Guidelines for Data integrity practices

Document Version: 1.01
Document Number: OLS-06-28G-Data Integrity-Guidelines

Release Date: 28-Aug-2020
Effective Date: 04-Sep-2020

A Larsen & Toubro Group Company

Document Authorization

Role	Name	Signature	Date
Author			
Compliance Lead	Swati Kochukulam	Refer to e mail authorization	
Reviewer			
Compliance Manager	Anjana Gopalakrishnan	Refer to e mail authorization	
Approver			
Compliance COE - Head	G S Vijayakumar	Refer to e mail approval	

Note: Refer to the e mail approval attached at the end of this document.

Document History

Version	Change Description	Author	Date
1.00	*Initial version*	*Swati Kochukulam*	*17 Apr 2020*
1.01	*Document title updated from OLS_06_27G_Data Integrity_Guidelines to OLS-06-28G-Data Integrity-Guidelines*	*Swati Kochukulam*	*26 Aug 2020*

Table of Contents

List of Tables
No table of figures entries found.

List of Figures
No table of figures entries found.

1 Introduction

Ensuring Data Integrity is an important component of industry's responsibility to ensure the safety, efficacy, quality etc., of drugs and devices and the Regulators ability to protect the public health. The impact of records and data integrity issues can be significant for a regulated company.

Data integrity refers to the completeness, correctness, consistency, accuracy etc., of data according to the ALCOA principles. Data integrity is critical throughout the data life cycle including creation, modification, processing, maintenance, archival, retrieval, transmission of data and disposition of data after the record's retention period ends. System design and controls shall enable easy detection of errors, omissions and aberrant results throughout the data's life cycle.

1.1 Objective

To provide guidelines for Data Integrity compliance as per Regulatory requirements for the GXP applications and services rendered in this area for Life sciences projects of L&T Infotech (LTI).

1.2 Scope

The scope covers all GXP applications, services and support rendered for systems in the GXP area as part of projects executed in the Life Sciences business of LTI. The scope includes primarily the electronic records that are generated by the systems that are developed or supported as well as those documentations and records generated as part of the development lifecycle of the systems.

1.3 Roles and Responsibilities

- **All resources of Life Sciences account:**
  Are responsible for ensuring data integrity as per the processes that they work on and adoption of the guidelines and carry out the practices defined in this guideline.

- **Project Managers:**
  Are responsible to ensure that appropriate personnel are trained on this procedure and that it is followed in all GxP projects executed.

- **Compliance COE:**
  Responsible for ensuring resources are periodically trained on Data integrity guidelines and verification of adherence to Data integrity related practices.

2 Terms and Abbreviations

Term/Abbreviation	Description
GDP	Good Documentation Practice
cGxP	Current Good X (Manufacturing, Clinical, Lab) practices
ALCOA plus	Attributable, Legible, Contemporaneous, Original, Accurate, Consistent, Enduring, Available, Complete, Credible, Corroborated.
DI	Data Integrity
COE	Centre of Excellence

3 Guidelines

- Definition of data includes all original records and true copies of original records, including source data and metadata and all subsequent transformations and reports of these data, which are generated or recorded at the time of the GXP activity.
- The purpose of data integrity practices is to enable confidence in the quality of data to allow full and complete reconstruction and evaluation of the GXP activities performed.
- Key concepts described by ALCOA and ALCOA+ principles shall be applied throughout the data life cycle
- Data should be accurately recorded by permanent means at the time of the activity.
- Data may be contained in paper records (such as worksheets and logbooks), electronic records, audit trails, photographs, microfilm or microfiche, audio- or video-files.
- Data integrity requirements are applicable to both paper and electronic data and records
- Date, time and time zones of all software's and computer systems used in GxP data recording and processing should be synchronized and controlled and should not be changed without authorization.
- Processed and computer- generated data must have appropriate authorization of the Author, reviewer and approver.
- Data migration/ transfer shall be validated wherever applicable to ensure data integrity, throughout the data life cycle.
- Unique usernames and passwords should be used for systems as appropriate.
- Login credentials should not be shared.
- Access and privileges should be in accordance with the responsibility and functionality of the individual with appropriate controls to ensure integrity (e.g. no modification, deletion or creation of data outside the application is possible).
- Training to personnel should be given to detect data integrity issues and must have the education, training, and experience, or any combination thereof, to perform their assigned duties.
- Appropriate segregation of duties should be applied. Account privileges should be limited to those required for individuals to perform their duties e.g, users, supervisors, administrators, quality team etc.,

