STM JOURNALS

Research & Reviews: A Journal of
Pharmaceutical Science

ISSN: 2229-7006
Volume 15, Issue 1, 2024
January–April
DOI (Journal): 10.37591/RRJoPS

http://pharmajournals.stmjournals.in/index.php/RRJoPS/index

Review RRJoPS

Data Integrity Best Practices in Pharmaceutical Quality Assurance: A Thorough Review

Patil Divyashree Kantilal[1,*], Amruta N. Patil[2], Mansi Dhankani[2], Sunil P. Pawar[3]

Abstract

Data integrity stands as a linchpin in the reliability and trustworthiness of systems involved in handling, analyzing, and retrieving information, safeguarding the accuracy and consistency of data from inception to disposal. This study delves into the multifaceted realm of data integrity, encompassing its definition, pivotal importance, regulatory underpinnings, core principles, and practical implementation strategies. A comprehensive exploration of regulatory guidelines, including ICH Q7, EU Annexure 11, and FDA regulations, underscores the paramount significance of data security and adherence to good documentation practices. Emphasis is placed on the pivotal role of corporate culture, risk assessment, and data governance in fortifying data integrity, bolstered by enlightening case studies illustrating instances of data integrity lapses. Key principles, encapsulated by the acronym ALCOA+ (Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, and Available), are meticulously examined to provide a foundational understanding for maintaining data integrity. The study culminates with insights into pivotal aspects such as data review, audit trails, data security measures, cultural influences, and an analysis of contemporary trends in FDA warning letters associated with data integrity breaches. Recognizing and implementing robust data integrity practices are posited as imperative for organizations, serving as a linchpin for ensuring product quality, upholding regulatory compliance, and fostering public trust. In a rapidly evolving landscape, staying abreast of current trends and challenges in data integrity is essential for organizations navigating the intricate terrain of the pharmaceutical industry.

Keywords: Data integrity, regulatory compliance, data governance, risk assessment, ALCOA+

INTRODUCTION

Systems that store, analyze, or retrieve data must all be designed with data integrity in mind and employ it. Maintaining the consistency and accuracy of data throughout its lifecycle is what it entails. Although being within the broad category of computers, the term has multiple applications and can indicate quite a few different things depending on the situation. Sometimes taken as a stand-in for data quality, data integrity necessitates data validation. Reverse data integrity is called data corruption. Making sure that data is collected precisely as intended is the primary goal of any data integrity strategy. Make sure the data remains the same as it did at the time of recording and does not change later.

Data integrity, to put it briefly, aims to stop inadvertent modifications to data. The discipline of protecting data from unauthorized parties is known as data security; it should not be confused with data integrity. A computer system can be used to

***Author for Correspondence**
Patil Divyashree Kantilal
E-mail: divyashree2609@gmail.com

[1]Research Scholar, Department of Quality Control, Poojya Sane Guruji Vidya Prasarak Mandal's College of Pharmacy, Shahada, Maharashtra, India
[2]Assistant Professor, Department of Quality Assurance, Poojya Sane Guruji Vidya Prasarak Mandal's Collage of Pharmacy, Shahada, Nandurbar, Maharashtra, India
[3]Principal, Poojya Sane Guruji Vidya Prasarak Mandal's Collage of Pharmacy, Shahada, Nandurbar, Maharashtra, India

Received Date: March 07, 2024
Accepted Date: March 26, 2024
Published Date: March 30, 2024

Citation: Patil Divyashree Kantilal, Amruta N. Patil, Mansi Dhankani, Sunil P. Pawar. Data Integrity Best Practices in Pharmaceutical Quality Assurance: A Thorough Review. Research & Reviews: A Journal of Pharmaceutical Science. 2024; 15(1): 22–30p.

electronically record data, such as observations, results, and other facts and information, or it can be manually recorded on paper and displayed as data. Combining manual and computer solutions is an additional option. Integrity is an English word derived from the Latin adjective integer, which implies whole or comprehensive.

Being able to be honest and possessing strong moral principles are characteristics of integrity. It is usually a matter of personal choice to uphold moral and ethical standards. A common definition of integrity in ethics is being truthful, precise, and upright in one's actions. A company with higher data integrity is likely to be more morally successful in the long run. Vulnerabilities and lax data integrity protocols damage the quality of records and evidence, which may ultimately impact the quality of medications.

