PHARMA DEVILS

QUALITY ASSURANCE DEPARTMENT

STANDARD OPERATING PROCEDURE	
Department: Quality Assurance	**SOP No.:**
Title: Data Integrity Policy	**Effective Date:**
Supersedes: Nil	**Review Date:**
Issue Date:	**Page No.:**

1.0 OBJECTIVE:

To lay down a Procedure for Data Integrity Policy.

2.0 SCOPE:

This SOP is applicable to all the manufacturing sites.

3.0 RESPONSIBILITY:

CQA (Officer/ Executive)	**:**	Preparation, Distribution (To Plant-QA and Corporate Departments), Revision, Retrieval and Destruction of this SOP.
CQA (Operating Manager)	**:**	Review, Training and Effective implementation of this SOP. (To Plant-QA and other Corporate Departments)
CQA (Lead Auditor)	**:**	To review Data Integrity compliances during Self Inspection
Plant QA (Officer/ Executive)	**:**	Preparation of Plant SOP in accordance with this SOP and Retrieval of this SOP.
Plant QA (Operating Manager)	**:**	Training and Effective Implementation of this SOP to all Concerned Department of Plant.
Concerned Department (Officer/ Executive)	**:**	Data Generation to comply Data Integrity routinely. Initiation and Implementation of CAPA.
Concerned Department (Operating Manager)	**:**	Monitoring Data Integrity issues Effective implementation of this SOP and Review of CAPA effectiveness. Review Data Integrity compliance

4.0 ACCOUNTABILITY:

Head CQA	**:**	Approval, Authorization and ensure Training and Implementation of this SOP. Approval Data Integrity compliance and mitigation plan.
Head QA	**:**	To ensure distribution to concerned Departments, Training and Effective Implementation of this SOP. Review and Approval of compliance report and CAPA effectiveness for Data Integrity

STANDARD OPERATING PROCEDURE	
Department: Quality Assurance	**SOP No.:**
Title: Data Integrity Policy	**Effective Date:**
Supersedes: Nil	**Review Date:**
Issue Date:	**Page No.:**

Concerned Department (Head) : Review Data Integrity compliance and CAPA.

5.0 ABBREVIATIONS:

ALCOA	Attributable Legible Contemporaneous Original Accurate
CAPA	Corrective Action and Preventive Action
CQA	Corporate Quality Assurance
GDP	Good Documentation Practice
GxP	Good x Practices (X can be: Laboratory, Manufacturing, Pharmaceutical, etc.)
Ltd.	Limited
MHRA	Medicines & Healthcare Product Regulatory Agency
No.	Number
PDF	Portable Document Format
Pvt.	Private
QA	Quality Assurance
QC	Quality Control
QMS	Quality Management System
SAP	Systems Applications Products
SOP	Standard Operating Procedure
VMP	Validation Master Plan
WHO	World Health Organization

6.0 PROCEDURE:

Note:

a. ***Data Integrity is everyone's Responsibility.***
b. ***Data Integrity is not a checkbox exercise.***
c. ***"Data Integrity problems mean that the quality system is deficient in some way. This takes a lot of resources to fix. A lot of this is about changing the culture within the company. When a data integrity problem is identified in an organization, it is just like the tip of the iceberg, and it speaks to the overall quality system of a company."***

6.1 DEFINITION:

6.1.1 DATA INTEGRITY:

The extent to which all data are complete, consistent and accurate throughout the data Lifecycle from initial data generation and recording through processing (including transformation or migration), use, retention, archiving, retrieval and destruction.

STANDARD OPERATING PROCEDURE	
Department: Quality Assurance	**SOP No.:**
Title: Data Integrity Policy	**Effective Date:**
Supersedes: Nil	**Review Date:**
Issue Date:	**Page No.:**

6.1.1.1 Data Integrity refers to the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data shall be Attributable, Legible, Contemporaneously recorded, Original or a True Copy, and Accurate (ALCOA).

6.1.1.2 Data Integrity is the degree to which a collection of data is complete, consistent and accurate throughout the data lifecycle. The collected data shall be attributable, legible, contemporaneously recorded, original or a true copy, and accurate. Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles and good documentation practice**s.**

6.1.2 **ALCOA** :

6.1.2.1 Data shall be attributable, legible, contemporaneously recorded, original or a true copy, and accurate **(ALCOA).**

Where,

A **:** Attributable to the person generating the data
L **:** Legible and permanent
C **:** Contemporaneous
O **:** Original record (or 'true copy')
A **:** Accurate

6.1.3 **ALCOA-PLUS:**

6.1.3.1 The acronym shall be used 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.

6.1.3.2 Data Integrity – A Lifecycle Approach"

- The degree to which a collection of data is complete, consistent and accurate.
- Compliance to data integrity starts from:
- Development ⟹ Manufacturing ⟹ Packing ⟹ Distribution
- Data integrity refers to maintaining and assuring the accuracy and consistency of data over the entire data life-cycle;

6.1.4 RAW DATA:

6.1.4.1 Original records and documentation, retained in the format in which they were originally generated (i.e. paper or electronic), or as a 'true copy'.