- Elevated privileges permitting activities such as data deletion, database amendment or system configuration changes should not be assigned to individuals with a direct interest in the data
- Wherever possible, automated data capture techniques should be applied to minimize data transcription errors
- Appropriately controlled and synchronized clocks should be available for recording timed events
- It is not acceptable to record data on pieces of paper that will be discarded after the data are transcribed to a permanent laboratory notebook.
- Similarly, it is not acceptable to store data electronically in temporary memory, in a manner that allows for manipulation, before creating a permanent record.
- Data integrity is under-pinned by well documented, validated GXP computerized systems and the application of appropriate controls throughout both the system and data life cycles
- Multiple GXP systems may be involved in supporting a data life cycle, as the data may be passed from one system to another. To ensure data integrity all GXP computerized systems should be trustworthy and validated for intended use.
- Specific areas impacting data integrity, which have been of particular regulatory focus and concern include:
    - Lack of basic access controls and security measures allowing unauthorized changes
    - Shared user logins
    - Missing or disabled audit trails
    - Lack of contemporaneous recording of activities
    - Failure to investigate data discrepancies
    - Testing into compliance
    - Incomplete collection, retention and review of data for quality decisions
    - Overwriting of deletion of original data
    - Data falsification
- Data which is manually recorded requires high level of supervision. Supervisory measures or technical controls should be considered to reduce risk.
- Records should be accessible at locations where regulated activities take place. Adhoc data recording and later transcription to official records should be discouraged.
- GXP systems should be validated for intended use and supporting infrastructure qualified

3.1 Software or Application development process

- Data integrity should be enforced into the design of any GXP IT solution i.e., data integrity by design. In addition to 21 CFR Part 11 requirements, the User Requirements Specifications or equivalent document should include data integrity requirements for critical data
- Record and data integrity should be built-in and maintained throughout the GXP system life cycle phases, from concept to project and from operations to retirement. The GXP system life cycle activities should be scaled based on the complexity and novelty of the system, and potential impact on product quality, patient impact and data integrity

- The Functional requirements specifications or equivalent document should define roles and access rules, reporting requirements which should include username, time stamps of generation, any information that could facilitate review etc.,
- The Software Design document or equivalent should include back-up and restore strategy, role definitions, security rules, password management, inactivity rules, audit trails, event logs etc., Systems should be designed to ensure that the execution of critical steps is recorded at the same time as they are performed and are individually traceable. Audit trails are required when users create, modify or delete regulated records during normal operation. The reason for change or deletion of regulated data should be documented and be consistent with regulatory expectations. Audit trail functionality should be available, enabled and verified.
- Functional testing should consider demonstrating the reliability of system features enabling compliance to data integrity through
    - Access testing
    - Back-up and restore testing
    - Audit-trail testing

3.2 Data integrity and Data review

- To ensure compliance to data integrity principles, the following data integrity control should be implemented
    - Review of audit trail
    - Review of events/ logs of the system
- Any audit trail should capture the following information
    - User ID
    - Date and time of actions
    - User action taken
    - Detail of change and record of original entry in case of any change
    - Reason for modifications or deletions as applicable
- The need for and extent of audit trail review should be based on a documented and justified risk assessment. Audit trail review is mandated for Regulated critical systems

3.3 Data Life cycle aspects

- Data transfer and migration should be designed and validated to ensure that data integrity principles are maintained.
- Copies of records should preserve the integrity of the original record.
- Back-up and recovery processes should be validated and periodically tested.
- Security controls should be in place to ensure data integrity of the record throughout the data retention period. Security controls should be validated where appropriate
- Archival arrangements should be established for the long-term retention of regulated data in compliance with legislation. The procedures for destruction of data should consider data criticality and any appropriate regulatory or legal requirements
- The physical location where the data is held, including the impact of any laws applicable to that geographic location should be considered.
- Data should be readily available through the retention period in accordance with defined and verified processes and approved procedures

- The relationships between data and associated metadata required to maintain GXP content and meaning, should be preserved securely to support future queries or investigations including reconstruction of GXP activities

