PDA Points To Consider: Fundamental Concepts in Data Integrity

Bob Buhlmann1.*, Madlene Dole2 and Zena Kaufmann3

Author Affiliations

* Corresponding Author: Bob Buhlmann, Director, Corporate Quality Assurance, Amgen, Inc., One Amgen Center Drive, Thousand Oaks, CA, 91320-1799; e-mail: buhlmann@amgen.com

Executive Summary

The purpose of this document is to describe behaviors, including the elements and controls, to ensure the integrity of GxP data in pharmaceutical manufacturing operations. Fundamental concepts such as ALCOA (attributable, legible, contemporaneous, original, and accurate) and the prevent/detect/respond approach to a data integrity program are defined and discussed. This paper was developed through the Parenteral Drug Association (PDA) Data Integrity Task Force and reviewed and approved by the PDA Regulatory and Quality Advisory Board as well as the PDA Board of Directors.

Data integrity is a significant component of a company’s Quality System, providing foundational assurance of the data a company uses to operate in compliance with regulatory requirements and to demonstrate its products are safe and effective for their intended use. Through data integrity the company recognizes its responsibility to prove the origin, transmission, and content of the company’s data and that data is what it is purported to be. To holistically address Data Integrity, the PDA is developing a set of tools in the form of PDA Technical Reports, PDA Training, Data Integrity Workshops, and Points To Consider documents that can be used by industry to address this serious issue. This document serves as an introduction to that suite of tools to follow.

Purpose

The purpose of this document is to describe behaviors, including the elements and controls, to ensure the integrity of GxP data in pharmaceutical manufacturing operations.

Data integrity is a significant component of a company’s Quality System, providing foundational assurance of the data a company uses to operate in compliance with regulatory requirements and to demonstrate its products are safe and effective for their intended use. Through data integrity the company recognizes its responsibility to prove the origin, transmission, and content of the company’s data and is what it is purported to be To holistically address Data Integrity, the Parenteral Drug Association (PDA) is developing a set of tools in the form of PDA Technical Reports, PDA Training, Data Integrity Workshops, and Points to Consider documents that can be used by industry to address this serious issue. This document serves as an introduction to that suite of tools to follow.

The Importance of Data Integrity throughout the Product Lifecycle

Nearly every GxP activity at a company generates some form of data or documentation, GxP regulations require companies to put systems in place to ensure the completeness and accuracy throughout the lifecycle of these records, including, but not limited to

- Creation and recording
• Processing and transferring
• Use, reporting, replication, and distribution
• Archival, backup, restoration, obsoleting, and retirement

Business processes establish procedures governing the use, correction, and movement of data, ensuring data can be traced throughout every stage of the lifecycle of the data. When data gets processed, the process is to be controlled in a manner ensuring the traceability.

Data and their documentation define the quality, safety, and efficacy of a company’s products on which public health depends. Data is created and processed throughout the lifecycle of a product as described in ICH Q10, Pharmaceutical Quality System, including the development, testing, manufacture, and distribution of products and therapies. The continual improvement of technologies and business requires companies to adapt the processes by which data and data management processes are managed.

Any mishandling of data, even if unintentional, has the potential to jeopardize the quality, safety, and efficacy of the product and ultimately public health.

Current Regulatory Trends and Recent Issues in Data Integrity

Data integrity is to be complete, accurate, and consistent throughout the data lifecycle. The expectations for data integrity have been the same for years. However, it has become far more complex to meet these requirements with the proliferation of electronic systems. There has been a recent increase in the frequency of regulatory citations for non-compliance, resulting in further actions being taken such as refusal to accept new product filings, market withdrawal, and other actions.

In addition, recent data integrity issues worldwide have also highlighted the need to modernize data integrity behaviors.

Data Management Systems Considerations

Data integrity encompasses a holistic approach beyond the review of audit trails to address the risks existing in many processes that would not be detected by review of audit trails. Quality Management Systems are updated to assure consistency with the company’s operational models and current regulatory expectations, especially if there has been a change to increase the level of computerization. Good documentation practices are assessed to assure that there are no additional risks to the integrity of the data. Focus may include both review of the hard copy generated (paper print-out) and audit trails to prevent the improper manipulation or the unintentional mishandling of data. Audit trails are to be designed to be robust, efficient, and easy to understand and detect data integrity issues.

Skills and capabilities of employees are to be sufficient to execute procedures using complex data technology and systems. In addition to training on good manufacturing practice (GMP) practices and procedures, companies should also consider training employees to develop a mindset consistent with an understanding of the differences between an electronic data system and a wholly paper-based system.