6.1.4.2 Raw data must be contemporaneously and accurately recorded by permanent means in the case of basic electronic equipment which does not store electronic data, or provides only a printed data output (e.g. balance or pH meter), the printout constitutes the raw data.

6.1.4.3 Raw Data shall**;**

- Be legible and accessible throughout the data lifecycle.
- Permit the full reconstruction of the activities resulting in the generation of the data.

6.1.4.4 Training shall be provided to concerned personnel to detect data integrity issues in purview of personnel requirements, which state that personnel must have the education, training, and experience to perform their assigned duties.

6.1.4.5 Data means 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 and allow full and complete reconstruction and evaluation of the GxP Activity.

6.1.4.6 Data shall 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 and audit trails, photographs, microfilm or microfiche, audio- or video-files or any other media whereby information related to GxP activities is recorded.

6.1.5 META DATA:

6.1.5.1 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, inter-relationships and other characteristics of data.

6.1.5.2 Metadata forms an integral part of the original record; without metadata, the data has no meaning.

6.1.5.3 Metadata is structured information that describes, explains, or otherwise makes it easier to retrieve, use, or manage data.

6.1.5.4 For Example, the number "23" is meaningless without metadata, such as an indication of the unit "mg".

6.1.6 DATA LIFE CYCLE:

6.1.6.1 All Phases of the process by which data are created, recorded, processed, reviewed, analyzed & reported, transferred, stored, retrieved and monitored until retirement and disposal.

6.1.6.2 A Planned approach to assessing, monitoring and managing the data and the risks to those data in a manner commensurate with potential impact on patient safety, product quality and/or the reliability of the decisions made throughout all phases of the data life cycle.

6.1.7 DYNAMIC RECORD FORMAT:

6.1.7.1 Records in dynamic format, such as electronic records, that allow for an interactive relationship between the user and the record content.

6.1.8 FULLY ELECTRONIC APPROACH:

6.1.8.1 This term refers to use of a computerized system in which the original electronic records are electronically signed.

6.1.9 GOOD DATA AND RECORD MANAGEMENT PRACTICES:

6.1.9.1 The Totality of organized measures that shall be in place collectively and individually to ensure that data and records are secure, attributable, legible, traceable, permanent, contemporaneously recorded, original and accurate.

6.1.9.2 In case Data and Records are not robustly implemented, can impact on data reliability and completeness and undermine the robustness of decision-making based upon those data records.

6.1.10 GOOD DOCUMENTATION PRACTICES:

6.1.10.1 Good Documentation Practices are those measures that collectively and individually ensure documentation, whether paper or electronic, is secure, attributable, legible, traceable, permanent, contemporaneously recorded, original and accurate.

6.1.11 GxP:

6.1.11.1 Acronym for the group of Good Practice Guides governing the preclinical, clinical, manufacturing, testing, storage, distribution and post-market activities for regulated pharmaceuticals, biological and medical devices, such as Good Laboratory Practices, Good Clinical Practices, Good Manufacturing Practices, Good Pharmacovigilance Practices and Good Distribution Practices.

6.1.12 HYBRID APPROACH:

6.1.12.1 A computerized system in which there is a combination of original electronic records and paper records that comprise the total record set that shall be reviewed and retained.

6.1.12.2 Example of a hybrid approach is where laboratory analysts use computerized instrument systems that create original electronic records and then print a summary of the results.

6.1.13 QUALITY METRICS:

6.1.13.1 Quality Metrics are objective measures used by management and other interested parties to monitor the overall state of quality of a GxP organization, activity or process or study conduct, as applicable.

6.1.13.2 Quality Metrics include measures to assess the effective functioning of quality system controls and of the performance, quality and safety of medicinal products and reliability of data.

6.1.14 QUALITY RISK MANAGEMENT:

6.1.14.1 A systematic process for the assessment, control, communication and review of risks to the quality of the pharmaceutical product throughout the product life cycle

6.1.15 SENIOR MANAGEMENT:

6.1.15.1 Person(s) who direct and control a company or site at the highest levels with the authority and responsibility to mobilize resources within the company or site.

