International Journal of Management, IT & Engineering
Vol. 14 Issue 8, August 2024
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Data Integrity: Ensuring Quality and Safety Through Robust Controls and Risk Management

Shikha Patel*
Krunal Soni**

Abstract

Data integrity is vital for ensuring reliable information in pharmaceutical manufacturing, directly impacting product quality and patient safety. This paper emphasizes the importance of maintaining complete, consistent, and accessible data throughout its lifecycle, from creation to storage and retrieval. With the rise of electronic data, traditional methods of ensuring data integrity are often insufficient. A risk-based approach is recommended, assessing and applying controls based on the data's criticality and vulnerability. This review discusses regulatory trends, risk management, and practical examples of maintaining data integrity in various systems. It also explores the principles of Quality Risk Management (QRM) and offers strategies for establishing suitable data integrity controls. The focus is on critical processes and data management systems within pharmaceutical facilities, underscoring the collective responsibility of all employees to ensure data accuracy and reliability. The paper highlights the necessity of robust procedures, regular testing, and continuous monitoring to safeguard against potential data breaches and ensure compliance with Good Manufacturing Practices.

Keywords:

Data Integrity;
Electronic Audit Tails;
Quality Risk Management;
GMP Compliance;
Pharmaceutical Manufacturing.

Author correspondence:

Shikha Patel,
Sr. Manager, Quality Technical Operations
Editas Medicines, Cambridge, Massachusetts, USA
Email: shikha.patel@editasmed.com; shikhapatel87@gmail.com

1. Introduction

Data integrity is crucial for ensuring that the information used to guarantee product quality and patient safety is reliable. Reliable manufacturing data depends on having good procedures, systems, and controls in place. These controls start when the data is first created and continue throughout its entire life, including how it's stored and later retrieved to maintain product quality.

*Senior Manager, Quality Technical Operations, Editas Medicines, Cambridge, Masschussetts- USA.
**Senior Director, Quality, eGenesis, Cambridge, Masschussetts- USA.

Data integrity means that data should be complete, consistent, durable, and available. Pharmaceutical companies must ensure that data is recorded and traceable to the person who performed the task. Data must not be deleted, omitted, or changed to misrepresent events. Any breaches, intentional or not, need to be investigated.

With advances in technology, there's been a big increase in electronic data. Old methods for ensuring data integrity may not work well now, so using a risk-based approach is important. This means assessing risks and applying controls based on those risks, whether using manual, electronic, or a mix of both systems. This report discusses regulatory trends, risk management, and offers examples of how to maintain data integrity in different systems.

1.1 Purpose

The rapid advancements in automation and information technology, coupled with affordable data storage and superior electronic audit trails, have prompted the pharmaceutical industry to reassess good manufacturing practices (GMP) controls. This has led to an increased focus on establishing and maintaining effective data integrity controls throughout the drug manufacturing process. While the importance of accurate and complete data is well recognized, there is still some confusion about the necessary level of data integrity control at each step to comply with GMP regulations. Many companies face challenges in determining the appropriate controls for each manufacturing operation and the necessary levels of review and verification to ensure reliable manufacturing data. This review outlines an approach using quality risk management (QRM) to establish and evaluate the suitability of data integrity controls for each manufacturing operation based on the data's criticality and vulnerability for its intended use.

Ensuring data integrity is a collective responsibility within an organization. Employees at any facility involved in manufacturing, processing, packaging, or holding finished pharmaceuticals, intermediate ingredients, or APIs must ensure that data collected throughout the manufacturing process is accurate and reliable. Managers, quality assurance personnel, operators, technicians, and support staff need to be constantly aware of the importance of maintaining and documenting data integrity to ensure the quality and safety of their products.

1.2 Scope

The information in this review is relevant to managing data at pharmaceutical facilities involved in the manufacturing, processing, packaging, or holding of finished pharmaceuticals, APIs, or intermediates. It focuses on data related to manufacturing operations, materials, facilities and equipment, production, packaging and labeling, including in-process controls and process analytical testing. Additionally, it covers the procedures, systems, processes, and controls used at a drug facility to ensure compliance with applicable laws, regulations, and directives, and to support the identity, strength, quality, and purity of the drugs.This review does not cover data integrity management in clinical practice or the implementation of clinical trials.