Data generated by paper-based and electronic systems alike must conform to the data integrity standards in all aspects of the quality management system. It is the responsibility of the manufacturer or distributor under inspection to maintain good data management and integrity procedures. They have an absolute responsibility to assess the effectiveness of their data management systems and to take the necessary steps to create and execute suitable data governance procedures in order to guarantee the preservation of data integrity [1].

REGULATORY FRAMEWORK

One essential regulatory requirement is data integrity. A number of guidelines and laws, including ICH Q7, EU Annexure 11, 21 CFR Part 211, and 21 CFR Part 11 of the FDA, are important in maintaining data accuracy and consistency as well as data integrity. Few regulatory parameters are as follows:

- The integrity of the data ought to be the management's concern. In order to make the personnel competent, they should guarantee appropriate training.
- The use of a database-equipped network system, guaranteeing data security system setup.
- Giving employees distinct identities when working electronically guarantees that any modifications made may be appropriately assessed. The document's electronic signature has to be verified.
- It is necessary to adhere to the company's SOP (standard operating procedure).
- Only an authorized individual may approve both physical documents and electronic data. The quality management system needs to review each document on a regular basis.
- Strict adherence to good documentation practices is required.
- Lab equipment needs to be properly calibrated and validated in order to reduce the possibility of errors in readings and measurements.
- Even when the correct SOP is followed, proper audit trails must be completed in order to ensure compliance with the legislation and aid in record maintenance [2].

DEFINITION AND IMPORTANCE

Definition

The organization must accept accountability for the data and systems it uses. The organizational culture should guarantee that all data, whether electronic or paper-based, is accurate, complete, and consistent. Organizational arrangements concerning personnel, systems, and facilities ought to be planned, run, and, when necessary, modified to facilitate an appropriate working environment. This entails setting up the proper conditions for data integrity controls to function as intended.

It is important to recognize the influence that corporate culture, senior management behavior, and performance indicators have on the effectiveness of data governance initiatives. Top management in the company should support the data governance policy (or something similar). It is expected of organizations to develop, create, and run a documented system that offers a sufficient level of control, taking into account the data integrity risk and providing justification. A good starting point would be to carry out a data integrity risk assessment (DIRA), which involves mapping out the processes that generate or collect data, identifying the formats and their controls, and documenting the underlying risks and data criticality.

Businesses should be mindful that switching back and forth between paper-based manual systems and computerized automated systems will not eliminate the requirement for adequate data integrity controls. Businesses should make sure that, in the event that vulnerabilities in data integrity are discovered, the necessary remedial and preventive measures are applied throughout all pertinent activities and systems, not just one. According to GXP MHRA Revision 1 of Data Integrity Guidance and Definitions, March 2018, Page 5 of 21, significant data integrity events, constituting 3.9%, should be reported to regulatory bodies in a manner that is suitable.

'ALCOA+' is not used in the guidance; instead, the term ALCOA is used. Complete, Consistent, Enduring, and Available is represented by the "+", while ALCOA stands for Attributable, Legible, Contemporaneous, Original, and Accurate. Historically, ALCOA has been thought of as specifying the characteristics of data quality appropriate for regulatory applications. To further highlight the needs, a '+' has been added. Whatever the term, the expectations are the same since data governance practices are supposed to guarantee that data is accurate, consistent, reliable, and accessible at all times during its lifecycle [3].

Importance

- Data integrity provides verified and correct information that can be used to ensure product efficacy, quality, and safety.
- The data's integrity contributes to the improvement and growth of trust between the company and regulatory bodies.
- Every step of the production process is inspected until the supply decreases, which guarantees less effort.
- It contributes to the recall of items that meet legal requirements, enhancing the company's standing in the marketplace.
- In conclusion, data integrity is beneficial since it offers entirely accurate and consistent data [2, 4].