6.1.16 STATIC RECORD FORMAT:

6.1.16.1 A static record format, such as a paper or PDF record, is one that is fixed and allows little or no interaction between the user and the record content.

6.1.17 TRUE COPY:

6.1.17.1 A true copy is a copy of an original recording of data that has been verified and certified to confirm it is an exact and complete copy that preserves the entire content and meaning of the original record, including, in the case of electronic data, all essential metadata and the original record format as appropriate

6.1.18 ELECTRONIC RECORD:

6.1.18.1 Electronic Record as any combination of text, graphics, data, audio, pictorial, or other information represented in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

6.1.18.2 Electronic Record must maintain authenticity, integrity and confidentiality of electronic records which shall be trustworthy, reliable and equivalent to paper records and handwritten signatures.

6.1.19 HYBRID SYSTEM:

6.1.19.1 A 'Hybrid System' is defined as an environment consisting of both Electronic and Paper-based Records (Frequently Characterized by Handwritten Signatures Executed on Paper).

6.1.20 AUDIT TRAIL:

6.1.20.1 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.

6.1.20.2 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.

6.1.20.3 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).

6.1.20.4 Electronic record-keeping systems, which include Audit Trails, can fulfill these cGMP requirements.

6.1.20.5 Whenever computerized systems are used to capture, Process, Report or store raw data electronically, system design shall always provide for the retention of full audit trails to show all changes to the data while retaining previous and original data.

6.1.20.6 The relevance of data retained in Audit Trails shall be considered by the company to permit robust data review / verification.

6.1.20.7 The items included in audit trail shall be those of relevance to permit reconstruction of the process or activity.

6.1.20.8 Audit trail review shall be a part of the routine data review / approval process, usually performed by the operational area which has generated the data (e.g. laboratory).

6.1.20.9 Concerned departments shall also review a sample of relevant audit trails, raw data and metadata as a part of self-inspection to ensure on-going compliance with the data governance policy / procedures.

6.1.20.10 Audit trails that capture changes to critical data shall be reviewed with each record and before final approval of the record.

6.1.20.11 Audit trails subject to regular review shall include, but are not limited to, the following: the change history of finished product test results.

6.1.20.12 The changes to sample run sequences, changes to sample identification, and changes to critical process parameters.

STANDARD OPERATING PROCEDURE	
Department: Quality Assurance	**SOP No.:**
Title: Data Integrity Policy	**Effective Date:**
Supersedes: Nil	**Review Date:**
Issue Date:	**Page No.:**

6.1.21 DATA GOVERNANCE:

6.1.21.1 The sum of arrangements to ensure that data, irrespective of the format in which it is generated, is recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data lifecycle.

6.1.21.2 Data governance shall address data ownership throughout the lifecycle, and consider the design, operation and monitoring of processes / systems in order to comply with the principles of data integrity including control over intentional and unintentional changes to information.

6.1.21.3 Data Governance systems shall include staff training in the importance of data integrity principles and the creation of a working environment that enables visibility of errors, omissions and aberrant results.

6.1.22 DATA LIFE CYCLE:

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

6.1.22.2 The procedures for destruction of data shall consider data criticality and where applicable legislative retention requirements. Archival arrangements shall be in place for long term retention of relevant data in compliance with legislation.

6.1.23 DATA TRANSFER / MIGRATION:

6.1.23.1 Data transfer is the process of transferring data and metadata between storage media types or computer systems.

6.1.23.2 Data migration changes the format of data to make it usable or visible on an alternative computerized system.

6.1.23.3 Data transfer/migration shall be designed and validated to ensure that data integrity principles are maintained.

6.1.24 DATA PROCESSING:

6.1.24.1 A sequence of operations performed on data in order to extract, present or obtain information in a defined format.

6.1.24.2 There shall be an adequate traceability of any user defined parameters used within data processing activities.

6.1.24.3 Audit trails and retained records shall allow reconstruction of all data processing activities regardless of whether the output of that processing is subsequently reported or otherwise used.

6.1.24.4 In case data processing has been repeated with progressive modification of processing parameters this shall be visible to ensure that the processing parameters are not being manipulated to achieve a more desirable end point.

6.1.25 RECORDING DATA:

6.1.25.1 Organization shall be an appropriate level of process understanding and technical knowledge of systems used for data recording, including their capabilities, limitations and vulnerabilities.

6.1.25.2 The selected method shall ensure that data of appropriate accuracy, completeness, content and meaning is collected and retained for its intended use.

6.1.25.3 Where the capability of the electronic system permits dynamic storage it is not appropriate for low-resolution or static (printed / manual) data to be collected in preference to high resolution or dynamic (electronic) data.