3.4 Human factors in Data integrity

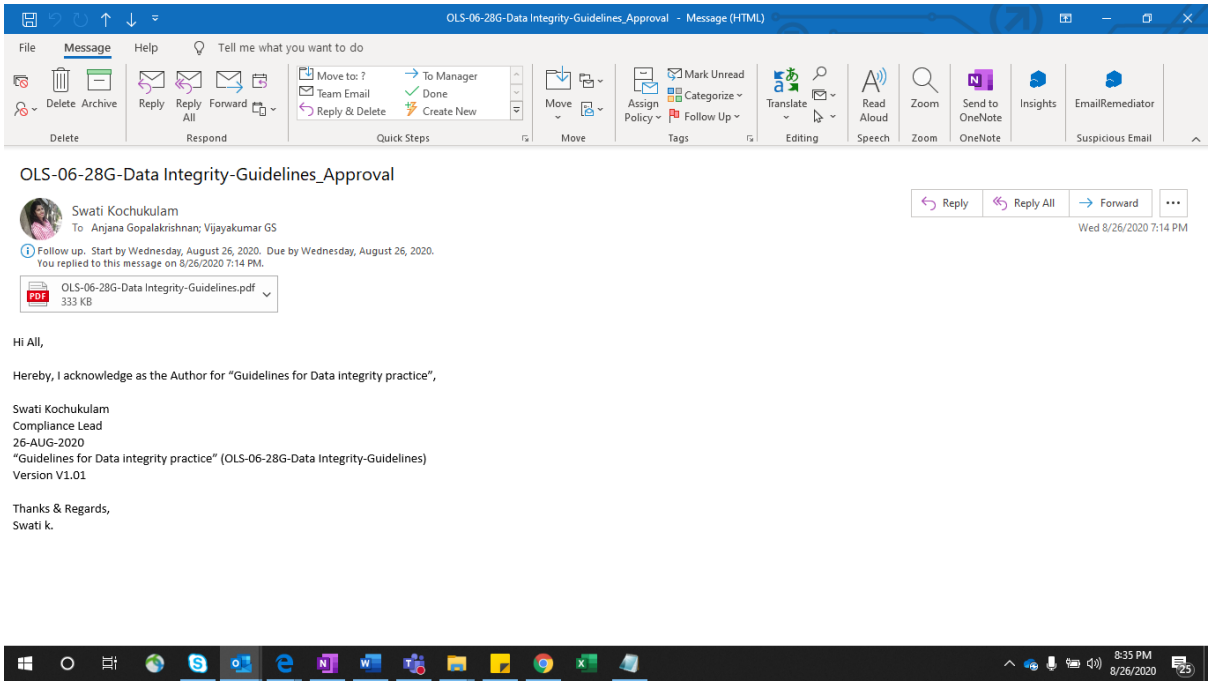
- Consideration of human factors is critical for effective data integrity
- Management should help employees to achieve the openness around data integrity that is needed for compliance
- Data integrity could often arise from genuine human error; however, regulators do not distinguish between human error and data falsification when assessing the impact of data integrity failure
- Personal gain or self-interest has been motivator in several data integrity related fraud cases. The extent and impact of falsification can be magnified if collusion is involved.
- Robust technical controls within all of the data generation, collection, processing or storage systems, coupled with effective data review processes, can reduce opportunities for fraud
- Effective mechanisms to reduce human error rates include using human data entry minimally and automated data capture maximally, data validation and edit checks etc.,

4 Annexure

NA

4.1 References

- ISPE GAMP Guide: Records and Data integrity, 2017
- FDA Data Integrity and Compliance with cGMP Guidance for Industry April 2016
- FDA 21 CFR Part 11. Electronic Records; Electronic Signatures
- Eudralex Volume 4 - Medicinal Products for Human and Veterinary Use: Good Manufacturing Practice EU GMP Annex 11 – Computerized Systems.
- MHRA GMP Data Integrity Definitions and Guidance for Industry March 2015.



OLS-06-28G-Data Integrity-Guidelines_Approval - Message (HTML)

File Message Help Tell me what you want to do

Delete Archive Reply Reply All Forward Move to: ? To Manager Team Email Done Reply & Delete Create New Move Assign Policy Mark Unread Categorize Follow Up Translate Read Aloud Zoom Send to OneNote Insights EmailRemediator

Delete Respond Quick Steps Move Tags Editing Speech Zoom OneNote Suspicious Email

OLS-06-28G-Data Integrity-Guidelines_Approval

Swati Kochukulam
To Anjana Gopalakrishnan; Vijayakumar GS

Reply Reply All Forward

Wed 8/26/2020 7:14 PM

Follow up. Start by Wednesday, August 26, 2020. Due by Wednesday, August 26, 2020.
You replied to this message on 8/26/2020 7:14 PM.