2. Glossary And Abbreviations

Audit Trail: A secure,computer generated, time stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification, or deletion of an electronic record. *(2)*

ALCOA +

Attributable: It should be possible to identify the individual or computerized system that performed the recorded task this applies to changes made to records as well: corrections, deletions, changes, etc.

Legible: All records must be legible- the information must be readable in order for it to be of any use. This applies to all information that would be required to be considered complete, including all original records or entries.

Contemporaneous: The evidence of actions, events or decisions should be recorded as they take place. This documentation should serve as an accurate attestation of what was done, or what was decided and why, i.e., what influenced the decision at that time.

Original: The original record can be described as the first capture of information, whether recorded on paper (static) or electronically (usually dynamic, depending on the complexity of the system). Information that is originally captured in a dynamic state should remain available in that state.

Accurate: Ensuring results and records are accurate is achieved through many elements of a robust pharmaceutical quality system this can be composed of:

- Equipment related factors such as qualification, calibration, maintenance and computer validation.
- Policies and procedures to control actions and behaviors, including data review procedures to verify adherence to procedural requirements.

Complete: All information that would be critical to creating an event is important when trying to understand the event a complete record of data generated electronically includes relevant metadata.

Consistent: Good documentation practices should be applied throughout any process, without exception, including deviations that may occur during the process. This includes capturing all changes made to data.

Enduring: Records must be kept in a manner such that they exist for the entire period during which they might be needed.

Available: Records must be available for review at any time during the required retention., accessible in a readable format to all applicable personnel who are responsible for their review whether for routine release decisions, investigations, trending, annual reports, audits or inspections. *(5)*

Critical Process (CP):A process that impacts a critical quality attribute of the, drug substance or drug product being manufactured and therefore should have established critical process parameters that can be monitored or controlled to ensure that the process produces the desired quality.*(8)*

Critical Process Parameter (CPP):A process parameter whose variability has an impact on a critical quality attribute and therefore should be monitored or controlled to ensure the process produces the desired quality.

Critical Quality Attribute (CQA): Physical, chemical, biological or microbiological property or characteristic that should be within an appropriate limit, range or distribution to ensure the desired product quality.

Data Integrity Controls: Controls put in place to either minimize the potential for a data integrity issue to occur or, if an issue does occur, the controls apply to increase the probability of detection.

Detectability: The ability to discover or determine the existence, presence or fact of a hazard *(6)*.

Mitigation: systematic steps taken or in place to reduce or limit the identified risk.
Peer Review: Review of data by a colleague who has a similar level of responsibilities as the person performing the activity or capturing the data.
Quality Unit: An independent quality unit/structure with authority to fulfill certain pharmaceutical quality system responsibilities *(7)*.
Risk Control actions implementing risk management decisions *(8)*.

2.1 Abbreviations

AHU/HVAC	Air Handling Unit/Heating, Ventilation And Air Conditioning
ALCOA	Attributable, Legible, Contemporaneous, Original And Accurate
API	Active Pharmaceutical Ingredient
BMS	Building Management System
BPR	Batch Processing Record
CAPA	Corrective Action, Preventive Action
CFR	Code Of Federal Regulations
CP	Critical Process
EBR	Electronic Batch Recording
FDA	U.S. Food And Drug Administration
GAMP	Good Automated Manufacturing Practice
GMP	Good Manufacturing Practice
GxP	Good Practice Quality Guidelines For Various Fields
HMI	Human Machine Interface
ICH	Human Conference On Harmonization
ISPE	International Society For Pharmaceutical Engineering
MES	Manufacturing Execution System
OOS	Out Of Specification
PLC	Programmable Logic Controller
QMS	Quality Management Systems
QRM	Quality Risk Management
SOP	Standard Operating Procedure

3. Risk Management For Data Integrity

The principles of Quality Risk Management (QRM) are relevant throughout the data lifecycle, encompassing data capture, recording, transcription, archiving, and other aspects of data management. This section uses examples to illustrate how certain elements can threaten the integrity of pharmaceutical and biopharmaceutical data.

