https://doi.org/10.48047/AFJBS.6.12.2024.4448-4458

AFJBS

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

An Overview Of Data Integrity in Pharmaceutical Industry

Ashish S. Jain[1*], Sayali.S. Shelke[1], Vaishali Jadhav[1]Sunita Gagare[1], Aditi Vitthal Sawant[1], Divya kalu shirsath[1],EmadKhan[1],Sanid Hadal[1].

1. Shri D Dvispute college of pharmacy and Research Center,Panvel.

Corresponding Author: drashishjain80@gmail.com , 1. Shri D Dvispute college of pharmacy and Research Center, Panvel.

Article History
Volume 6, Issue 12, 2024
Received: 15 June 2024
Accepted: 05 July 2024
doi:
10.48047/AFJBS.6.12.2024.4448-4458

Abstract :
Data integrity is the cornerstone of 21 CFR Part 11, which was created in the United States, and is essential for implementing rules. FDA officials sought to guarantee that the pharmaceutical industry collected accurate data across the course of a medication's lifecycle. Even while this data grows to be one of the most valuable resources for any company, if it is not reliable, it is not very useful. Accuracy and original data boost the likelihood of stability and performance in an organization. Data integrity is the extent to which all data are complete, accurate, and consistent during the course of the data's life cycle. In order to prevent data from being altered, copied, or transferred, it also entails using appropriate documentation practices. When discussing data integrity, "data" refers to any original records—whether stored electronically or on paper—including source data and metadata. Many regulatory agencies, such as the USFDA, Health Canada, and EMEA, recommended using ALCOA (Attributable, Legible, Contemporaneous, Original, and Accurate) to guarantee data integrity.

KEYWORDS: Data integrity, FDA, metadata, 21 CFR, ALCOA

Introduction:

Any system that stores, processes, or retrieves data needs to be designed, put into practice, and use data integrity. It is the maintenance and assurance of data accuracy and consistency across the course of its existence. Even though it falls under the broad category of computers, the term has multiple applications and can indicate quite a few different things depending on the context[1]. Data validation, which is occasionally used as a stand-in for data quality, is necessary for data integrity. The opposite of data integrity is data corruption. Ensuring that data is captured exactly as intended is the primary goal of any data integrity strategy (e.g., a database rejecting mutually exclusive alternatives appropriately)[2.]Also, confirm that the data remains unchanged from the time it was first captured for subsequent access. To put it briefly, data integrity aims to stop inadvertent modifications to data. Data security is the discipline of protecting data from unauthorized parties; it should not be confused with data integrity[3]. Data can be presented electronically utilizing equipment and equipment connected to a computerized system, or manually documenting an observation, results, or other data and information on paper. It is also possible to use a mix of electronic and manual systems[4]. The same restrictions required for media like photography or 402 scanning are also copied by DI together with other data sets (such pictures, movies, 400 DVDs, images, and chromatography plates). An explanation for selecting such an approach ought to be provided. Data integrity is a vital component of the design, implementation, and operation of any system that stores, processes, or retrieves data. It is a guarantee of the consistency and accuracy of data throughout its life[5]. Under the general heading of "computer," the term can refer to many things depending on the particular situation. It serves as a stand-in word for data quality[6], and data integrity requires data validation[7]. Data corruption is opposed by data integrity[8].

Table 1: Overview of Data Integrity Guidelines from Various Regulatory Agencies

Regulatory Agency	Guideline Title	Year of Publication	Key Focus Areas
World Health Organization (WHO)	Guidance on Good Data and Record Management Practices	2016	Data management, record integrity, audit trails
FDA	Data Integrity and Compliance With CGMP	2018	Data accuracy, prevention of data manipulation
EMA	GxP Data Integrity Guidance and Definitions	2022	Definitions, data lifecycle management, controls

Principle:

Regulators have discovered in recent years that a large number of firms are not upholding the necessary levels of data integrity within computerized systems. A WHO committee has agreed to develop new guidelines aimed at enhancing and consolidating current data integrity principles from guidance papers and current good practices, as a result of a growing amount of observations concerning data integrity made during inspections [9]

Definition of ALCOA:

Attributable: Every bit of information that is entered into the record needs to be able to be linked back to the person who entered it and the time it was taken.

Legible: All information, including metadata, needs to be persistent, readable, traceable, and intelligible to anybody looking over the record.

Contemporaneous: Information that is briefly recorded in the record at the time it is created.