6.1.26 EXCLUDING DATA:

6.1.26.1 Data shall only be excluded where it can be demonstrated through sound science that the data is anomalous or non-representative.

6.1.26.2 In all cases, this justification shall be documented and considered during data review and reporting.

6.1.26.3 All data (even if excluded) shall be retained with the original dataset, and be available for review in a format that allows the validity of the decision to exclude the data to be confirmed.

6.1.27 PRIMARY RECORD:

6.1.27.1 The record which takes primacy in cases where data that are collected and retained concurrently by more than one method fail to concur.

6.1.27.2 In situations where the same information is recorded concurrently by more than one system, the data owner shall define which system generates and retains the primary record.

6.1.27.3 In case of discrepancy. The ‘primary record’ attribute shall be defined in the quality system, and shall not be changed on a case by case basis.

6.1.27.4 Risk management principles shall be used to ensure that the assigned 'primary record' provides the greatest accuracy, completeness, content and meaning.

6.1.27.5 All data shall be considered when performing a risk based investigation into data anomalies (e.g. Out-Of-Specification results).

6.1.28 ORIGINAL RECORD:

6.1.28.1 Data as the file or format in which it was originally generated, preserving the integrity (accuracy, completeness, content and meaning) of the record.

6.1.29 TRUE COPY:

6.1.29.1 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).

6.1.29.2 Original records and true copies must preserve the integrity (accuracy, completeness, content and meaning) of the record.

6.1.29.3 Exact (true) copies of original records shall 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.

6.1.29.4 True copy 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.

6.1.29.5 A documented means to verify that the printed records are an accurate representation.

6.1.29.6 The electronic records are important to retain in their dynamic (electronic) format, to enable interaction with the data.

6.1.29.7 Data must be retained in a dynamic form where this is critical to its integrity or later verification. This shall be justified based on risk.

6.1.29.8 Computerized system configuration settings shall be defined, tested, 'locked' and protected from unauthorized access as part of computer system validation.

6.1.29.9 Only those variable settings which relate to an analytical run shall be considered as electronic raw data.

6.1.30 ELECTRONIC SIGNATURES:

6.1.30.1 An electronic signature or e-signature, refers to data in electronic form, which is logically associated with other data in electronic form and which is used by the signatory to sign.

6.1.31 BACKUP:

6.1.31.1 True copy of the original data that is maintained securely throughout the records retention period

6.1.31.2 The backup file shall contain the data (which includes associated metadata) and shall be in the original format or in a format compatible with the original format.

6.1.31.3 A copy of current (editable) data, metadata and system configuration settings (variable settings which relate to a record or analytical run) maintained for the purpose of disaster recovery.

6.1.31.4 Backup and recovery processes shall be validated and periodically tested.

6.1.31.5 Backup shall be performed as per respective Plant SOP.

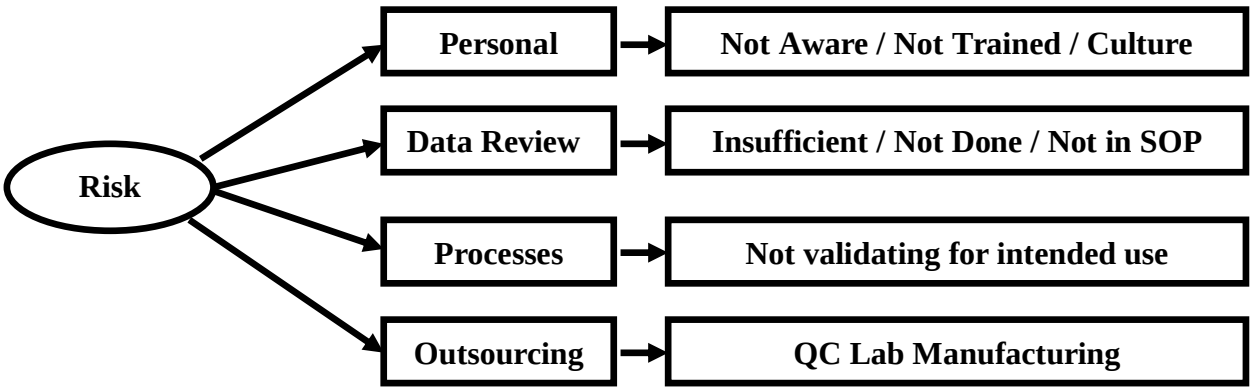
6.1.32 FLAT FILES:

6.1.32.1 A 'flat file' is an individual record which may not carry with it all relevant metadata (e.g. pdf, dat, doc. etc.).