Risks must be managed regardless of whether data is handled manually or through an automated electronic system. Any potential breaches affecting data integrity, such as loss, omission, alteration, or deletion, must be investigated and accounted for within the quality system and, if necessary, reflected in risk management documentation*(11)*. Since data can be managed and transferred across different formats or systems, measures should be taken to mitigate risks during these transfers. As the industry shifts from paper-based to hybrid (manual and electronic) systems, and eventually to fully electronic systems, careful and targeted application of data integrity principles is essential.

3.1 Risk Considerations

Risk assessments should be conducted proactively when a new data management system is implemented and should be captured within the overarching change control process. At this stage, risk assessments act as preventative measures to ensure data integrity is maintained throughout the system lifecycle. For existing data management systems, risk assessments should identify potential vulnerabilities based on the current level of controls and the criticality of the data for its intended use.*(13)*

Data integrity controls must be considered from both behavioral and technical perspectives. From a behavioral standpoint, the overall quality culture, including effective communication and training, is closely linked to the success of the data integrity program.

3.2 Risk Control Strategies

The potential impact on data must be determined and documented and, following the risk assessment, mitigations must be determined to reduce risk. For risk that have been identified as having a high probability of occurrence and a high impact on product quality or patient safety, balance risk control strategy will need to be implemented. Understanding the manufacturing process and data lifecycle processes is crucial to developing successful risk control strategies.

Although automation is not the solution to every problems, it can be useful tool as part of a risk control strategy. Intelligent barcodes can be used to confirm product and component identity and can prevent a process from proceeding until the error is rechecked and corrected. The time honored use of a second person checking or supervised and reviewing is also important, provided that it is timely. Frequently, the supervisory review takes place too long after an event to confirm that it occurred as recorded.*(15)*

3.3 Data Integrity Risk Management Model

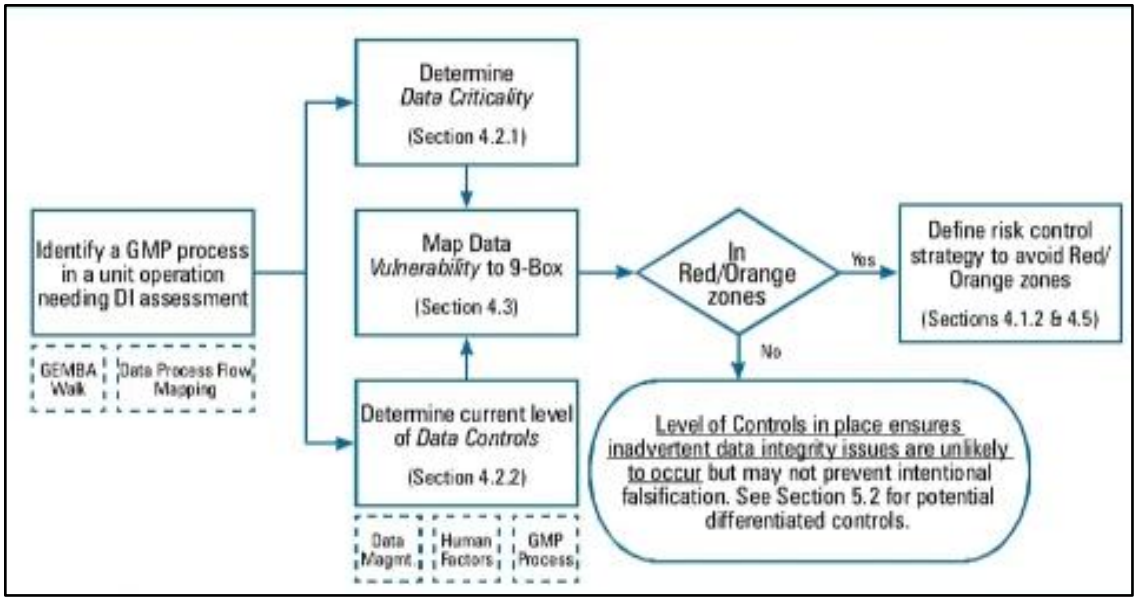
All data, whether recorded electronic or on paper, requires a risk management approach to determine what controls are important to assure data integrity.

