty or potentially hazardous FDA-regulated products is to remark that they should be taken off the market or fixed.
- ***Loss of Regulatory Trust :-*** When problems with data integrity occur, regulatory confidence is likely to be damaged. As a result, the factory will undergo more regular inspections in an effort to find additional proof to back up allegations, which will make it more difficult for businesses to obtain certification for routine faults.
- ***Need to Appoint Third Party Consultants for Data Integrity:-*** If the US FDA has issued a warning letter to the pharmaceutical facility, the FDA advises employing a third-party specialist who is adept at spotting data integrity issues to help the business with this evaluation and to help with the business' overall compliance with cGMP. Typically, hiring a consultant to help you uncover data integrity concerns and satisfy regulatory requirements takes time and money.
- ***Debarment and Imprisonment (for Individuals involved in data integrity issue):-*** A case study has a thorough understanding of how people involved in data integrity concerns can be impacted. At the now-defunct generic medicine company in New Jersey, Able Laboratories, a former vice president of the Quality Control Department and three supervising chemists pleaded guilty to a fraud including the systematic fabrication and manipulation of their drug test findings. Due to this, all 500 workers of Able Laboratories, Inc., had lost their jobs.

CAUSES OF DATA INTEGRITY PROBLEMS:

The idea that data integrity issues only result from deliberate fraud is a widespread one. Data integrity problems can result from a single component, deliberate fraud, but there are many additional variables that are just as likely to be at fault. Several factors are listed below:-

- ***Shortage of Manpower:-*** Inaccurate and inadequate paperwork may result from a staffing shortage and excessive work demands.
- ***Always follow a written procedure:-*** Many 483 and warning letters lack the degree of detail necessary to ensure consistent performance. Variability in output results from variation in performance.
- ***Quantity Vs Quality:-*** In order to reach production goals or delivery deadlines, employees could be compelled to compromise on acceptable quality levels. Every piece of information must always be included into the official record. All data created, even data that is invalidated due to known mistakes, must be correctly collected and documented in accordance with stated protocols. Without it, we are missing a comprehensive record of our decisions and actions for each batch of manufactured and tested goods.
- ***Lack of Awareness:-*** Employees are frequently not or not enough trained to grasp GMPs. As a result, workers view tasks as chores rather than seeing how important they are in the context of GMP.
- ***Effectiveness of Training:-*** Employees noted that despite the company's hiring of the top international trainers, language and accent obstacles prohibited the staff from comprehending the material, rendering the training ineffective.[33],[34],[35]

IMPORTANCE OF DATA INTEGRITY IN PHARMACEUTICAL INDUSTRY:

- Digital platforms and technological improvements are transforming how corporate operations are conducted in the global business world. To increase the productivity and efficiency of company, the big data explosion has assured that business and the digital platform have become synonymous. Business executives should constantly reflect on the economic and commercial potential of big data as well as its larger relevance for social and technical advancements. This means that in order for the pharmaceutical sector as a whole to profit from these technologies, new frameworks of action must be included into daily business operations.[36],[37]
- Data integrity (DI) ensures that the information produced during company operations and the production of pharmaceuticals is correct, complete, and trustworthy. Only when data is trustworthy can company owners make the decisions that are best for their companies, raise the calibre of their output, and boost their overall performance. The definition of data integrity, its significance for business owners, and the connection between data governance and industry best practises are all covered in this viewpoint. Last but not least, it provides concrete measures for incorporating big data and data integrity into current operations and explains why the pharmaceutical sector will place a high value on the capacity to create value by extracting informational value from digital waste. Only data generated during the production processes may be used by businesses to demonstrate the quality of their goods. [38],[26]
- In other words, the ability of businesses to guarantee the quality of their products depends on the data quality. The only evidence that your production process complies with quality requirements is found in data records. Data governance ensures the formal administration of records and data across the regulated firm. The people, procedures, and technology needed for efficient data management that finally yields high-quality products are all included in data governance.[38],[39],[40]

CONCLUSION:

In the pharmaceutical sector, data integrity is critical to maintaining the quality of a final product since malpractices might allow substandard products to reach patients, hence an established system is required to assure data integrity, data traceability, and reliability. On quality grounds, data integrity is a critical component of a Quality System. Quality data serves as the foundation for the company's trust in using proper data to function in line with regulatory obligations. Data integrity is vital to regulators for a variety of reasons, including patient safety, process efficiency, and product quality. The data's quality and dependability serve as a foundation for regulators' assessments of the firm. Detect bad data integrity procedures caused by a lack of quality system efficacy.

The Quality Risk Management (QRM) strategy may avoid, detect, and mitigate possible risks in situations where data is collected and utilised to make manufacturing and quality choices, ensuring that it is trustworthy and dependable. Data integrity ensures that electronic data remains intact. Reports are only as good as the facts they are based on. Data integrity can also apply to information that is not stored in a computer.