6.1.32.2 Last amendment, but may not audit trail the type and sequence of amendments. When creating flat file reports from electronic data, the metadata and audit trails relating to the generation of the raw data may be lost, unless these are retained as a 'true copy'.

6.1.32.3 There is an inherently greater Data Integrity risk with flat files (e.g. when compared to data contained within a relational database), in that these are easier to manipulate and delete as a single file.

6.2 DATA INTEGRITY RISK FACTOR:



6.3 DATA INTEGRITY CONTROLS:

6.3.1 Following elements are important to monitored Data Integrity

6.3.1.1 Prevention of Data Integrity:

6.3.1.1.1 Personnel (Internal/External)

6.3.1.1.2 Designing and Validation system

6.3.1.1.3 Managing Data and Record throughout the Data Life Cycle

6.3.1.1.4 Good Documentation Practices

6.3.1.2 Detection of Data Integrity:

6.3.1.2.1 Data Review

6.3.1.2.2 Audits

6.3.1.3 Addressing Data Reliability Issues:

6.3.1.3.1 Investigate/ Corrective and Preventive Actions

6.3.1.3.2 Impact Assessment

6.3.2 PREVENTION OF DATA INTEGRITY:

6.3.2.1 Data integrity shall be Prevented and controlled in following manner.

6.3.2.1.1 PERSONNEL (INTERNAL/EXTERNAL):

6.3.2.1.1.1 Contracted Organizations, Suppliers and Service Providers:

6.3.2.1.1.1.1 The increasing outsourcing of GxP work to contracted organizations, e.g. contract research organizations, suppliers and other service providers, emphasizes the need to establish and robustly maintain defined roles and responsibilities to assure complete and accurate data and records throughout these relationships.

6.3.2.1.1.1.2 The responsibilities of the contract giver and acceptor, shall comprehensively address the processes of both parties that shall be followed to ensure data integrity. These details shall be included in the contract described in the WHO GxP's relevant to the outsourced work performed or the services provided.

6.3.2.1.1.2 Training in Good Data and Record Management:

6.3.2.1.1.2.1 Personnel shall be trained in data integrity policies and agree to abide by them. Management shall ensure that personnel are trained to understand and distinguish between proper and improper conduct, including deliberate falsification, and shall be made aware of the potential consequences.

6.3.2.1.1.2.2 Management shall also ensure that, at the time of hire and periodically afterwards, as needed, all personnel are trained in procedures to ensure GDP for both paper and electronic records.

6.3.2.1.1.2.3 The quality unit shall include checks for adherence to GDP for both paper records and electronic records in their day-to-day work, system and facility audits and self-inspections and report any opportunities for improvement to management.

6.3.2.1.2 DESIGNING AND VALIDATION SYSTEM:

6.3.2.1.2.1 Record-keeping methodologies and systems, whether paper or electronic, shall be designed in a way that encourages compliance and assures data quality and reliability.

6.3.2.1.2.2 Computerized systems shall comply with regulatory requirements and associated guidance and be validated for their intended purpose.

6.3.2.1.2.3 In isolation from the intended process or end user IT infrastructure, vendor testing is likely to be limited to functional verification only, and shall not fulfill the requirements for performance qualification.

6.3.2.1.2.4 To assure the integrity of electronic data, computerized systems shall be validated at a level appropriate for their use and application. Validation shall address the necessary controls to ensure the integrity of data, including original electronic data and any printouts or PDF reports from the system.

6.3.2.1.2.5 User involvement. Users shall be adequately involved in validation activities to define critical data and data life cycle controls that assure data integrity.

6.3.2.1.2.6 Configuration and design controls: The validation activities shall ensure configuration settings and design controls for GDP are enabled and managed across the computing environment (including both the software application and operating systems environments). Activities include, but are not limited to:

- ✓ Documenting configuration specifications for commercial off-the shelf systems as well as user-developed systems, as applicable;
- ✓ Restricting security configuration settings for system administrators to independent personnel, where technically feasible;
- ✓ Disabling configuration settings that allow overwriting and reprocessing of data without traceability;
- ✓ Restricting access to time/date stamps.

6.3.2.1.2.7 For systems to be used in clinical trials, configuration and design controls shall be in place to protect the blinding of the trial, for example, by restricting access to randomization data that shall be stored electronically.

6.3.2.1.2.8 Data Life Cycle : Validation shall include assessing risk and developing quality risk mitigation strategies for the data life cycle, including controls to prevent and detect risks throughout the steps of:

- ✓ Data Generation and Capture;
- ✓ Data Transmission;
- ✓ Data Processing;
- ✓ Data Review;
- ✓ Data Reporting, including Handling of invalid and atypical data;
- ✓ Data Retention and Retrieval;
- ✓ Data Disposal.