Original: Data from the source, or the original recording medium on which the data was stored. The initial data entry as well as any additional data entries needed to completely describe the project's scope should be included in the original data record.

Accurate: A risk-based framework should be used to develop controls to ensure the accuracy of data, which should consist of true, accurate, complete, valid, and dependable information [9]

Fulfilling ALCOA Data Requirements :

Attributable: Necessitates the usage of electronic signatures and safe, distinct user logins. It is always best to avoid placing credentials or using generic login IDs. Individuals can be connected to the addition, deletion, or alteration of data in the record thanks to unique user logons. A secure connection between the signer and the final signature is necessary for a signature to be enforceable. It is not regarded as a secure or reliable way to electronically sign documents to employ digital reproductions of handwritten signatures from the Review of Good Data Integrity [9]

Legible: An electronic record needs to use controls such adhering to SOPs and creating a system that encourages saving electronic data in tandem with the completion of the task in order to be deemed legible, traceable, and permanent. The ideal way to achieve this is to forbid the formation of data in temporary memory and to require that all data be committed to permanent memory right away before being deleted. Operator actions must be documented using secure, time-stamped audit trails. Limiting security rights that enable users to erase data or disable the audit trail must be part of the system configuration. Whenever possible, these administrative rights ought to be kept separate for those who aren't in charge of the information included in the electronic records. The original value of the record is obscured when data is improperly overwritten or the audit trail is manipulated, which reduces the readability of the data [9]

Contemporaneous: Makes use of SOP writing controls and setting up instantaneous data commit to permanent memory. The record must also contain a safe time stamp mechanism that is unchangeable by users for the data to be deemed contemporaneous. Time and date stamps must match on all systems that are part of the GxP activity. When information is initially placed into an official electronic record after being captured on an unofficial document, it is not regarded as contemporaneous [9]

original: Standardized procedures must be followed for the inspection and approval of original electronic records, also known as certified true copies. The review process itself and any modifications to the data in the original records, including those recorded in audit trails or other pertinent metadata, should be covered in these procedures. The frequency, roles and duties, and methodology for the metadata review should all be outlined in written guidelines. Electronic data sets should be electronically signed to confirm their clearance after review. In order to ensure that original electronic documents are retained as long as feasible, controls should also be implemented. In the event that the original record is lost, it should be regularly backed up and kept separately in a secure area. An electronic archivist assigned to secure storage places who is not part of the GxP operation should exist. Periodic testing should be done to ensure that the copy may be removed and used from safe storage locations [9]

Accurate: A risk-based quality management system should be used to retain data. It is necessary to carry out routine calibration and equipment maintenance. Validation is necessary for computer systems that create, preserve, distribute, or archive electronic records. Critical data entry, including high.

Table 2: Common Data Integrity Issues and Mitigation Strategies

Data Integrity Issue	**Description**	**Mitigation Strategy**
Unauthorized Data Modification	Altering data without proper authorization	Implement role-based access controls (RBAC)
Incomplete Data Capture	Not recording all necessary data	Use automated data capture systems
Lack of Audit Trails	No records of changes made to data	Implement robust audit trail mechanisms
Data Loss	Data being lost or inaccessible	Regular data backups and recovery plans
Inadequate Training	Staff not trained on data integrity practices	Conduct regular training and awareness sessions

Values of data integrity :

- Most importantly, it makes sure that your company is safe from data losses or leaks. You must first make sure that your internal data is managed correctly in order to guarantee its security. Risks are reduced by accurately classifying and storing sensitive data through the use of error checking and validation procedures.
- Data integrity guarantees that the information you record for your company is reliable, accurate, and up to date. Your firm may lose money, time, and effort if choices are made based on biased or erroneous information. Data that is trustworthy and consistent must be the foundation of each effective data-driven decision. A tainted or defective database at your company could have long-term detrimental implications. Data integrity is essential for both helping you make the best business decisions and maintaining the reputation of your firm. For example, many companies collect personally identifiable information (PII) on their customers, which includes full name, address, Social Security number, and bank account information. Assume that there is a mistake in

this data collection. Due to a hacking attempt or an innocent typing error, your clients' personal information could be exposed or taken, falling into the wrong hands and being used maliciously.

• Finally, companies could retain less critical customer information, such as credit card numbers, which is nonetheless quite significant. If you track your customers' behaviors, for example, any errors in your data sets could lead to lost sales if you inappropriately categorize or target your consumers. As an example, if you track your customers' behavior on your website or solicit their comments, any mistakes in your data sets could lead to lost sales if you incorrectly categorize or target your consumers.