OLS-06-28G-Data Integrity-Guidelines.pdf
333 KB

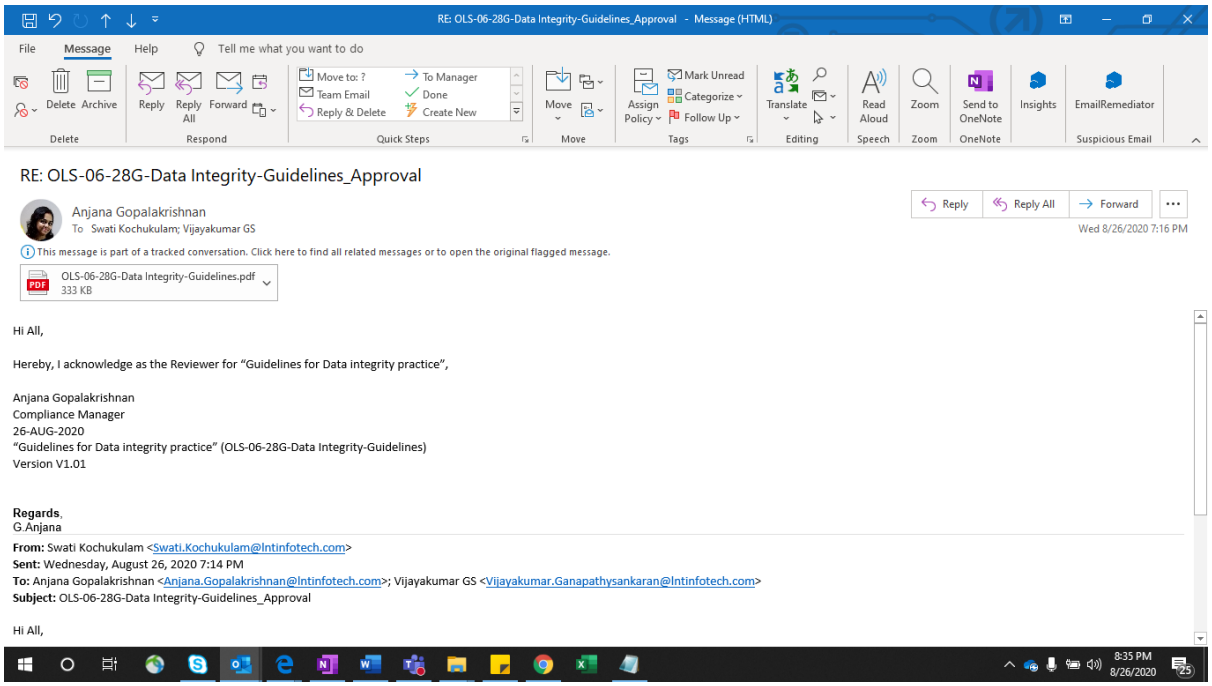
Hi All,

Hereby, I acknowledge as the Author for "Guidelines for Data integrity practice",

Swati Kochukulam
Compliance Lead
26-AUG-2020
"Guidelines for Data integrity practice" (OLS-06-28G-Data Integrity-Guidelines)
Version V1.01

Thanks & Regards,
Swati k.

8:35 PM
8/26/2020



RE: OLS-06-28G-Data Integrity-Guidelines_Approval - Message (HTML)

File Message Help Tell me what you want to do

Delete Archive Reply Reply All Forward Move to: ? To Manager Team Email Done Reply & Delete Create New Move Assign Policy Mark Unread Categorize Follow Up Translate Read Aloud Zoom Send to OneNote Insights EmailRemediator

Delete Respond Quick Steps Move Tags Editing Speech Zoom OneNote Suspicious Email

RE: OLS-06-28G-Data Integrity-Guidelines_Approval

Anjana Gopalakrishnan
To Swati Kochukulam; Vijayakumar GS

Reply Reply All Forward

Wed 8/26/2020 7:16 PM

This message is part of a tracked conversation. Click here to find all related messages or to open the original flagged message.

