PDA
Parenteral Drug Association

Technical Report No. 84

Integrating Data Integrity Requirements into Manufacturing & Packaging Operations

Integrating Data Integrity Requirements into Manufacturing & Packaging Operations

Authors

Els Poff, Merck (Chair)

James Curry, PhD, Teva Pharmaceuticals

John Grealis, PhD, Novartis

Anne Pericone, Johnson & Johnson

Susan Schniepp, Regulatory Compliance Associates Inc.

Nader Shafiei, PhD, Sanofi

Ronald Tetzlaff, PhD, Parexel Consulting

Anthony Warchut, AC Warchut GMP Consulting

Contributors

Jeffrey Broadfoot, Emergent BioSolutions, Inc.

Derek Glover, Mylan

Maryann Gribbin, Faith & Royale Consultants

Tina Morris, PhD, American Association of Pharmaceutical Scientists

Rebecca Parrilla, U.S. Food and Drug Administration

Carmelo Rosa, PsyD, U.S. Food and Drug Administration

Anil Sawant, PhD, Merck

Christopher Smalley, PhD, ValSource, LLC

Integrating Data Integrity Requirements into Manufacturing & Packaging Operations

Technical Report No. 84

ISBN: 978-1-945584-19-0

Table of Contents

FIGURES AND TABLES INDEX

1.0 Introduction and Scope

Data integrity is the cornerstone of establishing and maintaining confidence in the reliability of the data that assures product quality and patient safety. The reliability of manufacturing production and control data depends on the procedures, systems, processes, and controls in place to ensure data integrity. In production, these controls start at the point of data creation and continue through the entire data lifecycle, including the storage of data and the ability to retrieve it later to support the quality of the products manufactured.

The term "data integrity" has evolved to denote the degree to which data are complete, consistent, enduring, and available (ALCOA+) as well as the degree to which the characteristics of the data are maintained for all operations throughout the data lifecycle. Pharmaceutical manufacturers need to ensure that relevant data are available to document and provide traceability to what occurred, that the data are attributable to the person who performed the activity and entered the data, and that the data cannot be deleted, omitted, or in any way modified to misrepresent what occurred. All breaches of data integrity, whether intentional or unintentional, must be investigated.

Advances in information technology and in-process monitoring sensors, coupled with lower costs of computer memory and better processors, has resulted in explosive growth in electronic data generation, acquisition, and storage. Applying a one-size-fits-all approach to data integrity controls established on principles developed decades ago may be neither valuable nor, in certain instances, feasible. Therefore, the use of a risk-based approach is essential to developing a robust data integrity program, considering the requirements from a data-lifecycle perspective. Risk-based concepts apply even as industry transitions from manual documentation systems to fully electronic or hybrid (manual and electronic) systems.

This technical report addresses data integrity from the perspective of manufacturing operations. It discusses regulatory trends, risk management concepts, and recommendations for implementing appropriate data integrity controls in manufacturing operations applicable to paper-based, electronic-based and hybrid systems. The case studies included in this technical report provide examples of how to assess current data integrity risks and implement the concepts presented here.

1.1 Purpose

The continuous and rapid advances in automation and information technology, availability of economical data storage, and superiority of electronic audit trail capabilities over paper records have compelled the pharmaceutical industry to rethink good manufacturing practices (GMP) controls. Among the consequences is a heightened awareness of the need to establish and maintain effective data integrity controls at every stage of the manufacturing process for drug products. While the requirement to maintain accurate and complete data is well recognized by industry, what is not universally understood is the level of data integrity control needed at each step to comply with GMP regulations. Many companies continue to struggle when deciding what controls are appropriate for each manufacturing operation and what levels of review and verification are necessary to ensure reliable manufacturing control data. This technical report describes an approach using quality risk management (QRM) for establishing and assessing the appropriateness of data integrity controls for each manufacturing operation based on the criticality and vulnerability of the data for its intended use.

Developed by subject matter experts from global industry and regulatory agencies, this technical report summarizes manufacturing data integrity risks and identifies best practices that can be used to develop and sustain robust documentation as well as data integrity management procedures, systems, processes, and controls. Employing these practices will help users achieve compliance with applicable laws, regulations, and directives for pharmaceutical products such as active pharmaceutical ingredients (APIs), solid oral dosage forms, sterile injectables, biologics, and vaccines.

Assuring data integrity is an organizational responsibility. Employees at any facility that manufactures, processes, packages, or holds a finished pharmaceutical, intermediate ingredient, or API are responsible for ensuring that data collected throughout the manufacturing process are accurate and reliable. Managers, quality assurance personnel, operators, technicians, and support staff alike must

remain aware of the significance of maintaining and documenting data integrity for the quality and safety of their products.

1.2 Scope

The information in this technical report applies to the management of data at pharmaceutical facilities that manufacture, process, package, or hold a finished pharmaceutical, API, or intermediate. Specifically, it addresses data pertaining to manufacturing operations, materials, facilities and equipment, production, and packaging and labeling, including in-process controls and process analytical testing. It also applies to the procedures, systems, processes, and controls used at a drug facility to ensure that the drugs conform to applicable laws, regulations, and directives and that the data support the drug's identity, strength, quality, and purity.

The methods and processes described here can be applied to facilities that manufacture drugs intended for use both in clinical trials and for commercial distribution. The principles may be extended to facilities engaged in other activities (such as distribution of finished products to customers) or products (such as components, raw materials, medical devices, and combination products), though these were not a principal consideration. This technical report is not intended to apply to data integrity management in clinical practice and the implementation of clinical trials. Data integrity management in laboratory systems is discussed in PDA *Technical Report No. 80: Data Integrity Management System for Pharmaceutical Laboratories* ***(1)***, and data integrity management in quality management systems will be discussed in a future technical report.

2.0 Glossary and Abbreviations

Audit Trail

FDA

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)***.

MHRA

Metadata containing information associated with actions that relate to the creation, modification or deletion of GXP records. An audit trail provides for secure recording of life-cycle details such as creation, additions, deletions or alterations of information in a record, either paper or electronic, without obscuring or overwriting the original record. An audit trail facilitates the reconstruction of the history of such events relating to the record regardless of its medium, including the "who, what, when and why" of the action ***(3)***.

WHO

The audit trail is a form of metadata that contains information associated with actions that relate to the creation, modification or deletion of GXP records. An audit trail provides for secure recording of life-cycle details such as creation, additions, deletions, or alterations of information in a record, either paper or electronic, without obscuring or overwriting the original record ***(4)***.

Audit Trail Review Assessment (ATRA)

A tool that can be used to help determine what elements within the audit trail should be reviewed, and the frequency at which the review should take place for each part of the audit trail where a review is required.

ALCOA+

Attributable

It should be possible to identify the individual or computerized system that performed the recorded task. The need to document who performed the task / function is, in part, to demonstrate that the function was performed by trained and qualified personnel. 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.