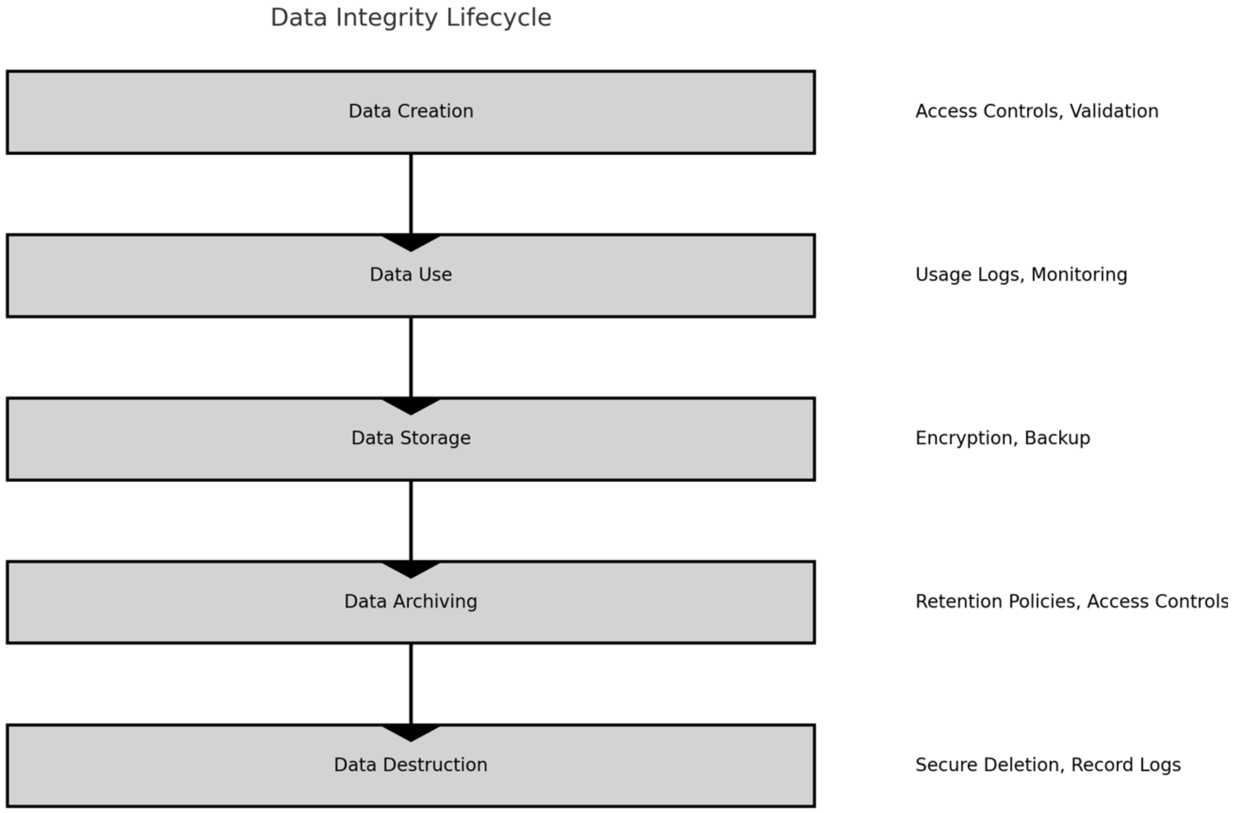

Figure 1 Data Integrity Lifecycle

• Data integrity becomes important for reasons other than legal ones. It has broad implications, such as strengthening your bonds with clients, maintaining a positive perception of your brand, and helping to keep your company protected from external threats.

Importance of data integrity:

• Authentic accurate data provided through data integrity may guarantee product efficacy, quality, and safety.

• The trust between the business and regulatory bodies develops and improves as a result of the integrity of the data.

• Tracking every step of the production process until the supply decreases, resulting in a decreased workload

• It assists in returning products that comply to regulations and improves a company's reputation within the sector.

• In conclusion, data integrity contributes by offering data that is entirely precise and consistent.

