



## DATA INTEGRITY: AN OBLIGATORY TOOL TO SURVIVE PHARMA INDUSTRY

Sunita Sunil Gagare<sup>1\*</sup>, Sunil Krushna Gagare<sup>2</sup> and Dr. Ashish Suresh Jain<sup>1</sup>

<sup>1</sup>Shree D. D. Vispute College of Pharmacy and Research Center, New Panvel.

<sup>2</sup>Quality Assurances Department, Cipla Pvt Ltd.

**\*Corresponding Author: Sunita Sunil Gagare**

Shree D. D. Vispute College of Pharmacy and Research Center, New Panvel.

Article Received on 07/12/2018

Article Revised on 28/12/2018

Article Accepted on 18/01/2019

### ABSTRACT

Medicines and health products are important for addressing health problems and improve quality of lives. They form an indispensable component of health systems in the prevention, diagnosis and treatment of disease and in alleviating disability and functional deficiency. All regulatory bodies (e.g. USFDA, WHO, MHRA) are supporting countries in ensuring equitable access to essential medicines and other health products that are safe, effective and of assured quality. For assured quality the manufacturing should be carried out according to cGMP. The regulatory bodies regularly practice audits and inspections to know cGMP followed or not by respective industries. The assurance is done by auditing data retained by respective industries. Therefore data retained must be integrated.

**KEYWORDS:** cGMP, ALCOA, data integrity, warning letters.

### INTRODUCTION

Consumers have right to get drugs that they are consuming to be safe and effective. To ensure the same pharmaceutical industries are governed by various laws and regulatory bodies. The regulatory bodies have set certain standards to assure the quality of drugs. The main regulatory standard for ensuring pharmaceutical quality is the current Good Manufacturing Practice (cGMP). It's important to assure safety and efficacy of medicines by manufacturing them under cGMP requirements e.g. Facilities that are in good condition, equipment that is properly maintained and calibrated, employees who are qualified and fully trained and processes that are reliable and reproducible. Finally how the regulatory bodies come to know that every process or step is done according to cGMP? And answer is through inspections

and verification of data retained by the respective industry. To retain data there is again some amendment have been done in cGMP. The data retained should be integrated there for another term gets introduced Data integrity.

As per FDA *data integrity* refers to the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be attributable, legible, contemporaneously recorded, original or a true copy, and accurate (ALCOA).

Data integrity refers to maintaining and assuring the accuracy and consistency of data over the entire data life cycle. (Fig.1).



**Figure 1: Data Life Cycle.**

It is measure of extent to which all data are complete consistent and accurate throughout the data lifecycle.

#### 1. Basic Principle of data integrity is 'ALCOA'

**1.1 Attributable** means- clearly indicate who records the data or performed the activity. The data should be signed and dated. Who wrote the document and when should be mentioned. It is must be possible to

read/interpret data after it is recorded. In other words, knowing where the data originated from and identifying the person who did the work or entered the data's origin.

**1.2 Legible** means data should be permanent, No unexplained, hieroglyphics, properly corrected if required. It also means presenting the data in a clear, readable way. If changes are there in the data, both the new and old values can be reviewed

**1.3 Contemporaneous** means data must be recorded at the time generated, close proximity to location where data generated. The data entered at the time or as close to possible when the activity occurred.

**1.4 Original-** Data must be preserved in unaltered state, if not it is explained as to why not, certified copies. Inclusion of the earliest record in all data which should not be obscured by following records.

**1.5 Accurate-** Data must be correctly reflected the action/observation made. Data checked where necessary. Modifications explained if not evident. Valid representation of results from a data source and ensuring that all corrections are recorded and acceptable explanations are provided for why changes took place

## 2. Some Concepts in data integrity

Before discussing about data integrity at glance certain terms, concepts used in data integrity must be known.