6.3.2.1.2.9 SOPs and Training: The validation activities shall ensure that adequate training and procedures are developed prior to release of the system for GxP use. These shall address:

- ✓ Computerized systems administration;
- ✓ Computerized systems use;
- ✓ Review of electronic data and meaningful metadata, such as Audit Trails, including training that shall be required in system features that Enable users to efficiently and effectively process data and review Electronic data and metadata.

6.3.2.1.3 MANAGING DATA AND RECORD THROUGHOUT THE DATA LIFE CYCLE:

6.3.2.1.3.1 Data processes shall 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 during this process through storage and retrieval.

6.3.2.1.3.2 Data Integrity risks are likely to occur and to be highest when data processes or specific data process steps are inconsistent, subjective, open to bias, unsecured, unnecessarily complex or redundant, duplicated, undefined, not well understood, hybrid, based upon unproven assumptions and/or do not adhere to GDP.

6.3.2.1.3.3 Good data process design shall consider, for each step of the data process, ensuring and enhancing controls, whenever possible, so that each step is:

- ➢ Consistent;
- ➢ Objective, Independent and secure;
- ➢ Simple and Streamlined;
- ➢ Well-defined and understood;
- ➢ Automated;
- ➢ Scientifically and Statistically sound;

- Properly documented according to GDP.

6.3.2.1.3.4 Data collection and recording: All data collection and recording shall be performed following GDP and shall apply risk-based controls to protect and verify critical data.

6.3.2.1.3.5 **Data Processing:** To ensure data integrity, data processing shall be done in an objective manner, free from bias, using validated/qualified or verified protocols, processes, methods, systems, equipment and according to approved procedures and training programmes.

6.3.2.1.3.6 **Data Retention and Retrieval:** Retention of paper and electronic records is discussed in the section above, including measures for backup and archival of electronic data and metadata.

6.3.2.1.4 GOOD DOCUMENTATION PRACTICES:

6.3.2.1.4.1 The basic building blocks of good GxP data are to follow GDP and then to manage risks to the accuracy, completeness, consistency and reliability of the data throughout their entire period of usefulness that is, throughout the data life cycle.

6.3.2.1.4.2 Personnel shall follow GDP for both paper records and electronic records in order to assure data integrity. These principles require that documentation has the characteristics of being attributable, legible, contemporaneously recorded, original and accurate (referred to as ALCOA). These essential characteristics apply equally for both paper and electronic records.

6.3.2.1.4.3 Identify the risk; Controls to prevent and detect data integrity issues as per **CQA SOP "Quality Risk Management".**

6.3.2.1.4.4 Managing the life of the data (e.g. paper-based and/or electronic) from initial creation, review and approval, storage (including archival), through obsoletion (in accordance with data retention rules) as per **CQA SOP "Documentation and Data Control".**

6.3.2.1.4.5 Date and time shall be controlled as per **CQA SOP "Good Documentation Practices".**

6.3.2.1.4.6 Good Documentation Practices shall be followed through the life-cycle of documents as per **CQA SOP "Good Documentation Practices".**

6.3.2.1.4.7 Computer and Lab instruments timestamp shall be controlled.

6.3.2.1.4.8 Ensure policies and procedures define the requirements for both paper and electronic data and their usage.

STANDARD OPERATING PROCEDURE	
Department: Quality Assurance	**SOP No.:**
Title: Data Integrity Policy	**Effective Date:**
Supersedes: Nil	**Review Date:**
Issue Date:	**Page No.:**

Good Documentation Practices		
Requirement	**Paper Records**	**e-Records**
Legible	• Print name or use signature log	• Name associated to login ID
Contemporaneous	• Dated in sequence of actions	• Time/date stamped in sequence of actions
Permanent	• Pen (black or blue) • Don't use pencil or white out	• Audit modifications or deletions • Don't use annotation tools
Attributable	• Signature or initials	• Login or e-signature
Traceable	• Attach supporting data	• Link to supporting data
Time/Date Stamped	• Dated	• Time/date stamped
Changes	• Single line cross-out	• Audit trail

6.3.3 **DETECTION OF DATA INTEGRITY:** Data Integrity issue shall be detected / identified through following manner;

6.3.3.1 Data Review

6.3.3.2 Audits

6.3.3.3 **DATA REVIEW:**

6.3.3.3.1 Data shall be reviewed and, where appropriate, evaluated statistically after completion of the process to determine whether outcomes are consistent and compliant with established standards.