World regulatory recommendation for data integrity :

• USFDA: 21-CFR: The federal register, which is codified in 21-CFR (Code of Federal Regulation), is a publication used by the executive departments and agencies of the federal government to establish complete and permanent rules. Title 21 of the CFR contains the regulations governing the

Food and Drug Administration. Each book or volume has its CFR modified once a year, on or around April 1st.'[10,11,12]

- MHRA: The current EU GMP criteria for active ingredients and dosage forms are intended to be enhanced by the MHRA's guideline on GMP data integrity requirements for the pharmaceutical industry. Data integrity is crucial to the pharmaceutical quality system, which ensures that drugs are of the necessary caliber.'[14,15]
- TGA: The Australian regulatory body Therapeutic Goods Administration (TGA) establishes the benchmark for data integrity as a deficit. a weakness in a method or process that has produced or could produce a product that is harmful to users. It also occurs when it's found that the maker has fabricated, misrepresented, or duped products or data. [10,11]
- cGMP: In considering the significance of this issue, the FDA created recommendations on Data Integrity and Compliance with cGMP. The FDA acknowledges the trend of increasing data integrity breaches in these guidelines. cGMP-compliant record-keeping practices prevent data obscuration or loss. [14,15]The FDA is able to regulate cGMP thanks to the FD&C Act. Section 501 A A drug is deemed adulterated if "its manufacture, processing, packing, or holding methods, facilities, or controls do not conform to, or are not operated or administered in conformity with current best practices in order to assure that such drug meets the requirement of the act as to safety and has the identity and stringent quality controls.[10,15,16]
- Good Documentation Practices: In the context of these recommendations, "good practices" are defined as the collective and individual techniques that ensure that documentation, whether on paper or electronic, is trustworthy, readable, traceable, eternal, contemporaneously documented, precise, and original. [9]
- WHO: Within the framework of these recommendations, "good practises" are defined as those procedures that together and individually ensure that documentation, whether on paper or electronic, is accountable, readable, traceable, permanent, contemporaneously documented, original, and accurate. One of the most important stages in the process, which has numerous participants and activities, is ensuring the reliability and precision of the data manufacturers give to national regulatory organizations. That information needs to be comprehensive, accurate, truthful, and up to date in order to ensure the standard of research supporting petitions for pharmaceuticals to be approved for sale. Additionally, it needs to adhere to several standards, including good laboratory practices (GLP), good clinical practices (GCP), and good manufacturing procedures (GMP). [10,17,20]
- EMA: The European Medicines Agency (EMA) has released new Good Manufacturing Practice (GMP) rules to protect the integrity of data created throughout the testing, manufacture, packaging, distribution, and monitoring of medicines. Regulators utilize these data to evaluate the quality, safety, and efficacy of pharmaceuticals as well as to monitor the benefit-risk profile of those drugs over the course of their whole life cycle. Regulatory bodies and pharmaceutical companies may make well-informed judgments thanks to efficient data record administration, which guarantees accurate and consistent data production.[10,18,19]
- Data integrity and GDPR Compliance: Data integrity is essential for compliance with data protection laws like the GDPR. Businesses that don't follow these guidelines risk paying hefty penalties. They may be used in addition to these exorbitant prices on occasion. A company's closure is a possible outcome of persistent noncompliance.[10]

Types of data Integrity:

Physical and logical integrity are the two categories of data integrity. Both refer to a group of procedures and techniques used in relational and hierarchical databases to implement data integrity.

1) Structural soundness The preservation of data accuracy and completeness throughout archiving and retrieval is known as physical integration. When power outages occur, hackers interfere with database operations, or natural calamities terminate, physical integrity is jeopardized. It is impossible for data controllers, system programmers, seas application programmers, and internal

auditors to access reliable data because of human error, storage erosion, and numerous other problems.[21,22]

2) Clarity of reasoning Because the relational database uses logical integrity differently, the data is unaffected. Unlike physical integrity, logical integrity data offers safeguards against hackers and human error. Four various types of logical integrity exists.

3) The integrity of the entity In order to guarantee that the rows in a table are not empty, unique values must be created. Relational systems have the feature of storing data in arrays that may be connected and utilized in various ways.

4). Integrity of references A number of procedures known as "referential integrity" help guarantee that data is consistently used and stored. Only suitable additions, deletions, or changes are identified thanks to the rules built into the foreign key usage database's structure. Access to unapproved data may be canceled, duplicate data entries can be eliminated, and data accuracy may be assured, among other things.

5) Integrity of domain A collection of procedures known as "domain integrity" guarantee the veracity of every piece of data within the domain. A domain in this sense is a range of appropriate values that can be entered into a column. These could consist of limitations and other techniques that control the kind, quantity, and character of the data that is entered.