To estimate the level of exposure to potential data integrity issues, the following elements as illustrated in *Figure 1*, must be controlled:

- Data criticality
- Data Management
- GMP Process and Human factors

International Journal of Management, IT & Engineering
Vol. 14 Issue 8, August 2024
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Figure 1: Data Integrity Risk Management Model



Data Criticality	Definition
High	When the intended use of the data directly impacts product quality and/or product Safety: • Quality monitoring and control of processes that may be responsible for causing variability during manufacturing, release or distribution impacting critical quality attributes, critical material attributes including those that may be linked with the product registration. • Product Safety monitoring and control of processes that ensure effective management of field alerts, recalls, complaints or adverse effects.
Medium	When the intended use of the data relates to quality attributes common material attributes, process parameters, key process parameters, or process controls that are not COAs/Critical Processes(CPs)/CPPs and may or may not be in the product registration; this includes parameters of the manufacturing process that "may not be directly linked to critical product quality attributes but need to be tightly controlled to assure process consistency" *(28)*
Low	when the intended use of the data is to provide evidence of GMP compliance relating to monitoring and control of processes that do not fall into the High or Medium category.

3.4 Classification Of Data Criticality

Data criticality reflects the connection between specific data and the quality of the product. This concept is grounded in the knowledge acquired from process development, validation, and quality processes throughout the product lifecycle. It is assessed through a series of pertinent questions that categorize data criticality as high, medium, or low (*see Table 1*).

4. Data Integrity Controls

Numerous events during manufacturing can compromise data integrity. These can be triggered by various factors such as human error, inadequate training, system failures, improper system qualification or configuration, poor procedures, non-compliance with procedures, and intentional falsification. Preventing breaches in data integrity involves implementing and maintaining robust controls for both electronic and paper-based data. Ensuring data integrity involves protecting original data from accidental or intentional modification, falsification, and deletion. For several decades, global regulations have required data to be ALCOA+ throughout its lifecycle.

Data integrity controls can be embedded in operational procedures and practices or included in computer system validation and equipment qualification. These controls aim to minimize the likelihood of data integrity issues and increase the probability of detecting any that occur. Regulations specify core elements necessary for ensuring data integrity within a robust QMS, such as:

- Standard operating procedures (SOPs) for record completion and retention.
- Adequate training for individuals based on their job roles.
- Validation or qualification of systems for their intended purposes.
- Access to necessary records for personnel to perform their duties, with data integrity addressed as part of the QRM process.
- A management review process that elevates data integrity issues to the highest organizational level.
- An endorsed data governance policy to promote a strong data integrity culture across the organization.
- Routine data verification and periodic surveillance checks.
- Self-inspections to verify the effectiveness of data integrity controls.
- A robust change management system.

These measures collectively help in minimizing the potential for data integrity breaches and ensure a robust quality management system (QMS).

4.1 Storage and Access to Archived Records

Table 2 lists various controls to prevent issues with storing and accessing completed or archived paper records. These controls are applied at the record or system level to prevent potential data integrity problems.

All documents should be stored in a way that maintains their readability over time. High and medium-criticality documents, like batch records and validation protocols, should be kept in a climate-controlled area with restricted access. Access should be tracked using a card key system and a logbook to record the removal and return of records. It is advisable to review access permissions annually.

For low-criticality documents, such as user access authorization forms (when training evidence is recorded elsewhere), storage in an office location like a file cabinet with restricted key access is acceptable. Access to the keys should be reviewed every six months.

International Journal of Management, IT & Engineering
Vol. 14 Issue 8, August 2024
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Table 2: Data Integrity Control for Storage and Access to Archive Records

Storage and Access to Completed and Archived Records		**High Data Criticality**	**Medium Data Criticality**	**Low Data Criticality**
Prevention Control	Where Stored	Climate-controlled room	Climate-controlled room	Climate-controlled room
	How Removed and Returned	Access control to room and logbook recording of removal and return of the record	Access control to room and logbook recording of removal and return of the record	Logbook recording of documents checked-in/ checked-out
	Access Control	Card Key access or limited key access with entry documented in logbook	Card Key access or limited key access with entry documented in logbook	Limited key access
	Periodic User Access Review	Annually	Annually	Every 2 years

4.2 Generation and Reconciliation of Documents

High-criticality records, such as batch records, should be issued by a designated unit and assigned a unique identifier. The printing of these records should be strictly controlled, with authorization limited to specific personnel designated by the quality unit. A thorough reconciliation of the records, including any extra sheets or additional pages, is mandatory after their use.