Maintaining data integrity, whether digital or textual, is essential for making sound business decisions. As data becomes a commodity, it must be kept in mind to ensure consistency with little effort. After all, the more data you have available to you, the more your firm can expand. Any regulated lab's reputation is highly influenced by the quality of data provided. Consider that inspections and audits can only do a review; discovering one incident of fabrication raises the issue of how many more instances of noncompliance exist. As a result, guaranteeing data integrity is critical for every organization's analytical scientists, managers, and quality assurance personnel, since the consequences of getting it wrong are extremely costly, and it will take a long time to rebuild regulatory faith.

DECLARATION:

Ethics approval and consent to participate- The writers of this article did not engage in any animal related activities.

Consent for publication- As a corresponding author, I give my consent for publication of my review paper to your reputed journel.

Availability of data and material- Open Access.

Competing interest- The authors declare that they have no conflict of interest.

Funding- There is no funding source.

Authors contribution- All the co- authors have contributed for drafting and compilation of review paper.

Acknowledgement: I want to express my gratitude to all of the co-authors for their assistance with the article's preparation. I would specially like to thank Prof. Vaishali Jadhav for all of her assistance and direction during the review process. Also I would liketo show my gratitude to Principal Dr. Ashish Jain and Management of D.D Vispute College of Pharmacy and Management of D.D Vispute College of Pharmacy and Reserch Center.

REFERENCES

(1) Qas19-819-Rev1-Guideline-on-Data-Integrity.Pdf. https://www.who.int/docs/default-source/medicines/norms-and-standards/current-projects/qas19-819-rev1-guideline-on-data-integrity.pdf (accessed 2023-04-19).

(2) WHO-Guideline-on-Data-Integrity-Draft.Pdf. https://rx-360.org/wp-content/uploads/2018/08/WHO-Guideline-on-Data-Integrity-Draft.pdf (accessed 2023-04-19).

(3) Nikam, N. R.; Patil, P. R.; Vakhariya, M. R. R.; Mohite, D. S. K. DATA INTEGRITY: AN OVERVIEW. 2020, 11.

(4) Boritz, J. E. IS Practitioners' Views on Core Concepts of Information Integrity. Int. J. Account. Inf. Syst. 2005, 6 (4), 260–279. https://doi.org/10.1016/j.accinf.2005.07.001.

(5) What is Data Integrity? Definition, Types & Tips. https://www.digitalguardian.com/blog/what-data-integrity-data-protection-101 (accessed 2023-04-19).

(6) Ojeda, S. Understanding ALCOA+ & Data Integrity for Pharma Companies | AssurX. Quality Management Software + Regulatory Compliance | QMS Software | AssurX. https://www.assurx.com/understanding-alcoa-principles-and-data-integrity-for-pharma/ (accessed 2023-04-19).

(7) ALCOA+ Principles for Data Integrity in Life Sciences. Eurotherm Limited. https://www.eurotherm.com/in/life-sciences-cpg/data-integrity-life-sciences/alcoa/ (accessed 2023-04-19).

(8) Principles of Data Integrity : Pharmaguideline. https://www.pharmaguideline.com/2018/04/principles-of-data-integrity.html (accessed 2023-04-19).

(9) Koehler, S. Principles of Data Integrity. EMMA International. https://emmainternational.com/principles-of-data-integrity/ (accessed 2023-04-19).

(10) Ahmad, S.; Kumar, A.; Hafeez, A. Importance of Data Integrity & Its Regulation in Pharmaceutical Industry; preprint; Preprints, 2022. https://doi.org/10.22541/au.166265947.70683270/v1.

(11) Hart, S. Data Integrity: TGA Expectations.

(12) Rachel, P. K.; Gupta, N. V. Data Integrity – Regulations and Current Scenario. No. 05.

(13) Data_integrity_definitions_and_guidance_v2_Withdrawn.Pdf. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/697053/Data_integrity_definitions_and_guidance_v2_Withdrawn.pdf (accessed 2023-04-19).

(14) New MHRA "GxP Data Integrity Guidance and Definitions" published - ECA Academy. https://www.gmp-compliance.org/gmp-news/new-mhra-gxp-data-integrity-guidance-and-definitions-published (accessed 2023-04-19).

(15) McLaughlin, E. Guidance for Industry. Quest. Answ. 2018.

(16) Ensuring CGMP Standards for Data Integrity. https://www.pharmtech.com/view/ensuring-cgmp-standards-for-data-integrity (accessed 2023-04-19).

(17) Data Integrity and Compliance With CGMP | PharmaTutor. https://www.pharmatutor.org/articles/data-integrity-and-compliance-with-cgmp (accessed 2023-04-19).