### 2.1 Metadata

Metadata is the contextual information required to understand data. A data value is by itself meaningless without additional information about the data. Metadata is often described as data about data. Metadata is structured information that describes, explains, or otherwise makes it easier to retrieve, use, or manage data. For example, the number is meaningless without metadata, such as an indication of the unit “mg.” Among other things, metadata for a particular piece of data could include a date/time stamp for when the data were acquired, a user ID of the person who conducted the test or analysis that generated the data, the instrument ID used to acquire the data, audit trails, etc.<sup>[2]</sup>

Data should be maintained throughout the record's retention period with all 88 associated metadata required to reconstruct the CGMP activity (e.g., §§ 211.188 89 and 211.194). The relationships between data and their metadata should be 90 preserved in a secure and traceable manner. Metadata is data that describe the attributes of other data, and provide context and meaning. Typically, these are data that describe the structure, data elements, interrelationships and other characteristics of data. It also permits data to be attributable to an individual. CDER-OMQ\_CGMP\_Guidance\_Plenary\_3-20-2017\_S508.pdf.

### 2.2 Audit trail

For purposes of this guidance, *audit trail* means 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. An audit trail is a chronology of the “who, what, when, and why” of a record. For example, the audit trail for a high performance liquid chromatography (HPLC) run could include the user name, date/time of the run, the integration parameters used, and details of a reprocessing, if any, including change justification for the reprocessing.

Electronic audit trails include those that track creation, modification, or deletion of data (such as processing parameters and results) and those that track actions at the record or system level (such as attempts to access the system or rename or delete a file).

CGMP-compliant record-keeping practices prevent data from being lost or obscured (see §§ 211.160(a), 211.194, and 212.110(b)). Electronic record-keeping systems, which include audit trails, can fulfill these CGMP requirements.<sup>[2]</sup> GMP audit trails are metadata that are a record of GMP critical information (for example the change or deletion of GMP relevant data), which permit the reconstruction of GMP activities. Where computerized systems are used to capture, process, report or store raw data electronically, system design should always provide for the retention of full audit trails to show all changes to the data while retaining previous and original data. It should be possible to associate all changes to data with the persons making those changes, and changes should be time stamped and a reason given. Users should not have the ability to amend or switch off the audit trail. The relevance of data retained in audit trails should be considered by the company to permit robust data review / verification. The items included in audit trail should be those of relevance to permit reconstruction of the process or activity. It is not necessary for audit trail review to include every system activity (e.g. user log on/off, keystrokes etc.), and may be achieved by review of designed and validated system reports. Audit trail review should be part of the routine data review / approval process, usually performed by the operational area which has generated the data (e.g. laboratory). There should be evidence available to confirm that review of the relevant audit trails have taken place. When designing a system for review of audit trails, this may be limited to those with GMP relevance (e.g. relating to data creation, processing, modification and deletion etc). Audit trails may be reviewed as a list of relevant data, or by a validated ‘exception reporting’ process. QA should also review a sample of relevant audit trails, raw data and metadata as part of self inspection to ensure ongoing compliance with the data governance policy / procedures. If no audit trailed system exists a paper based audit trail to demonstrate changes to data will be permitted until a fully audit trailed (integrated system or independent audit software using a validated interface) system becomes available.

### 2.3 Backup Data

A copy of current (editable) data, metadata and system configuration settings (variable settings which relate to an analytical run) maintained for the purpose of disaster recovery. Backup and recovery processes must be validated. Action plan in case of disaster should be ready.

### 2.4 Original record

Data as the file or format in which it was originally generated, preserving the integrity (accuracy,

completeness, content and meaning) of the record, e.g. original paper record of manual observation, or electronic raw data file from a computerised system.

### 2.5 True Copy

An exact verified copy of an original record. Data may be static (e.g. a 'fixed' record such as paper or pdf) or dynamic (e.g. an electronic record which the user / reviewer can interact with).

Original records and true copies must preserve the integrity (accuracy, completeness, content and meaning) of the record. Exact (true) copies of original records may be retained in place of the original record (e.g. scan of a paper record), provided that a documented system is in place to verify and record the integrity of the copy.

It is conceivable for raw data generated by electronic means to be retained in an acceptable paper or pdf format, where it can be justified that a static record maintains the integrity of the original data.