KEY PRINCIPLES

Principles

1. *Attributable:* Information generated or gathered must be able to be linked back to the source of the data.
2. *Legislative:* Standards for data legibility and understanding are denoted by the phrases "legible" and "permanent". This is crucial for the pharmaceutical sector because a misspelled word could lead to the delivery of an entirely different medication.
3. *Contemporaneous:* At the time the work is done, the data must be documented; should have dated signature or initials.
4. *Original:* Information needs to be kept either as a certified accurate copy or in its original format.
5. *Accurate:* All information entered should be accurate, true, full, legitimate, dependable, error-free, and representative of the observation [4].
6. *Complete:* Making sure the data has all the necessary metadata for thorough documentation.
7. *Consistent:* Keeping the data in the proper chronological order to maintain sequence and consistency.
8. *Enduring:* Preserving the longevity and integrity of data as it is being used and stored.
9. *Available:* Making it simple for authorized personnel to verify and gain access [5].

DATA LIFECYCLE

Every stage of a piece of data's existence, from its creation and recording to its processing, usage, retention, archiving, retrieval, and destruction. This is rather straightforward and entails handling all data produced during an analysis, from birth to death. The definition is alternatively explained as follows: To ensure data integrity, data governance must be implemented throughout the entire data lifecycle. Data can be kept in the original system, in an acceptable archive, or under the right controls. Conversely, data governance is defined in the same paper as follows: the protocols to guarantee that

data are recorded, processed, stored, and utilized to guarantee the record throughout the data lifecycle, regardless of the format in which they are generated [6].

RISK ASSESSMENT

One of the most important procedures for guaranteeing the accuracy and dependability of data inside an organization is data integrity risk assessment. The growing dependence of organizations on data for decision-making and operational procedures necessitates the identification and mitigation of potential risks that may jeopardize the accuracy, consistency, and completeness of data. Data integrity will be defined at the outset of the introduction, along with its importance in the current corporate climate. We had also talk about regulatory standards related to data integrity to highlight the legal constraints that firms have to follow. We will look at the risk assessment method and its major steps for locating, assessing, analyzing, and minimizing possible risks to data integrity. Finding and assessing any risks that could jeopardize the quality, completeness, and dependability of data is the goal of conducting a risk assessment for data integrity.

Organizations can devise strategies to manage risks and gain insight into the vulnerabilities present in their data systems by using this evaluation. Organizations may get data-driven insights and evidence-based arguments to help them make educated decisions regarding protecting data integrity by adopting an analytical and research-driven strategy. Potential data integrity threats are assessed, along with their impact and likelihood, by means of a risk assessment. Organizations that want to find and fix any holes or weaknesses in their data management procedures must conduct a data integrity risk assessment first. It assists in guaranteeing that integrity standards, including precision, entirety, coherence, and dependability of data, are fulfilled during its entire existence.

Organizations can prevent regulatory compliance problems or jeopardize the quality and safety of their goods and services by proactively identifying potential integrity violations through a rigorous risk assessment. Performing audit trail reviews, remediation tasks, and life cycle management control implementation are just a few of the actions that make up this evaluation. In order to preserve patient safety and public confidence, industries like pharmaceuticals are required to abide by stringent data integrity criteria established by regulatory authorities, such as the Pharmaceutical Inspection Cooperation Scheme (PIC/S) [7].

DATA GOVERNANCE

Together, these mechanisms ensure data integrity, and that is what data governance is. Through these agreements, data is guaranteed to be an accurate, complete, consistent, enduring, and readily available record for the duration of its lifecycle, regardless of the process, format, or technology used to generate, record, process, retain, retrieve, and use it. Although creating a “data governance system” may not be required by law, doing so helps manufacturers organize, prioritize, and explain their data integrity risk management efforts. Lack of coordination across data integrity systems and possible gaps in control mechanisms can be indicated by the absence of a data governance system.

Data generation, processing, reporting, verification, usage in decision-making, storing, and eventual disposal at the conclusion of the retention period are all included in the data lifecycle. Throughout the lifecycle, information about a process or product may cross several borders. Information exchange across computerized and paper-based systems, as well as across organizational borders, is one example of this. It can also occur between service providers or between contract givers and acceptors, as well as between production, quality control, and quality assurance inside an organization.

Data governance techniques should be included in the PIC/S GMP/GDP Pharmaceutical Quality System. It should address data ownership over the whole lifetime and consider the architecture, operation, and oversight of systems and procedures to guarantee adherence to data integrity standards. This entails keeping an eye on intentional as well as unintentional data changes and removals. Data

governance systems combine technology, data security measures, well-designed systems, and specialist knowledge to effectively control data management and integrity. For regulated companies to successfully plan, develop, implement, run, and oversee data governance systems, the appropriate resources need to be deployed and made available. These resources ought to be commensurate with the operations, complexity, risk, and vitality of the information.