(18) Purdie, F. P. Data Integrity and Compliance With CGMP Guidance for Industry.

(19) Trs1033-Annex4-Guideline-on-Data-Integrity.Pdf. https://cdn.who.int/media/docs/default-source/medicines/norms-and-standards/guidelines/inspections/trs1033-annex4-guideline-on-data-integrity.pdf?sfvrsn=6218a4e6_4&download=true (accessed 2023-04-19).

(20) EMA-Presentation-at-Mumbai-Conference-Feb-2017.Pdf. https://rx-360.org/wp-content/uploads/2018/08/EMA-Presentation-at-Mumbai-Conference-Feb-2017.pdf (accessed 2023-04-19).

(21) EMA recommendation paper: Safety, data integrity key to decentralized trial conduct. https://www.raps.org/news-and-articles/news-articles/2022/12/ema-recommendation-paper-safety-data-integrity-key (accessed 2023-04-19).

(22) Irwin, L. The GDPR: Understanding the 6 data protection principles. IT Governance Blog En. https://www.itgovernance.eu/blog/en/the-gdpr-understanding-the-6-data-protection-principles (accessed 2023-04-19).

(23) AN APPROACH OF DATA INTEGRITY IN PHARMACEUTICAL INDUSTRIES. Eur. Chem. Bull. 2023, 12 (1). https://doi.org/10.31838/ecb/2023.12.1.002.

(24) Trs966-Annex05-Who-Record-Management-Practices.Pdf. https://www.who.int/docs/default-source/medicines/norms-and-standards/guidelines/regulatory-standards/trs966-annex05-who-record-management-practices.pdf (accessed 2023-04-20).

(25) What Is Data Integrity? How It Makes Your Business Trustworthy. G2. https://www.g2.com/articles/data-integrity (accessed 2023-04-20).

(26) What is Data Integrity and Why is it Important? | Egnyte. https://www.egnyte.com/guides/governance/data-integrity (accessed 2023-04-19).

(27) IT Data Integrity Risk - Open Risk Manual. https://www.openriskmanual.org/wiki/IT_Data_Integrity_Risk (accessed 2023-04-20).

(28) Spilka, S. Data Integrity: Relevancy, Risks and the Appropriate Use. ANEXIA Blog. https://anexia.com/blog/en/data-integrity-relevancy-risks-and-the-appropriate-use/ (accessed 2023-04-20).

(29) The Importance of Data Integrity for Your Business. Commercient. https://www.commercient.com/the-importance-of-data-integrity-for-your-business/ (accessed 2023-04-20).

(30) Gonzalez, J. M. 7 Methods to Reduce Data Integrity Risks. Webhead: We do IT for You. https://webheadtech.com/blog/reducing-data-integrity-risks/ (accessed 2023-04-20).

(31) Steps to Minimize the Data Integrity Risk : Pharmaguideline. https://www.pharmaguideline.com/2019/04/how-data-integrity-risk-can-be-minimized.html (accessed 2023-04-20).

(32) 12 Ways To Reduce Data Integrity Risk. https://www.pharmaceuticalonline.com/doc/ways-to-reduce-data-integrity-risk-0001 (accessed 2023-04-20).

(33) Data Integrity Issues: Causes and Solutions. https://www.pda.org/pda-europe/news-archive/full-story/2015/03/30/data-integrity-issues-causes-and-solutions (accessed 2023-04-20).

(34) Oqotech. Causes of identified data integrity problems. Oqotech. https://www.oqotech.com/en/blog/data-integrity-en/causes-of-data-integrity-issues-identified-by-regulatory-agencies/ (accessed 2023-04-20).

(35) What causes data integrity issues?. Quora. https://www.quora.com/What-causes-data-integrity-issues (accessed 2023-04-20).

(36) Jean-François Tremblay. Indian Drug Firms Struggle with Quality Issues. CEN Glob. Enterp. 2016, 94 (16), 23–25. https://doi.org/10.1021/cen-09416-bus2.

(37) Why Is Data Integrity Important In Pharma? - Pharmabeej. https://pharmabeej.com/why-is-data-integrity-important/ (accessed 2023-04-20).

(38) Steinwandter, V.; Herwig, C. Provable Data Integrity in the Pharmaceutical Industry Based on Version Control Systems and the Blockchain. PDA J. Pharm. Sci. Technol. 2019, 73 (4), 373–390. https://doi.org/10.5731/pdajpst.2018.009407.

(39) Kimachia, K. An overview of data integrity and its importance. TechRepublic. https://www.techrepublic.com/article/what-is-data-integrity/ (accessed 2023-04-19).

(40) Data-Integrity-in-the-Pharmaceutical-Industry.Pdf. https://qbd.eu/wp-content/uploads/Data-Integrity-in-the-pharmaceutical-industry.pdf (accessed 2023-04-20).