However, the data retention process must be shown to include verified copies of all raw data, metadata, relevant audit trail and result files, software / system configuration settings specific to each analytical run, and all data processing runs (including methods and audit trails) necessary for reconstruction of a given raw data set. It would also require a documented means to verify that the printed records were an accurate representation. This approach is likely to be onerous in its administration to enable a GMP compliant record. Many electronic records are important to retain in their dynamic (electronic) format, to enable interaction with the data. Data must be retained in a dynamic form where this is critical to its integrity or later verification. This should be justified based on risk.

### 3. Causes of data integrity and challenges

- 3.1 **Lack of Awareness:** In Pharma industries people are working with different qualifications at different levels as per requirement of work done. As many persons are not from Pharma background by profession they may not aware that they are dealing with health of peoples.
- 3.2 **Training ineffectiveness:** Most of the time training is carried out with certain assumptions or without modifications in traditional methods.
- 3.3 **Shortage of Manpower:** Most of the time this may not be issue for data integrity as all industries prefer to provide sufficient manpower. Sometimes there may be delay in recruitment of new employee at the place of relived employee that creates mess.
- 3.4 **Quantity over quality:** According to market demand there is continuation of production of medicines too. If market demand gets increased to meet the market demand this issue can arise.
- 3.5 **Poor management support:** Sometimes management does not support or develop data integrity policies may be due to other issues.

### 4. Solutions for problems of Data Integrity:

#### 4.1 Systems should be designed in a way that encourages compliance with the principles of data integrity.

Written Procedure (SOP) should be there for every action. Access to clocks for recording timed events. Accessibility of batch records at locations where activities take place so that ad hoc data recording and later transcription to official records is not necessary. Automated data capture or printers attached to equipment such as balances. Proximity of printers to relevant activities

#### 4.2 Control over blank paper templates for data recording.

In ideal data integrity practice blank paper should not be used. But if it is used create control through the limiting use by specifying the maximum number can be used should be as formatted with serial number and documented. Access to be limited for pdf to word conversion and documented.

#### 4.3 Preparation of SOPs

Data handling SOPs should be designed. For data destruction or deletion reasons should be given or can make SOP for the same. Path forward of the organization should be clear in case of data integrity and it should be very clear in SOPs.

#### 4.4. Validated

Pharmaceutical industry should practice with validated System, Process, Procedure and Equipment.

#### 4.5 Computerized system asses should be limited through authorized person.

So as to the authorized person will be responsible for data deletion or any change in data or violation of data. Design software which is sophisticated as well as user friendly and nobody can make deletion or editions once data get generated. Computerized system configuration settings should be defined, tested, 'locked' and protected from unauthorized access as part of computer system validation. Only those variable settings which relate to an analytical run would be considered as electronic raw data. User access rights which prevent (or audit trail) data amendments.

#### 4.6 Training Effectiveness

Training should be effective. The training records should be maintained. The non technical staff also should be included in basic training or special training programs should be designed. Make all people aware about they are directly or indirectly dealing health of peoples and patients. Retraining and effectiveness require for elucidation.

#### 4.7 Protocol Preparation

Always plan your work then start performing. Mainly in quality control laboratories. Make list of priorities then ensure it then start the analysis so as to there will not be

any overlay of two different analysis on one instrument so as to there will not be any case of withdrawal of analysis.

#### 4.8 Who can be a Part of Data Integrity?

From higher management authority to the sweeper or office boy everyone should be a part of data integrity. Each and every person who is working directly or indirectly for industry should be aware about data integrity and its importance. Also convince to raw material suppliers to do so.

#### 4.9 Audit trail

Data should be secured and should not have the option to edit or delete. In audit trail record following information should be recorded.

1. Date and time
2. Name of person making change
3. Original and changed value
4. Reason for change made with justification.
5. Invalid attempts to log on the system should also be recorded in the audit trail.

#### 4.10 Organizational policy on Data Integrity

Every organization should support for

- Zero Tolerance
- Oath from each employee.
- No falsification of data
- Good Documentation Practices.
- Reconciliation of Issuance, Archival and Destruction.
- Contemporaneous documentation.
- Secured computerized / non-computerized systems.
- Periodic audit to detect data integrity issues.
- Investigation, impact assessment & CAPA for any data integrity issues identified.
- Respect to the quality functions and decisions, high degree of acknowledgement.
- Provide adequate number of staff.
- Software support to reduce / eliminate manual interventions for QMS.
- Controlled Systems for data storage and archival.