Globalization and Cultural Factors

With a global supply chain, it is critical to assure a consistent understanding of the importance of a program throughout the lifecycle of the data. There are to be processes in place to assure transparency and escalation of risks and/or failures of data integrity. It is important to note that all business partners within global supply chains may not be as mature in their GxP understanding, and might not have the infrastructure locally to effectively manage risk of data handling issues. Also, as the number of vendors increase in the supply chain, a risk-based approach can be employed to assure appropriate qualification and continued oversight.

Training is an important way to address these factors. Through training, all employees, especially frontline employees and management, are empowered to raise potential concerns regarding data integrity. Senior management takes data integrity issues seriously when employees raise awareness to senior management. Conduct training for operators on the shop floor, and analysts in quality control
laboratories, to assure complete understanding of how data and documentation is linked to product quality. Conduct training to assure complete understanding of the need to follow procedures, especially as unexpected issues arise during execution of processes.

Elements of Data Integrity

Data integrity is the extent to which all data (electronic, paper-based, or hybrid) are complete, consistent, and accurate throughout the lifecycle of the data. Data defines product quality and ensures public safety. There are basic elements “ALCOA+” (1) to be applied to both the data and the documentation practices, irrespective of the type of system (e.g., paper-based, electronic, or hybrid).

ALCOA describes the requirements for good data management. All data is to be

- A—Attributable to the person generating the data. Information is to be captured identifying the source of the data. For example: Who performed the action and when? If a record is changed, who did it and why?
- L—Legible and permanent. Data is to be recorded permanently in a durable medium and always be readable.
- C—Contemporaneous. Information is to be recorded at the time of data generation or event observation (e.g., at the time the work is performed).
- O—Original record (= a true copy). Data is to be used or presented as when it was created (i.e., the first time).
- A—Accurate. Data is to be verified as correct via repeatable calculation, algorithm, or analysis; there are to be no errors (e.g., correct number of digits).
- +—In addition, data is to be complete, complete, consistent, enduring, and available (2).

Holistic Approach to a Data Integrity Program through the Data Lifecycle

A data integrity program consists of three main elements which protect critical GxP data from accidental or intentional modification, falsification, and deletion. The main elements are

- Prevent
- Detect
- Respond

The best way to prevent data integrity issues is for all levels within the company to take personal ownership and accountability for their own data and documentation. The PDA has developed the elements of a Code of Conduct for Data Integrity in the Pharmaceutical Industry (3), which is available for companies to use in defining expectations for individual ownership and accountability.

The Quality Management System should give consideration to identifying metrics, which measure the effectiveness of data integrity to identify opportunities for improvements.

Prevention
The prevention of data integrity breaches can be addressed with three primary elements: Personnel and Training, a Validation Program, and Security.

**Personnel and Training.**

Data Integrity begins with each employee taking ownership and accountability for their own data and documentation. Company standards of ethical conduct are defined to be followed, assuring that each employee acts with integrity in the execution of their work. Each employee is responsible for the validity and integrity of their data and documentation, whether it is a paper-based or electronic system. Each employee is to understand the requirement to identify, escalate issues, and to report to management if procedures are not followed. For example, employees immediately notify their supervisor of potential breaches of ethical behavior such as (but not limited to) the following:

- Improper data manipulation
- Adjustment of time clocks
- Backdating of information
- Creating records after the fact or without actually executing the procedure
- Excluding adverse information
- Sharing of passwords
- Discarding or destroying original records

Companies are to establish and maintain training programs to assure employees' understand of high standards of ethics and integrity, including a focus on proper data handling and reporting (4). This training program is to include all levels within the company, building this into the company values and code of conduct.

It is imperative that everyone in the company understands they are ultimately responsible for data integrity.

**Validation Program.**

Systems (electronic or paper–based) are to be designed to ensure data is accurate, reliable, and consistent and fit for their intended use (5). Validation of these systems includes the ability to identify data changes and their relation to the intended use of the system throughout the data lifecycle.

For example: A company's computer system validation process, designed to ensure data systems are accurate, reliable, consistent, and fit for their intended use, includes the following elements:

- Identifying data changes and their relation to the intended use of the system
- Backup/restore, copying, and archiving of data
- Electronic record review by supervisory personnel
- Maintenance and review of audit trails
- Security design including segregation of duties
- Periodic review

**Security.**

Programs are designed to assure the integrity of the data both at the physical level (i.e., buildings and rooms) and at the informational level (i.e., systems). Elements of a security program include:

- Requirement for each employee, whether full–time or contract worker, to have a secure access identification (ID) to a company's facility.
- Restriction of access to restricted rooms such as data centers, manufacturing suites, and document storage centers to authorized personnel.
• Granting of access to GxP computer applications only to authorized personnel.
• Requirement for employees to log on to a computer system and the relevant data application software using only their uniquely assigned login ID and password.
• Requirement for employees to log off or lock a computerized system when their use is complete, and to secure unattended computer terminals.
• Control of computers to assure computers automatically lock and/or log off when the computer is inactive for a predetermined time period.
• Requirement for employees to change their password immediately if the possibility exists that the security of the password has been compromised.
• Requirement for passwords to be changed on a predetermined frequency.

