POLICY ON DATA INTEGRITY

INTRODUCTION:

This document provides the policy to investigate and handle incidences related to GXP data, identified during internal/external audit or during review of data at any stage, for reliability of data, either paper or electronic, with an intention to safeguard the integrity of GXP data.

SCOPE:

Applicable to all functions and departments where GXP activities generated by electronic and paper-based systems at …………….. associated sites, …………. affiliate companies and contractors/service providers.

POLICY DETAILS:

….……. should develop:

1. A culture within the organization to ensure that the data is complete, consistent, and accurate in all its form throughout data lifecycle (paper and electronic).

2. To create the right environment to enable data integrity controls to be effective. Employee responsibilities related to data reliability should be communicated to each level of employee as a code of conduct and every concerned employee should acknowledge the same.

3. Organizational culture driven by performance indicators on the success of data governance measure.

4. Approach to perform the data integrity risk assessment. Any departure from data reliability should be investigated and an impact assessment should be performed.

5. Governance measures to ensure periodic audits to detect data integrity failures within organization's systems.

6. Mechanism to investigate impact of data integrity failure to the patient or environment.

7. Data integrity controls for both, manual and computerized systems.

8. Where data integrity weaknesses are identified, appropriate corrective and preventive actions should be implemented across all relevant activities and systems and not in isolation.

9. Controls over intentional and unintentional changes to data.

10. Systems and processes in a way that facilitate compliance with the principle of data integrity.

General Information:

Appropriate controls should be applied across the whole data lifecycle to provide assurance of data integrity and same should be documented. Good documentation practices should be in place.

Any alteration in data should be appropriately controlled, reasoned, initiated, approved, and documented. Documents prepared should be free from intentional and unintentional errors.

POLICY ON DATA INTEGRITY

All documents and data should be Attributable, Legible and Permanent, Contemporaneous, Original / Reliable, Accurate, Complete, Consistent, Enduring and Available ($ALCOA^{+}$).

Criterion	Meaning
Attributable	Attributable means information is captured in the record so that it is uniquely identified as executed by the originator of the data (e.g. a person, computer system). Who performed the activity and when. If the record is changed, who did it and why. Link to the source document.
Legible and Permanent	Data are readable, understandable and allow a clear picture of the sequencing of steps or events in the record.
Contemporaneous	Contemporaneous is process of documentation (on paper or electronically) at the time of an activity.
Original	Original data includes the first or source capture of data or information and all subsequent data required to fully reconstruct the conduct of the GXP activity.
Accurate	The term "accurate" means data are correct, truthful, valid, and reliable.
Complete	The data must be whole, a complete set.
Consistent	The data must be self-consistent.
Enduring	Durable; lasting throughout the data lifecycle.
Available	Readily available for review or inspection purposes.

GMP activities should be designed in a manner to support data reliability across the data life cycle to ensure data is complete and meets the requirements set forth in the 'Good Documentation Practices and Documentation Control', Policy number 1035-Policy-056.

Validation of data process should be designed to adequately mitigate and control and continuously review the data integrity risks associated with the steps of acquiring, processing, reviewing, and reporting data as well as the physical flow of the data and associated metadata across this process through storage and retrieval.

All computerized and non-computerized systems should have security controls in place. All computerized system should be tamper-evident. Systems generating and storing data should be password protected and changes done should be traceable.

….……… as a contract giver should ensure data ownership, governance and accessibility with contract acceptor which should be agreed upon by both the parties as part of contract/ quality technical agreement.

Employees should be made aware of the specific data reliability requirements for the activities to be performed by them. Awareness programme of applicable laws, regulation and legislative directives that pertain to documentation and record keeping should be designed and implemented. Training programme should be in place for staff on importance of data integrity principles.

Data integrity is a life cycle approach; it refers to maintaining and assuring the accuracy and consistency of data over the entire data life cycle i.e. from

Data generation ➡ Data collection ➡ Data processing ➡ Data review ➡ Data approval ➡ Data reporting ➡ Data archival.

Assuring data integrity requires appropriate quality and risk management systems for each data/ processing step, including adherence to sound scientific principles and good documentation practices.

POLICY ON DATA INTEGRITY

Compliance to data integrity starts from

Development ➡ Manufacturing ➡Packing ➡Distribution ➡ Other (post-marketing activities like pharmacovigilance/ complaints etc.).

Principles of data integrity apply to paper records, electronic records, records generated through hybrid systems and by other data such as photography, imagery, chromatography plates etc. that were created during manufacturing, packaging, testing, holding, shipping and distribution and any other ancillary or supporting activities within the framework of GXP.

Procedure to investigate and handle data integrity incidence:

During the life cycle of GXP processing inclusive of documentation, following procedure should be followed to investigate and suggest corrective actions. If any observation related to breach to data integrity is noted in below cases which are not limited to:

1. Doer himself reported his data integrity incidence.
2. During periodic review of GXP document.
3. During internal and regulatory audit.
4. At any point of time of review (other than doer).
5. During investigation.

The individual identifying the event of breach to data integrity should report the incident to the department head. Department head should inform the respective unit/site Human Resource Business Partner (HRBP) and Head Unit Quality Assurance immediately in writing or telephonically or physically within one (1) working day.

Such data integrity should be thoroughly investigated to find out root cause, assess impact and assign appropriate corrective action and preventive actions through deviation procedure immediately.