Controls over the data lifecycle that are consistent with the values of quality risk management should be implemented via the data governance system. An efficient data governance system will show that senior management is aware of and committed to good data governance practices, which include understanding data criticality, data risk, and data lifecycle, as well as the need for a combination of suitable organizational culture and behaviors. Additionally, there should be proof that expectations have been communicated to staff members at all organizational levels in a way that guarantees their empowerment to report shortcomings and possibilities for development. As a result, there is less motivation to remove, modify, or fabricate data. The pharmaceutical quality system should have documentation of the organization's data governance arrangements, which should be periodically evaluated [8].

DATA REVIEW AND AUDIT TRAILS

International rules such as EU GMP Guide Annex 11 and US 21 CFR Part 11 mandate audit trail assessments. According to clause 9, "based on a risk assessment, consideration should be given to building into the system the creation of a record of all GMP-relevant changes and deletions (a system-generated "audit trail")". When deleting or altering GMP-relevant material, the rationale must be stated in writing. Accessible, usually comprehensible, and subject to frequent inspection are requirements for audit trails. Regulations concentrate on the addition, removal, and alteration of GMP-relevant data, yet many IT systems are either unable to produce audit trails for GMP-relevant data at all or are unable to produce audit trails at all. Consequently, the goal of this course is to help you discover data that is important to GMP and learn how to conduct and record an audit trail review as part of a second-person review [9].

DATA SECURITY

The safeguarding of data against unwanted access, alteration, or deletion is known as data security. This covers both IT and physical security, such as firewalls, encryption, and authentication, as well as safe storage spaces and access controls [10].

CULTURAL ASPECTS

It is crucial to realize that data integrity and your quality culture are related. As soon as you accept this connection, you can find weaknesses, carry out the required risk assessment, and reduce your risks in advance of an inspection. Through the guidance guidelines, regulators have made it rather evident that an organization's culture affects the accuracy of the data that is being produced. It is projected that in the future, audits will concentrate on evaluating an organization's health in light of its data and culture [10].

CASE STUDIES AND EXAMPLES

Case Studies

1. Failure to investigate and document out-of-specification results obtained for (b)(4), API.
    i. For example, on Month/day/year (b) (4) lot # (b) (4) failed the assay test with an average out-of-specification (OOS) of (b)(4)%(specification is (b)(4)%). However, the firm released the batch using a passing retest result without conducting an investigation.
    ii. In your response you state that the OOS could not be related to the quality of the product because of the individual values obtained ((b)(4)% and (b)(4)%). Your response is inadequate in that you provided no scientific justification to support your conclusion. All out-of-specification results must be investigated and documented. We are concerned that you released this batch based on a passing retest result without conducting an investigation.

2. Failure to ensure that approved test procedures for (b)(4) and (b)(4) HPLC are followed.
    i. For example, the inspection found no scientific justification for the current sequence of chromatographic injections performed, which is different to these quence included in the approved analytical method. Your analytical method requires that (b)(4) and then by the injection of the samples to be tested. The inspection found that a different sample and standard sequence was used for the assay analysis of (b)(4). Although your response to the inspectional observations state that analysts have been retrained, we remain concerned about current laboratory practices, in that not all injection results are being reported.
    ii. For example, the assay test for lots #failed to include all the injection results performed as part of the chromatographic run. Your response provides no explanation regarding why analytical results are selectively reported.
3. Failure to have complete and reliable laboratory control records derived formal tests conducted to ensure compliance with established specifications and standards.
    i. For example, the inspection revealed that your firm lacks raw data of the sample and standard weights used for the HPLC assay of (b)(4). The only record available was an Excel spread sheet with values entered to calculate the final assay results. In addition, some of the HPLC chromatographs of the lots tested were not included in the batch record.
    ii. In your response you acknowledged missing raw data, and stated that all raw data is now required to be maintained and included as part of the batch record [11].