For medium-criticality documents, like calibration forms, a unique identifier is not necessary. However, control over printing should ensure that only a limited number of individuals authorized by the quality unit can print the templates. There should be established procedures for the destruction of unexecuted (blank) forms, which may be carried out by either the operating unit or the issuing unit.

Low-criticality documents, such as blank forms used for recording training activities, may be printed by the end user without a unique identifier, and no reconciliation activities are required after use. There is no restriction on the number of copies that can be printed, and unexecuted (blank) forms can be discarded by the user without the direct involvement of the quality unit in the process.

4.3 Electronic Audit Trail Review

Audit trails are a type of metadata that record details such as the creation, addition, deletion, or alteration of data within a system. They ensure secure recording of lifecycle details without overwriting the original record. When equipment like instruments or devices is used to handle relevant GMP data electronically, the system must include and retain a suitable audit trail.

A secure, computer-generated timestamp or trail should allow the reconstruction of the history of events related to the record, including who performed the action,

what was done, and when it occurred. If modifications or corrections are made, a comment should be added to record the value of the activity as part of the audit trail. If it is not technically possible to record the reasons for changes or deletions within the audit trail, alternative documentation should be used.

The electronic audit trail may consist of multiple sources related to the equipment, such as event logs, alarm logs, system logs, history files, trends, or reports. It is crucial to understand where the information is recorded within the system, at both the operating system and application levels, to protect the data and know where to look when performing an audit trail review.

In the following sections, audit reviews for three types of data within electronic audit trails are discussed:

- Data associated with batch setup, such as the recipe used and set points or times planned for specific activities during the batch.
- Batch run data, which includes data from the manufacturing process, such as temperatures, duration of activities, and who performed the activities.
- System configuration data, which includes data relevant to the batch but associated with the system's configuration, such as user account information, privileges granted to users, and where data is stored.

Reviewing audit trails helps detect potential data integrity issues. Some regulations require that audit trails be reviewed periodically. The person performing the audit trail review must be independent, technically capable of understanding the audit trail, and should not have been involved in the creation or verification of the data being reviewed.

4.4 Backup of Electronic Data

This section covers preventive measures for backing up electronic data. Companies should create a backup strategy based on key principles to determine how often data backups should occur. This strategy should consider the company's risk tolerance and the importance of ensuring that manufacturing activities can be recreated if there is a system failure and data has not been backed up.

A principle-based backup strategy means that companies must evaluate which data is most critical and how frequently it should be backed up. For instance, data that is crucial to ongoing manufacturing processes may need more frequent backups than less critical information. By assessing the importance of different types of data, companies can prioritize their backup efforts to ensure minimal disruption in case of a system failure.

Additionally, companies should conduct regular tests of their backup systems to verify that data can be restored effectively. These tests help identify any weaknesses in the backup process and ensure that, in the event of a failure, the company can quickly recover essential data and continue operations with minimal downtime. Regular testing and updating of backup procedures are essential components of a robust data management strategy, safeguarding against potential data loss and ensuring business continuity.

5. Conclusion

Ensuring data integrity is paramount in pharmaceutical manufacturing, as it underpins product quality and patient safety. This review highlights the critical need for complete, consistent, and accessible data throughout its lifecycle, emphasizing that data integrity controls must be embedded within both manual and electronic systems. The shift towards electronic data management necessitates a risk-based approach to identify vulnerabilities and apply appropriate controls. This method ensures that the integrity of data is preserved, regardless of whether it is managed manually, electronically, or through a hybrid system.

Quality Risk Management (QRM) principles play a crucial role in maintaining data integrity. By assessing the criticality and vulnerability of data, companies can implement targeted controls to minimize the risk of data breaches. The review outlines various strategies, such as implementing robust procedures, conducting regular system tests, and continuous monitoring, which are essential to prevent data integrity issues. Ensuring that all personnel understand and adhere to these practices is critical, as maintaining data integrity is a collective responsibility within an organization.