External providers of software computer services are to meet the requirements set forth by internal company policy and procedures. Use of contractors and vendors for GxP services, including but not limited to clinical trial management, analytical testing, and contract manufacturing, are to include requirements for these suppliers to meet requirements to assure data integrity.

Quality agreements are to provide roles, responsibilities, and expectations for supplier services, requiring suppliers to notify the company of any significant issues affecting data integrity.

Detection

There are two primary controls used to detect data integrity issues: Audits and Data Review.

Audits.

Companies are to establish and maintain a risk–based audit program to assess the continued state of compliance of its data integrity program (6). GxP audits are to be performed by trained and qualified auditors, who focus on adherence to company operating standards and procedures. Auditors have knowledge and/or have completed special training on how to check the security and integrity of paper and electronic GxP:

• Compliance of employees with policies, procedures, and established controls.
• Compliance of standard operating procedures (SOPs) with existing and emerging regulations and current practice.
• Continued proper functioning of all systems.

Data Review and Audit Trails.

The essential characteristics of good data are defined by the company's Quality Management System (QMS) under the good documentation policy.

Audit trails are reviewed based on the intended use and risk associated with each system (7). There are two primary types of audit trails:

System configuration audit trail:

• Tracks actions of system administrator.
• Tracks changes to "rules" for operating the system.
• Is reviewed as part of the system periodic review process.

Data audit trail:

• Tracks actions of users, reviewers, and approvers.
• Tracks changes to data.
• Is reviewed when the data is reviewed (includes data and meaningful metadata).

Procedures to review data are system-specific in that each computerized system is to define what data to review and when to review it. When electronic reviews are not available, other means of reviews can occur. These may include equipment use logs, security logs to check access to restricted areas, or a two-person review of critical transcribing or recording of information.

Response

There are three primary areas through which responses to data integrity issues are managed: governance, findings and investigations, and corrective and preventive actions (CAPAs).

Governance.

Companies establish and maintain processes and procedures to define how data systems are designed, validated, and maintained. Company governance identifies opportunities to drive efficiencies, share best practices, simplify processes, and resolve issues across the company.

• As part of the Quality Management Review identified in ICH Q10 Pharmaceutical Quality Systems, the metrics of the data integrity program can be reviewed to assure the program remains in a state of control and to identify areas of improvement and compliance.
  ◦ Key quality performance indicators.
  ◦ Assessment of data trends.

Data Integrity Findings and Investigations.

Employees are to report potential issues resulting from non-compliance from GxPs, procedures, or company standards (8). These reports may be generated from different sources. For example, potential issues may be captured through the quality system or through an anonymous report received by a company’s business conduct hotline. Any report involving potential data integrity concerns are to be documented and reviewed by a multidisciplinary team to determine if it requires further investigation.

Investigation into potential data integrity reports is a formal process and requires the following considerations:

• Careful examination of the facts.
• Discussion and outline of an investigation plan.
• Guidance from compliance, human resources (HR), or the legal department, as required.
• Documentation of the investigation using the nonconformance system.
• Conduct of investigation consistent with procedures applicable to quality investigations.

Any investigation encompassing aspects of quality and confidential HR matters is to be documented on both systems. If necessary, HR may issue a memorandum confirming that a formal investigation has been conducted without disclosing confidential information.

Corrective and Preventive Actions (CAPAs).

Any effective data integrity program includes a way to monitor and assess actions taken to resolve past or potential nonconforming conditions. The CAPA system uses objective indicators to analyze the measures taken to ensure the resolution of nonconforming conditions. CAPA activities are communicated to the responsible parties and company management, as required.

Conclusion

Data Integrity is a significant component of the Quality Management System, providing foundational assurance to stakeholders that a company operates in
compliance with regulatory requirements, its data systems can be trusted, and therefore that its products are safe and effective for their intend use.

Data integrity problems can emanate from many sources, from electronic records to paper-based systems—or combinations of the two. They can be unintentional—driven by human error—or intentional.

Inspectors around the world have made it very clear that good intentions are no defense against compromised data. Whatever their causes, issues with data integrity continue to be identified by global regulatory authorities and continue to be of concern to senior management. Individuals at all levels need to take action to build an organizational quality culture capable of preventing, detecting, and responding to these issues.

Additional PDA resources related to data integrity can be found on its website at pda.org/dataintegrity.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Appendix

View this table: In this window  In a new window

Appendix: Glossary of Data Integrity Terms

© PDA, Inc. 2016

References