6) Integrity that is user-defined Rules and limitations that the user has established to suit their own requirements are included in user-defined integrity. Data security can occasionally be compromised by factors other than entity, context, and domain integrity. Initiatives pertaining to data integrity must also consider and make use of certain business principles.[20,21]

Data Integrity Risk:

The integrity of data in a database can be compromised by a number of different situations. Here are a few instances:-

- Human error: Data integrity is compromised when someone enters incorrect information, duplicates or removes data, doesn't follow the correct protocol, or makes mistakes when carrying out the process for information security objectives. Transfer errors: A transfer error occurs when information cannot be successfully moved from one location in a database to another. When a piece of data is present in a relational database's destination table but absent from its source table, transfer errors take place.
- Bugs and viruses: Software elements such as spyware, malware, and viruses can infiltrate a computer and alter, remove, or steal data.
- Hardware compromise:- Serious failures that may point to defective hardware include unexpected and sudden computer or server breakdowns, as well as problems with a computer's or other system's operation. Hardware that has been compromised may generate data that is erroneous or incomplete, limit or prohibit data access, or make information difficult to use.[23,24 ,25]

Advantages of Data Integrity

- Control of data redundancy: The database system aims to eliminate extremes by combining files. While the database system manages the amount of redundancy in the database, it does not completely remove it.
- Data consistency: To reduce the risk of consistency, the database approach removes or controls redundancy. It ensures that every copy of data will be maintained continuously.
- Greater information from the same quantity of data: The database system's integration of the data makes it possible to obtain greater information for the same amount of data.
- More information from the same quantity of data: The data is integrated by the database system, allowing for the acquisition of more information for the same quantity of data.
- Better data integrity: The database's integrity ensures the consistency and validity of the data that is saved. Limitations are sometimes employed when discussing integrity; one example is the consistency rule, which prohibits breaking a database.

• Better maintenance: The database system gives users freedom over their data. Changes to the database's data structure will affect the application software, making database applications easier to manage.
• More concurrency: Interactive data access can be effectively managed by the database. By preventing user interference, this guards against the loss of information or integrity.

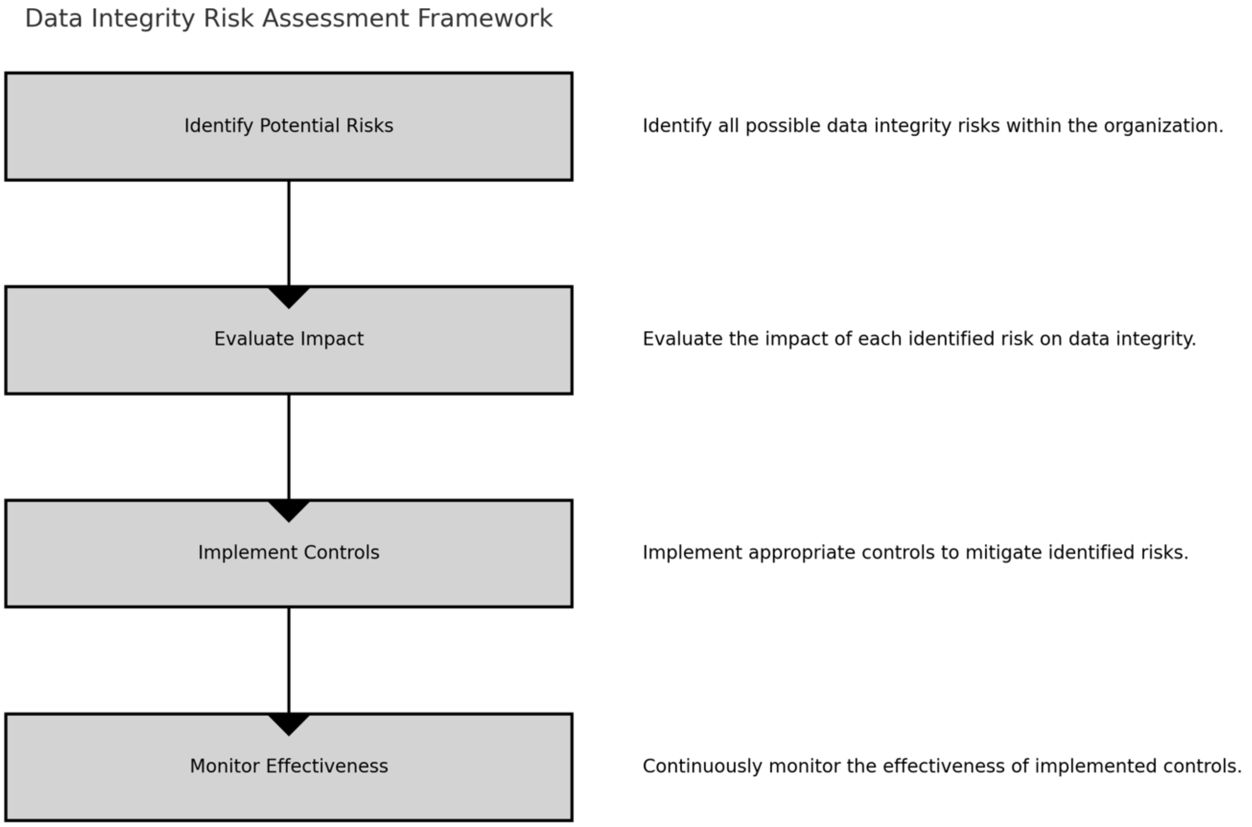
Data Integrity Risk Assessment Framework
Identify Potential Risks
Identify all possible data integrity risks within the organization.
Evaluate Impact
Evaluate the impact of each identified risk on data integrity.
Implement Controls
Implement appropriate controls to mitigate identified risks.
Monitor Effectiveness
Continuously monitor the effectiveness of implemented controls.