6.3.3.3.2 The evaluation shall be taken into consideration all data, including atypical, suspect or rejected data, together with the reported data. This includes a review of the original paper and electronic records.

6.3.3.3.3 The approach to reviewing specific record content, such as critical data fields and metadata such as cross-outs on paper records and audit trails in electronic records, shall meet all applicable regulatory requirements and be risk-based.

6.3.3.3.4 Whenever out-of-trend or atypical results are obtained they shall be investigated. This includes investigating and determining corrective and preventive actions for invalid runs, failures, repeats and other atypical data. All data shall be included in the dataset unless there is a documented scientific explanation for their exclusion.

6.3.3.3.5 During the data life cycle, data shall be subjected to continuous monitoring, as appropriate, to enhance process understanding and facilitate knowledge management and informed decision-making.

6.3.3.3.6 Document shall be reviewed by concerned department with Legible, Contemporaneous, Permanent, Attributable, Traceable, and Time/Date Stamped in routinely.

6.3.3.3.7 Original data include the first or source capture of data or information and all subsequent data required to fully reconstruct the conduct of the GxP activity. The GxP requirements for original data include the following:

- ✓ Original data shall be reviewed;
- ✓ Original data and/or true and verified copies that preserve the content and meaning of the Original data shall be retained;
- ✓ As such, original records shall be completed, enduring and readily
- ✓ Retrievable and readable throughout the records retention period.

6.3.3.3.8 Audit Trail Review:

Note: Audit trail review and Access and privilege control of software shall be performed as per respective Plant SOP.

6.3.3.3.9 Comprehensive Audit trail Review:

- ➢ Multiple processing of data to “pass”.
- ➢ Altering metadata to make results pass.
- ➢ Hiding or altering data on reports sent to QA.
- ➢ Uncovering persistent suspicious behavior around security of data.
- ➢ Deletion of data.
- ➢ Altering system policies /configuration / settings without change control procedures.
- ➢ To uncover possible cases of fraudulent behavior.

6.3.3.3.10 System Audit Trail:

- ➢ System audit trails shall be reviewed by QA authorized personnel only.
- ➢ System audit trails shall be reviewed in following manner.
  - ✓ Tracks actions of System Administrator.
  - ✓ Reviewed periodically based on risk.
  - ✓ Defined in Administrators responsibility.

6.3.3.3.11 Data Audit Trail:

- ➢ Data audit trails shall be reviewed by QA authorized personnel only.
- ➢ Data audit trails shall be reviewed in following manner.

- ✓ Tracks actions of users, reviewers, and approvers.
- ✓ Is reviewed when the data is reviewed.
- ✓ Defined in User Operational responsibility.

6.3.3.4 AUDITS:

6.3.3.4.1 The audit program will include periodic audits to confirm adherence to established requirements for data integrity.

6.3.3.4.2 Data Integrity inspection Check point as follows;

- ✓ Data entries
- ✓ Are printed data consistent with results recorded in the system?
- ✓ Calculation
- ✓ Data entered manually in worksheets
- ✓ Log Books entries and tractability
- ✓ Deviation / discrepancy reports
- ✓ Date/Signatures

6.3.4 ADDRESSING DATA RELIABILITY ISSUES:

6.3.4.1 Investigation / Corrective and Preventive Action:

6.3.4.1.1 Data Integrity and procedures to address data ownership throughout the lifecycle as per **SOP "Documentation and Data Control".**

6.3.4.1.2 Investigation with Root Cause Analysis shall be performed as per **CQA SOP "Root Cause Analysis".**

6.3.4.1.3 Corrective and preventive action shall be taken for compliances of data integrity issue as per **CQA "Corrective Action and Preventive Action (CAPA)".**

6.3.4.2 Impact Assessment

6.3.4.2.1 The investigation shall not be limited to the specific issue identified but should also consider potential impact on previous decisions based upon the data and systems found to be unreliable.

PHARMA DEVILS

QUALITY ASSURANCE DEPARTMENT

STANDARD OPERATING PROCEDURE	
Department: Quality Assurance	**SOP No.:**
Title: Data Integrity Policy	**Effective Date:**
Supersedes: Nil	**Review Date:**
Issue Date:	**Page No.:**