OLS-06-28G-Data Integrity-Guidelines.pdf
333 KB

Hi All,

Hereby, I acknowledge as the Reviewer for "Guidelines for Data integrity practice",

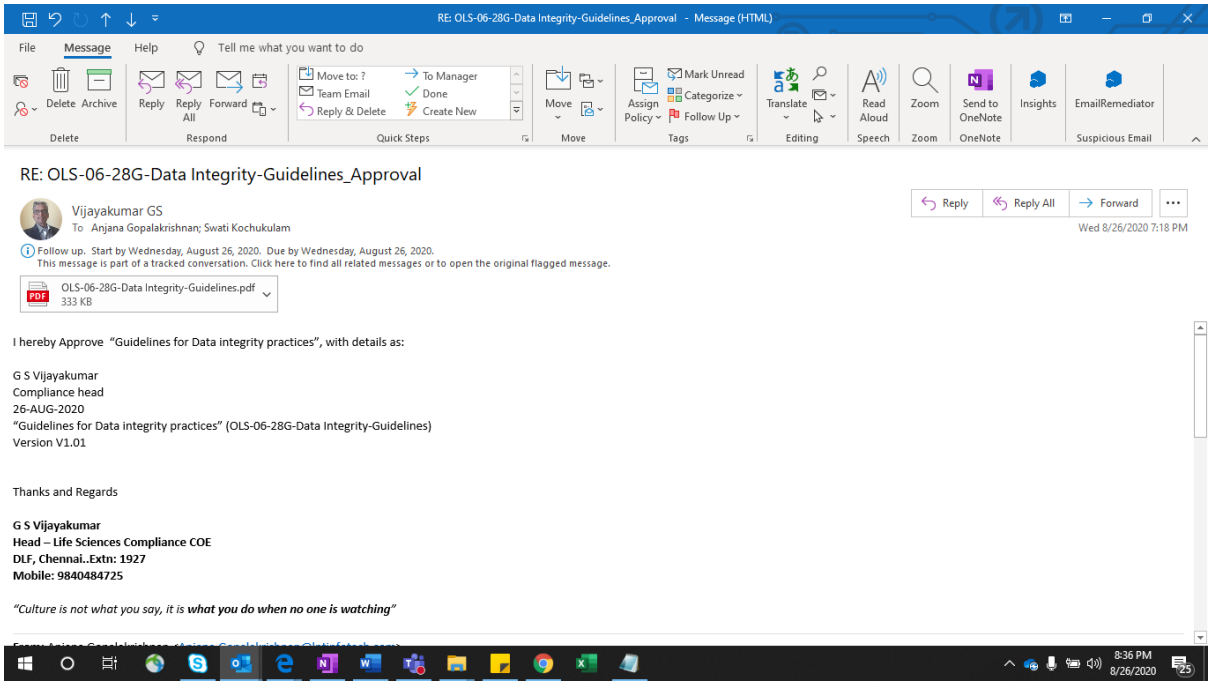
Anjana Gopalakrishnan
Compliance Manager
26-AUG-2020
"Guidelines for Data integrity practice" (OLS-06-28G-Data Integrity-Guidelines)
Version V1.01

Regards,
G.Anjana

From: Swati Kochukulam <Swati.Kochukulam@lntinfotech.com>
Sent: Wednesday, August 26, 2020 7:14 PM
To: Anjana Gopalakrishnan <Anjana.Gopalakrishnan@lntinfotech.com>; Vijayakumar GS <Vijayakumar.Ganapathysankaran@lntinfotech.com>
Subject: OLS-06-28G-Data Integrity-Guidelines_Approval

Hi All,

8:35 PM
8/26/2020



RE: OLS-06-28G-Data Integrity-Guidelines_Approval - Message (HTML)

File Message Help Tell me what you want to do

Delete Archive Reply Reply All Forward Move to: ? To Manager Team Email Done Reply & Delete Create New Move Assign Policy Mark Unread Categorize Follow Up Translate Read Aloud Zoom Send to OneNote Insights EmailRemediator

Delete Respond Quick Steps Move Tags Editing Speech Zoom OneNote Suspicious Email

RE: OLS-06-28G-Data Integrity-Guidelines_Approval

Vijayakumar GS
To Anjana Gopalakrishnan; Swati Kochukulam

Reply Reply All Forward

Wed 8/26/2020 7:18 PM

Follow up. Start by Wednesday, August 26, 2020. Due by Wednesday, August 26, 2020.
This message is part of a tracked conversation. Click here to find all related messages or to open the original flagged message.

OLS-06-28G-Data Integrity-Guidelines.pdf
333 KB

I hereby Approve "Guidelines for Data integrity practices", with details as:

G S Vijayakumar
Compliance head
26-AUG-2020
"Guidelines for Data integrity practices" (OLS-06-28G-Data Integrity-Guidelines)
Version V1.01

Thanks and Regards

G S Vijayakumar
Head – Life Sciences Compliance COE
DLF, Chennai..Extn: 1927
Mobile: 9840484725

*"Culture is not what you say, it is **what you do when no one is watching**"*

8:36 PM
8/26/2020