Figure 2 Data Integrity Risk Management

Disadvantages of data integrity

• Complexity: Database management system software is highly complex. All parties involved need to be aware of its benefits and make the most of it. Thus, training is necessary for administrators, designers, and users alike.
• Size: Large amounts of disc space and main RAM are needed for database management systems to operate correctly.
• Performance: The database technology offers many applications, albeit some may not operate as well as before, in place of a small number of specialized ones.
• Greater effect of a failure: Centralizing the database strategy makes the system more vulnerable. A malfunctioning component might significantly worsen customer service when you have to respond to every user and rely on the availability of the application database.
• Conversion cost: The business will incur additional costs for training and equipment purchases.

Importance of data integrity in pharmaceutical industry :

Advancements in technology and digital platforms are revolutionizing the way corporations operate in the global commercial arena. Business and digital platforms are now synonymous, thanks to the big data boom that has guaranteed increased productivity and efficiency of companies. Executives in business should always consider big data's wider significance for social and technological breakthroughs in addition to its commercial and economic potential. This means that new frameworks of action need to be included into regular business operations if the pharmaceutical industry is to benefit from these technologies as a whole.[31,32]

Technological developments and the emergence of digital platforms are completely changing how businesses function in the international marketplace. Today, businesses and digital platforms go hand in hand because of the big data explosion, which has ensured higher levels of efficiency and productivity for businesses. Business executives should always take into account not only the commercial and economic possibilities of big data, but also its broader significance for social and technical advancements. This implies that if the pharmaceutical sector is to gain from these technologies overall, new frameworks of action must be included into routine business processes.[28,33]

Stated differently, the quality of data determines a company's capacity to ensure the caliber of its output. Data records are the only proof that your production process conforms with quality standards. Data governance makes guarantee that documents and data are formally managed across the regulated company. Data governance encompasses the processes, people, and technology required for effective data management that ultimately produces high-quality outputs.[28,29,30]

Strategies to Prevent Data Integrity :-

Internal Quality Control Management: Although most problems with data integrity are caused by subpar organizational behaviors, we frequently believe that fraud data is the reason why it still exists. By implementing an appropriate quality management system, the organization may eliminate these problems. Good functioning may result from ideals, work ethics, and appropriate training. Using data governance, it is possible to guarantee greater data integrity. It is a set of procedures that guarantee that data are recorded, processed, stored, and used to maintain the record for the duration of the data lifetime, regardless of the format in which they are generated.

Design-Based Control : The company may use a variety of designs to guarantee data integrity. These policies might be created based on what the corporation deems convenient. Here are a few examples of control by design measures.

Validation of Computer Systems : It is a crucial component of design-based control. The outcome could be different if the computer is not adequately validated. Process control over both technology and procedure is guaranteed by a computer system validation.

Employees: Every employee in the company needs to receive the appropriate training. The company requires that the individual adhere to the validated process. Only authorized people are permitted to make changes to any GMP-related documents, including additions, modifications, or deletions. Each individual operating in the sector needs to be suitably qualified and accountable for their work.