Examples

1. A batch document has been sent back to production after QA batch review/release stage found missing signatures/dates and missing data entries [12].
2. Changing the original.
3. Raw data and records.
4. Repeating the assay with the same sample without providing a reason.
5. Looking into out-of-spec analysis.
6. Manipulating a poorly defined analytical procedure and related data analysis to obtain passing results.
7. Back dating test results to comply with protocol requirements; producing acceptable test results without conducting tests.
8. Substituting testing for another batch using test results from prior batches [13].

CURRENT TRENDS

Figure 1 shows that FDA warning letters citing DI breaches have become more commonplace, as reported by Unger Consulting Incorporation. This could be because operators are ignorant and irresponsible, inspectors are more likely to take risks in breaching DI for a variety of reasons, inspectors are better equipped to spot DI concerns, or pharmaceutical inspectors intentionally look for breaches. Because the growing frequency of DI problems and the management of them seem to be relatively new phenomena, it is difficult to identify the underlying reasons for DI breaches.

Tables 1 and 2 also show that the majority of the DI violations cited concerns as manual, automatic, mechanical, and electronic equipment. Examples of these violations include “failure to maintain written records and calibrate written records” and “failure to exercise appropriate controls over computers or related systems to assure that changes are made to production and control records, laboratory records, or other records only by authorized personnel”.

The next few most frequently reported DI infractions deal with pharmaceutical product quality control. China and India are the top two nations receiving warning letters related to DI (Table 3 and Figure 2). Parent pharmaceutical companies in the US and Europe have been known to relocate their manufacturing facilities to these nations in order to lower production costs. It is also critical to stress that the FDA frequently cites DI breaches while conducting inspections of domestic producers [15].

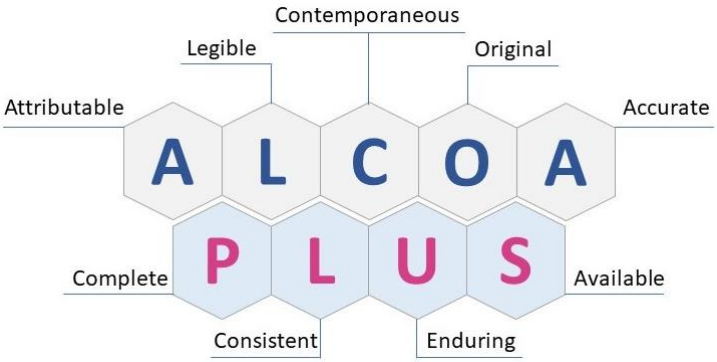

Figure 1. Principles of data integrity [14].

Table 1. Drug GMP inspections, citations frequency by regulations and year [15].

Citation	Short description	2013	2014	2015	2016	2017	2018	2019
Total Form 483s issued using FDA tools for drug inspections		690	645	678	691	694	716	779
§211.22(d)	Procedures applicable to the quality unit shall be in writing and shall be followed	168	148	165	153	185	208	215
§211.192	Investigations of discrepancies	239	209	250	227	278	183	167
§211.42(c)	Facilities shall include defined areas of sufficient size	94	125	235	227	148	134	156
§211.160(b)	Lab controls should include scientifically sound specifications	199	165	246	133	207	209	145
§211.166(a)	Stability testing	104	82	126	124	72	111	135
§211.100(a)	Production and process controls shall be supported by written procedures	135	107	123	110	116	102	129
§211.67(b)	Equipment cleaning and maintenance	83	80	91	102	91	112	124
§211.188	Master production and control records	114	74	110	100	208	93	123
§211.113(b)	Control of microbiological contamination	119	109	157	118	92	71	121
§211.25(a)	Personnel qualifications	132	115	119	99	113	47	113
§211.67(a)	Equipment shall be cleaned/ sanitized or sterilized	71	94	113	94	54	81	99
§211.110(a)	Sampling and testing of in process materials and final product	79	71	85	65	68	86	94
§211.165(a)	Appropriate lab tests shall be used to determine conformance to specifications	66	64	80	73	64	56	90
§211.68(a)	Automatic, mechanical and electronic equipment	69	64	72	80	67	60	67
§211.100(b)	Contemporaneous documentation of activities	84	62	72	70	65	60	54

FDA: US Food and Drug Administration: GMP: good manufacturing practice.

Table 2. Frequent data Integrity violations and regulation citations in FDA warning letters [15].