#### 5. Some Data integrity issues arise during US FDA audits at certain Pharmaceutical industries

The given table shows rational and warning letter no. (Warning letters are available on US FDA website <https://www.fda.gov/>).

| Sr. No | Rationale  | Warning Letter No   |
|--------|--|---|
| 1.     | Failure to exercise sufficient controls over computerized systems to prevent unauthorized access or changes to data, and to provide adequate controls to prevent omission of data.                                   | 320-16-07, 320-16-12, 320-16-29(21CFR211.68(b), 320-16-19                                     |
| 2.     | Failure to have laboratory control records that include complete data derived from all laboratory tests conducted to ensure compliance with established specifications and standards.                                | 320-16-31, 320-17-05  |
|        | Failure to maintain complete data derived from all laboratory tests conducted to ensure compliance with established specifications and standards.  | 320-17-03, 320-17-01,320-17-13. 320-16-26, 320-16-24  |
|        | Failure to maintain complete data derived from all laboratory tests conducted to ensure compliance with established API specifications and standards.  | 320 -17-04  |
|        |  | 320-17-13 (21CFR211.194(a))   |
|        |  | 320-16-26   |
|        | Written procedure for  |   |
|        | Cleaning and maintenance of equipment-21 CFR 211.67(b).  | 320-16-36   |
|        | for production and process controls, including validation protocols and reports,   | 320-16-37   |
| 3.     | 21 CFR 211.113(b), for the preparation of master production and control records designed to assure uniformity from batch to batch. (21 CFR 211.186(a))   | 320-17-01   |
|        | written procedures that are designed to prevent microbiological contamination of drug products purporting to be sterile, and that include validation of all aseptic and sterilization processes (21 CFR 211.113(b)). | 320-17-13   |
|        | and responsibilities applicable to the quality control unit. (21 CFR 211.22(d))  | 320-17-12   |
| 4.     | Failure to prevent unauthorized access or changes to data, and to provide adequate controls to prevent manipulation and omission of data.  | 320-17-02, 320-16-26, 320-16-13, 320-16-11, 320-16-24, 320-17-04, 320-17-13(21CFR 211.68(b)), |
| 5.     | Data Integrity Remediation   | 320-16-13, 320-16-29, 320-17-04,  |

|    |  |  |
|----|--|--|
|    |  | 320-17-05, 320-17-13, 320-16-26, 320-16-24, 320-16-32, 320-17-32, 320-17-03, 320-16-31, 320-17-02, 320-17-01 |
| 6. | Failure to record activities at the time they are performed.   | 320-16-26, 320-16-24   |
|    | Failure to record activities at the time they are performed, and destruction of raw data.              | 320-16-11  |
|    | Failure to record activities at the time they are performed, and destruction of original records.      | 320-17-13  |
|    | Failure to ensure that all quality-related activities are recorded at the time they are performed.     | 320-17-03  |
|    | Failure to document manufacturing operations at the time they are performed.                           | 320-16-19  |
| 7  | Failure to maintain training records of employees involved in the manufacture of intermediates or API. | 320-16-27  |

### CONCLUSION

Data integrity is most imperative an inescapable tool to meet cGMP requirements. Pharma industries are adopting and developing work culture accordingly. It is mandatory to endure and to be competent in market for Pharma industry to espouse Data Integrity and its requirements.

### REFERENCES

1. Loren Smith, Agilent Technologies, Inc. Santa Clara, CA USA Data Integrity in Pharmaceutical Quality Control Laboratories: What You Need to Know.
2. Food and Drug Administration Data Integrity and Compliance with CGMP Guidance for Industry. U.S. Department of Health and Human Services, April 2016.
3. Sarah Barkow, Karen Takahashi, Current expectations and guidance, including data integrity and compliance with CGMP Center for Drug Evaluation and Research March 30, 2017 Society of Quality Assurance Annual Meeting National Harbor, MD.
4. MHRA GMP Data Integrity Definitions and Guidance for Industry March 2015.
5. Guidance for Industry Quality Systems Approach to Pharmaceutical CGMP Regulations.