Note: Initial categorization of all deviations as an outcome of breach to data integrity should be “Critical”. Final categorization of deviation may or may not change based on detailed investigation by task force committee.

Department head should communicate information of data integrity incidence to Head Site Quality Assurance, Unit Head, Site Head and HR.

The Unit Head / Head Unit Quality Assurance should be the lead investigator and enlist other discipline heads as necessary.

Suspected or known falsification of records should be fully investigated under the CGMP quality system to determine the effect of the event on patient safety, product quality, and data reliability; to determine the root cause; and to ensure the necessary corrective actions are taken, if necessary, global CAPA(s) should be initiated.

Investigation should be conducted by Task force investigation committee which consist of following members:

- Site HR head or an assigned representative(mandatory)
- Concerned department head (mandatory)
- Reporting manager of the concerned person (optional)
- Quality head of the unit (mandatory)
- Unit head (mandatory)
- Head Site Quality (same/other location)
- Site QC head (same/other location)
- Site head (same/other location)
- Other cross functional team members as applicable

POLICY ON DATA INTEGRITY

Note: If person mentioned above is not present then, person can nominate peer or superior (even from other location) which should be considered in task force investigation team.

Investigation should contain summary of all information from applicable GMP areas, laboratories, manufacturing operations, processing and information systems covered by the assessment. In case of exclusion of any part of the operation, justification for the same should be prepared.

An assessment of the extent of data integrity deficiencies at the facility should be conducted.

Comprehensive retrospective evaluation should be conducted to identify the nature of the data integrity deficiencies; these should include all the work that the individual may have done before.

Risk assessment should be performed to identify the potential effect of the observed failures on the quality of the product that was released. The risk assessment should include the following but not limited to:

- Analysing risks to patients
- Risks posed by ongoing operations
- Any impact on the veracity of data submitted to regulatory agencies including data related to product registration dossiers.
- Long-term measures describing any remediation efforts and enhancements to procedures, processes, methods, controls, systems, management oversight, and human resources (e.g., training, staffing improvements) designed to ensure the integrity of data.

Based on the data integrity incidence, investigation carried out and conclusion derived, disciplinary action should be taken by ‘Task Force Investigation Committee’ as per ‘…….. Data Integrity Guideline’.

Appropriate notification to regulatory authorities should be made where significant data integrity incidents have been identified which has an impact on product quality and patient safety in instances where product already released to market by unit QA in consultation with site QA and respective stakeholders.

AMENDMENT AND WAIVER:

The company reserves the right to amend, alter and/ or terminate this policy at any time.

DEFINITION:

Data integrity : Data integrity is the degree to which data are complete, consistent, accurate, trustworthy, reliable and that these characteristics of the data are maintained throughout the data life cycle. The data should be collected and maintained in a secure manner, so that they are attributable, legible, contemporaneously recorded, original (or a true copy) and accurate.

ALCOA plus: A commonly used acronym for “attributable, legible, contemporaneous, original and accurate”, which puts additional emphasis on the attributes of being complete, consistent, enduring, and available – implicit basic ALCOA principles.

Hybrid data: Data is generated by using hybrid system where both paper-based and electronic records constitute the original record.

Other data: The data generated is captured by a photograph or imagery (or other media).

Data reliability: Data reliability is the degree to which a collection of data is complete, consistent, and accurate throughout the data lifecycle. The collected data should be attributable, legible, contemporaneously recorded, original or a true copy and accurate.

Data lifecycle: All phases in the life of the data from generation and recording through processing (including analysis, transformation, or migration), use, data retention, archive/retrieval, and destruction.

Data Governance:
The arrangements to ensure that data, irrespective of the format in which they are generated, are recorded, processed, retained, and used to ensure the record throughout the data lifecycle.

Breach of data integrity:
It is a violation of the integrity of data to get intended results or to test products into compliance. This means, the actions performed, and the documents/records written do not reflect the truth and the reality which has taken place. Common terms used are falsification of data, alteration of data and events, misleading information, statements or facts, misrepresentation of what happened, untruthful statements, deceit, forgery.
Few examples of breach to data integrity are as below, but not limited to:

- Data falsification and generation of unauthorized documents.
- Signing off or owning records for activity not performed by self.
- Intentionally misplacing or replacing documents.
- Trial runs in analysis (Actual standards, reference, working / test standards) should not be used to perform system suitability test.
- Manipulating date and time in computer system or any other system used for GMP activities.
- Manipulating and or misrepresenting any parameters such as process or analytical parameters etc.
- Reprocessed chromatograph not retained for review.
- Recording of an activity not performed.
- Copying existing data as new data, unless supported by original data.
- Re-running samples without justification and investigation.
- Discarding/deletion of data, unless authorised.
- Releasing failing product.
- Not saving electronic or hard copy data.

ABBREVIATIONS:

CAPA	:	Corrective Action and Preventive Action
GMP	:	Good Manufacturing Practices
GXP	:	Good X Practices where X stands for Chromatographic, Clinical, Manufacturing, laboratory, distribution, quality, pharmacovigilance etc.
HR	:	Human Resources
SOP	:	Standard Operating Procedure

REFERENCES:

MHRA : GXP Data Integrity Guidance and Definitions.
USFDA : Guidance on Data Integrity and Compliance with drug cGMP – Guidance for Industry PIC/S: Draft Guidance on – Good practices for data management and integrity in regulated environment.