21 CFR reference	Number of times cited	Title of CFR section
211.194	10	Laboratory records, review of all data
211.188	6	Batch production and control records
211.165 (a) and (b)	5	Testing and release for distribution
211.192	5	Production record review, deviations and investigations
211.68	2	Automatic, mechanical and electronic equipment

Table 3. Number of data integrity associated warning letters by country (2008 to 2018) [15].

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	Total
China	1	1	3	1			2	2	14	19	15	58
USA	1	2	1	1	1			0	7	15	8	36
India	1	1		2		6	7	10	9	12	6	54
Europe		1					1	2	6	3	1	14
Brazil									3			3
Japan	1								2	1	3	7
Thailand								1				1
Canada			1		1					2	1	5
Mexico					2					1	1	4
UAE					1							1
Jamaica					1							1
South Korea											4	6
Singapore										1		1
Australia											1	1
Taiwan											1	1
Dominican Republic											1	1
Total	4	5	5	4	6	6	10	15	41	56	42	194

UAE: United Arab Emirates.

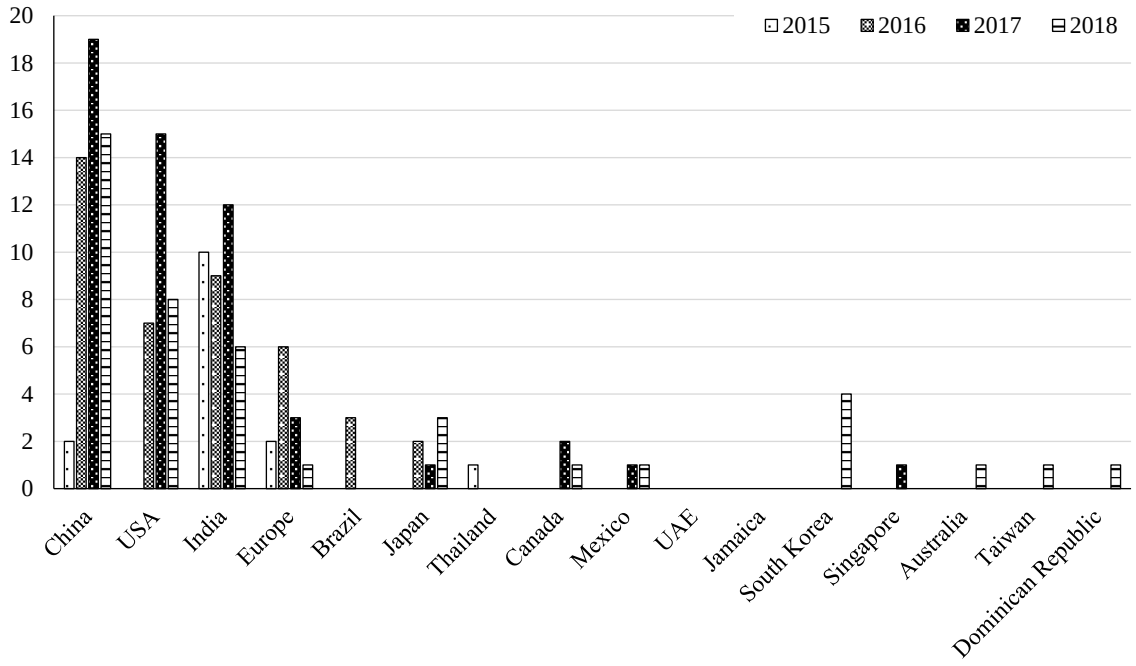

Figure 2. Percentage of DI associated warning letters by country (2008 to 2018) [15].
DI: Data Integrity.

CONCLUSION

In conclusion, data integrity stands as a linchpin in the realms of information management, ensuring the accuracy, consistency, and reliability of data throughout its lifecycle. The regulatory framework, encompassing guidelines like ICH Q7, EU Annexure 11, and FDA regulations, underscores the paramount importance of data security, training, and adherence to standard operating procedures. Corporate culture, risk assessment, and robust data governance play pivotal roles in fortifying data integrity practices.

The ALCOA+ principles serve as a beacon, emphasizing the need for data to be Attributable, Legible, Contemporaneous, Original, Accurate, Complete, Consistent, Enduring, and Available. Case studies vividly illustrate the repercussions of lapses in data integrity, emphasizing the imperative for thorough risk assessments and proactive measures.