Trails of Audits: Computer-generated date, time, and workflow sequence are known as audit trails. The majority of warning letters for data integrity issues are sent out as a result of audit trail failure. The company needs to make sure that all of the systems, including chromatography and HPLC, have audit trails enabled. It facilitates workflow authorization.

Safety The organization's premises need to be adequately secured. Data integrity problems could result from any security violation. It is necessary to prevent illegal individuals from entering. High security should be maintained in areas used for data storage, backup, and archiving. When it comes to cloud computing, it is especially important to comprehend the ownership, retrieval, retention, and security of data as well as the service provider.

Control by monitoring : Effective process monitoring can positively affect data integrity as well. third-party and internal audits. The internal auditing committee is responsible for conducting internal audits. Teams of reviewers are recruited in a third-party audit to check the data's validity, correctness, and traceability before providing a report. Today, with all data stored on computers, audits are also completed online. Among the things to take into account while conducting an audit are:

- An electronic record is centered within the system. This Paper is not essential to the examination.
- The ER/ES software must be configured.
- Examining the entries from audit trials.
- Another area of interest is the electronic signature inside a document.

Conclusion :
Since malpractices may allow subpar products to reach patients, data integrity in the pharmaceutical industry is essential to ensuring the quality of a final product. As a result, an established system is needed to ensure data integrity, data traceability, and reliability. Data integrity is an essential part of a Quality System from a quality perspective. The company's faith in using appropriate data to operate in compliance with regulatory requirements is built on quality data. For several reasons, including patient safety, process effectiveness, and product quality, regulators view data integrity as critical. Regulators base their evaluations of the company on the reliability and quality of the data. Identify flawed data integrity practices brought on by insufficient system efficacy. In circumstances where data is gathered and used to make decisions about manufacturing and quality, the Quality Risk Management (QRM) approach may help to prevent, identify, and reduce potential risks while guaranteeing that the information is reliable and trustworthy. Electronic data is kept intact via data integrity. The quality of a report depends on the facts upon which it is based. Information that is not kept on a computer can nonetheless be considered to be of high integrity. Properly managing digital or textual data is crucial for making wise business decisions. Data is becoming a commodity, thus it needs to be remembered to guarantee consistency with minimal work. After all, your company can grow to a greater extent the more data you have at your disposal. The quality of data provided has a significant impact on the reputation of any regulated lab. Taking into account that inspections and audits are limited to a review, the question of how many other instances of noncompliance there may be arises from the discovery of one fabrication incidence. Because of this, ensuring data integrity is crucial for analytical scientists, managers, and quality assurance staff in any organization. Making a mistake can have very expensive implications, and restoring regulatory trust will take time.

References:

1. Qas19-819-Rev1-Guideline-on-Data-Integrity. (2023). Retrieved from https://www.who.int/docs/default-source/medicines/norms-and-standards/currentprojects/qas19-819-rev1-guideline-on-data-integrity.pdf (accessed 2023-04-19).
2. WHO-Guideline-on-Data-Integrity-Draft. (2023). Retrieved from https://rx-360.org/wp-content/uploads/2018/08/WHO-Guideline-on-Data-IntegrityDraft.pdf (accessed 2023-04-19).
3. Nikam, N. R., Patil, P. R., Vakhariya, M. R. R., and Mohite, D. S. K. (2020). Data integrity: An overview. Hum Pathol. 11, 280-286.
4. World Health Organization. (2019). Working document QAS/19.819, Guideline on Data Integrity, October 2019, 14-16.
5. Boritz, J. (n.d.). IS Practitioners Views on Core Concepts of Information Integrity. Int. J. Account. Inf. Syst, Elsevier.
6. Veracode. (2012). What is data integrity. Retrieved from https://www.veracode.com/blog/2012/05/what-is-data-integrity (accessed 2023-04-19).
7. Digital Guardian. (n.d.). What is data integrity. Retrieved from https://digitalguardian.com/blog/what-data-integrity-dataprotection-101 (accessed 2023-04-19).
8. Uberveillance and the Social Implications of Microchip Implants: Emerging (n.d.). Page 40.
9. World Health Organization. (2016). Guidance on good data and record management practices. Retrieved from http://www.who.int/medicines/publications/pharmprep/WHO_TRS_996_annex05.pdf
10. Ahmad, S., Kumar, A., and Hafeez, A. (2022). Importance of Data Integrity & Its Regulation in Pharmaceutical Industry. Preprints. https://doi.org/10.22541/au.166265947.70683270/v1.
11. Hart, S. (n.d.). Data Integrity: TGA Expectations.