The review also underscores the importance of regulatory compliance, highlighting that adherence to Good Manufacturing Practices (GMP) is non-negotiable. Companies must stay vigilant in their efforts to protect data from accidental or intentional modification, falsification, or deletion. The establishment of effective data governance policies, routine verification, and periodic surveillance are vital components of a robust quality management system (QMS). Ultimately, the integrity of pharmaceutical data is not only a regulatory requirement but a fundamental aspect of delivering safe and effective products to patients. By adopting a comprehensive, risk-based approach to data integrity, pharmaceutical companies can enhance their manufacturing processes, ensure compliance, and uphold the highest standards of product quality and safety.

References(10pt)

The main references are international journals and proceedings. All references should be to the most pertinent and up-to-date sources. References are written in APA style of Roman scripts. Please use a consistent format for references – see examples below (9 pt):

[1] Parenteral Drug Association. *Technical Report No. 80: Data Integroty Management System for Pharmaceutical Laboratories*; PDA: Bethesda, Md., 2018; p 63.

[2] Parenteral Drug Association *Technical Repor No. 84: Integrating Data Integrity Requirements into Manufacturing & Packaging Operations;* Bethesda, Md., 2020.

[3] U.S. Food and Frug Administration. *Data Integrity and Compliance with cGMP: Questions and Answers, Guidance for Industry*; U.S. Department of Health and Human Services: Silver Spring, Md., 2018.

[4] Medicines and Healthcare produces Regulatory Agency. *'GXP' Data Integrity Guidance and Definitions, Rev. 1:* MHRA: London, 2018.

[5] World Health Organization. *Annex 5: Draft Guidance on Good Dara and Record Management Practices*; WHO: Geneva, 2016 p46.

[6] Parenteral Drug Association. *Technical Reeport No. 54-2: Implementation of Quality Risk Management for Pharm,aceutical and Biotechnology Manufacturing Operations, Annex 1: Case Study Examples for Quality Risk Management in Pakaging and Labeling*; PDA: Bethesda, Md., 2013.

[7] International Conference for Harmonization. *Quality Guideline Q10: Pharmaceutical Quality System*; ICH: Geneva, 2008.

[8] International Conference for Harmonization. *Quality Guideline Q10: Quality Risk Management*; ICH: Geneva, 2005.

[9] U.S. Food and Drug Administration. *21CFR Part 211- Current Good Manufacturing Practice for Finished Pharmaceuticals, Subpart J- Records and Reports*; Government Publishing Office: Washington, D.C., 2005.

[10] U.S. Food and Drug Administration. Part 133- Drugs; Current Good Manufacturing Practice in Manufacture, Processing, Packing, or Holding. *Fed Regist* **1963**, 28 (120, Part II), 6385-87.

[11] U.S. Food and Drug Administration. Current Good Manufacturing Practice in Manufacture, Processing, Packing, or Holding. *Fed Regist* **1978,** 43 (44813, Book2), 45014-336.

[12] U.S. Food and Drug Administration. *FDA Compliance Program Guidance Manual*; 7346.832 (5/12/2010), Pre-approval Inspections. U.S. Department of Health and Human Services: Silver Spring, Md., 2010.

[13] U.S Food and Drug Administration, *21 CFR Part 11, Electronic Records; Electronic Signatures- Scope and Application*; Pharmaceutical CGMPs. Government Publising Office: Washington, D.C., 2003.

[14] F-D-C Reports, Inc. Data Manipulation is Being Uncoverd and Referred for Criminal Investigation. *The Gold Sheet **2007**, 41(4).*

[15] U.S. Food and Drug Administration. 21 CFR 58 Good Laboratory Practice for Nonclinical Laboratory Studies: U.S. Department of Health and Human Services: Washington, D.C., 1978.

[16] Australina Therapeutic Goods Administration. *Data Management and Data Integrity (DMDI)*; TGA: Symonston ACT, Australia, 2017.

[17] International Society for Pharmaceutical Engineering. *GAMP Guide: Records & Data Integrity*; ISPE: Bethesda, Md., 2017.

[18] International Conference for Harmonisation. *Quality Guidance Q12: Technical and Regulatroty Considerations for Pharmaceutical Product Lifecycle Management;* ICH: Geneva, 2017.

[19] European Commission. *Annex 11: Computerised Systems. EudraLex- Volume 4- Good Manufacturing Practice for Medical Products for Human and Veterinary Use*; European Commission: Brussels, 2011.