Data review, audit trails, and stringent security measures contribute to maintaining data integrity, while acknowledging the interconnectedness of quality culture and accurate data production. As current trends suggest an increasing focus on data integrity breaches in regulatory inspections, organizations must prioritize robust systems and practices to ensure compliance, product quality, and public trust. In essence, upholding data integrity is not just a regulatory requirement but a cornerstone for the credibility and success of organizations in a data-driven landscape.

REFERENCES

1. Snehal Chandrashekhar Jale, *et al*. A Review: An Illustration of Data Integrity. Int J Res Publ Rev. 2023 May; 4(5): 5620–5629.
2. Sahoo P, Kamaraj R. Review of Data Integrity in Pharmaceutical Industry. Int J Res Pharm Sci. 2020; 11(Spl 4): 1323–1328. Accessed March 26, 2024. https://ijrps.com/home/article/view/2131
3. Ankur Choudhary. (2023). ALCOA Principles of Data Integrity. [Online]. Pharmaguideline. https://www.pharmaguideline.net/what-is-data-integrity-in-pharmaceutical-industry/
4. Sushmita Singh, *et al*. Importance of Data Integrity in Pharmaceutical Industry. EPRA International Journal of Economics, Business and Management Studies (EBMS). 2023 Feb; 10(2): 100–106.
5. Pharma Lex. (2023 Aug 16). Data Integrity in Pharmaceuticals. [Online]. Accessed March 26, 2024. https://www.pharmalex.com/thought-leadership/blogs/data-integrity-in-pharmaceuticals-empowering-trustworthy-decisions-from-source-to-success-via-registration-dossier/#:~:text=Legible%20and%20Permanent%3A%20Ensuring%20data,its%20source%20to%20subsequent%20modifications.
6. McDowall RD. Data Integrity Focus, Part VII: A Data Life Cycle for Chromatography. LCGC N Am. 2019 Aug 1; 37(8): 532–537.
7. Chris Sasidhar Duggineni. Data Integrity and Risk. Open J Optim. 2023; 12(02): 25–33. doi: https://doi.org/10.4236/ojop.2023.122003
8. Pharmaceutical Inspection Convention Pharmaceutical Inspection Cooperation Scheme. Good Practices for Data Management and Integrity in Regulated Gmp/Gdp Environments Pi 041-1. 2021 Jul 1.
9. Gmp-compliance. (2018 Apr 20). Copenhagen, Denmark Audit Trail Review. [Online]. Accessed March 26, 2024. https://www.gmp-compliance.org/training/gmp-course-conference/audit-trail-review
10. Ramesh Chand D. (2023 Feb 11). Corporate Head -Audit and Compliance at Steriscience Data Integrity, Quality Culture, Sustainability Challenges & FDA Focus. [Online]. https://www.linkedin.com/pulse/data-integrity-quality-culture-sustainability-challenges-dogra
11. Aham Magaly E. (VP Compliance Pharma-BioServ US, Inc). Data Integrity Case Studies Pharmaceutical Industry Trends. Conference, São Paulo, Brazil. 2017 Mar 14. www.pda.org
12. Mark Dickson. Data integrity overview and case study examples. National Validation & GMP Forum, Melbourne. 2017 Jul 24–25. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.pharmout.net/wp-content/uploads/2018/02/D2.T1.4.3-Data-Integrity-overview-and-workshop-examples-National-Validation-and-GMP-Forum-Jul-2017-MD-answers_Mark-Dickson.pdf
13. Kumar K. Data Integrity in Pharmaceutical Industry. J Anal Pharm Res. 2016; 2(6): 00040. DOI: 10.15406/japlr.2016.02.00040
14. Pharma Digest. (2023 May 17). Data Integrity in Pharmaceutical Industry. [Online]. Pharma Digests. Accessed March 26, 2024. https://pharmadigests.com/data-integrity-in-pharmaceutical-industry/
15. Sia Chong Hock, *et al*. Pharmaceutical Data Integrity: issues, challenges and proposed solutions for manufacturers and inspectors. Generics and Biosimilars Initiative Journal (GaBI Journal). 2020; 9(4): 171–82. DOI: 10.5639/gabij.2020.0904.028 Volume 9 / Year 2020 / Issue 4 Page: 171-82