12. Rachel, P. K., and Gupta, N. V. (n.d.). Data Integrity – Regulations and Current Scenario. No. 05.
13. Data_integrity_definitions_and_guidance_v2_Withdrawn. (2023). Retrieved from 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. ECA Academy. (n.d.). New MHRA "GxP Data Integrity Guidance and Definitions" published. Retrieved from https://www.gmp-compliance.org/gmp-news/new-mhra-gxp-data-integrity-guidance-and-definitions-published (accessed 2023-04-19).
15. PharmaTutor. (n.d.). Data Integrity and Compliance With CGMP. Retrieved from https://www.pharmatutor.org/articles/data-integrity-and-compliance-with-cgmp (accessed 2023-04-19).
16. Purdie, F. P. (n.d.). Data Integrity and Compliance With CGMP Guidance for Industry.
17. Trs1033-Annex4-Guideline-on-Data-Integrity. (2023). Retrieved from 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).
18. EMA-Presentation-at-Mumbai-Conference-Feb-2017. (2023). Retrieved from https://rx-360.org/wp-content/uploads/2018/08/EMA-Presentation-at-Mumbai-Conference-Feb-2017.pdf (accessed 2023-04-19).
19. RAPS. (2022). EMA recommendation paper: Safety, data integrity key to decentralized trial conduct. Retrieved from https://www.raps.org/news-and-articles/news-articles/2022/12/ema-recommendation-paper-safety-data-integrity-key (accessed 2023-04-19).
20. Qas19-819-Rev1-Guideline-on-Data-Integrity. (2023). Retrieved from https://www.who.int/docs/default-source/medicines/norms-and-standards/currentprojects/qas19-819-rev1-guideline-on-data-integrity.pdf (accessed 2023-04-19).
21. Talend. (n.d.). What is Data Integrity. Retrieved from https://www.talend.com/resources/what-is-data-integrity/
22. AfterAcademy. (n.d.). What is Data Integrity. Retrieved from https://afteracademy.com/blog/what-is-data-integrity
23. Egnyte. (n.d.). What is Data Integrity and Why is it Important?. Retrieved from https://www.egnyte.com/guides/governance/data-integrity (accessed 2023-04-19).
24. Open Risk Manual. (2023). IT Data Integrity Risk. Retrieved from https://www.openriskmanual.org/wiki/IT_Data_Integrity_Risk (accessed 2023-04-20).
25. Spilka, S. (2023). Data Integrity: Relevancy, Risks and the Appropriate Use. ANEXIA Blog. Retrieved from https://anexia.com/blog/en/data-integrity-relevancy-risks-and-the-appropriate-use/ (accessed 2023-04-20).
26. Nikam, N. R., Patil, P. R., Vakhariya, M. R. R., and Mohite, D. S. K. (2020). Data intgrity: An overview. Hum Pathol. 11, 280-286.e
27. An Approach of Data Integrity in Pharmaceutical Industries. (2023). Eur. Chem. Bull. 12 (1). https://doi.org/10.31838/ecb/2023.12.1.002
28. Steinwandter, V., and Herwig, C. (2019). Provable Data Integrity in the Pharmaceutical Industry Based on Version Control Systems and the Blockchain. PDA J. Pharm. Sci. Technol. 73 (4), 373–390. https://doi.org/10.5731/pdajpst.2018.009407.

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

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

30. QBD. (2023). Data Integrity in the Pharmaceutical Industry. Retrieved from https://qbd.eu/wp-content/uploads/Data-Integrity-in-the-pharmaceutical-industry.pdf (accessed 2023-04-20).
31. Tremblay, J.-F. (2016). Indian Drug Firms Struggle with Quality Issues. CEN Glob. Enterp. 94 (16), 23–25. https://doi.org/10.1021/cen-09416-bus2.
32. PharmaBeej. (2023). Why Is Data Integrity Important In Pharma?. Retrieved from https://pharmabeej.com/why-is-data-integrity-important/ (accessed 2023-04-20).
33. Egnyte. (2023). What is Data Integrity and Why is it Important?. Retrieved from https://www.egnyte.com/guides/governance/data-integrity (accessed 2023-04-19).