EXPECTATIONS FOR PAPER RECORDS AND ELECTRONIC RECORDS (BUT ARE NOT LIMITED TO)	
I.	**ATTRIBUTABLE**
	Paper Records
A.	Maintain a signature log for employees that work in respective Area (GxP AREA)?
B.	Are staffs trained in Good documentation Practices outlining that GxP records shall be initialed and dated?
C.	Attribution of actions in paper records should occur, as appropriate, through the use of;
D.	Initials of signature
E.	Full handwritten signature; Date and time
	Electronic Records
F.	Does the system use unique user login and privileges
G.	Are there audit trails in place recording the identity of operators entering, changing, confirming or deleting data?
H.	Does the system identify and record the person releasing or certifying the batches? Is an electronic signature used?
I.	Are staffs trained on the fundamentals of data integrity which emphasizes never to disclose their username or password with other staff?
II.	**LEGIBLE, TRACEABLE AND PERMANENT**
	Paper Records
A.	Are controls in place to ensure data is recorded using permanent indelible ink?
B.	Is the use of correction fluid, pencils and erasures prohibited?
C.	Is there controlled issuance of bound, paginated notebooks with sequential numbered pages?
D.	Are archiving of paper records performed by an independent, designated archivist?
E.	Are operators trained to use single-line cross outs accompanied by an initial and date when recording changes to a record?
F.	No use of opaque correction fluid or otherwise obscuring the record;
G.	Archival of paper records by independent, designated personnel insecure and controlled paper archives.
	Electronic records

STANDARD OPERATING PROCEDURE	
Department: Quality Assurance	**SOP No.:**
Title: Data Integrity Policy	**Effective Date:**
Supersedes: Nil	**Review Date:**
Issue Date:	**Page No.:**

EXPECTATIONS FOR PAPER RECORDS AND ELECTRONIC RECORDS (BUT ARE NOT LIMITED TO)	
H.	Use of secure, time-stamped audit trails that independently record operator actions and attribute actions to the logged-on individual.
I.	Is your stored data checked periodically for readability?
J.	configuration settings that restrict access to enhanced security permissions(such as the system administrator role that can be used to potentially turn off the audit trails or enable overwriting and deletion of data), only to persons independent of those responsible for the content of the electronic records
K.	Designing and configuring computer systems and writing standard operating procedures (SOPs), as required, that enforce the saving of electronic data at the time of the activity and before proceeding to the next step of the sequence of events
EXPECTATIONS FOR PAPER RECORDS AND ELECTRONIC RECORDS (BUT ARE NOT LIMITED TO)	
L.	(e.g. controls that prohibit generation and processing and deletion of data in temporary memory and that instead enforce the committing of the data at the time of the activity to durable memory before moving to the next step in the sequence).
M.	Is Application specific automated timer-outs?
N.	archived data checked periodically for readability?
O.	Is data backed up in a manner permitting reconstruction of an activity?
P.	Configuration settings and SOPs, as required, to disable and prohibit the ability to overwrite data, including prohibiting overwriting of preliminary and intermediate processing of data
III.	**CONTEMPORANEOUS**
Paper Records	
A.	Are staffs trained in Good documentation Practices emphasizing the importance of recording data entries at the time of activity?
B.	Are staffs trained in Good Documentation Practices emphasizing that it is improper to back date or forward date a record?
Electronic Records	
C.	Does your system automatically generate a timestamp?
D.	Do electronic signatures contain an automatically generated timestamp?
E.	Are users able to change the timestamp applied to record?
F.	Is data saves to unauthorized stored locations such as USB sticks?
G.	Are there sufficient availability of user terminals at the location where a GxP activity takes place?
IV.	**ORIGINAL**
Paper	

STANDARD OPERATING PROCEDURE	
Department: Quality Assurance	**SOP No.:**
Title: Data Integrity Policy	**Effective Date:**
Supersedes: Nil	**Review Date:**
Issue Date:	**Page No.:**

EXPECTATIONS FOR PAPER RECORDS AND ELECTRONIC RECORDS (BUT ARE NOT LIMITED TO)	
A.	Are sticky notes or order unofficial notepads permitted in GMP areas of facility?
B.	Are qualification/validation activities performed on original pre-approved protocols?
C.	Is there a controlled and secure area for archiving of records?
D.	Are original records readily available for inspection?
EXPECTATIONS FOR PAPER RECORDS AND ELECTRONIC RECORDS (BUT ARE NOT LIMITED TO)	
Electronic	
E.	Is it possible to print out batch release records, showing any data that has been changed since the original entry?
F.	Are your electronic signature permanently linked to their respective record?
G.	Does the personal processing the data have the ability to influence what data is reported or how it is presented?
H.	Does the system prevent deletion of original data?
I.	Is it possible to take screenshots and use shipping tools to manipulate data?
J.	Is metadata periodically reviewed?
V.	**ACCURATE**
Paper	
A.	Are forms, logbooks and notebooks formatted to easily allow for the entry of correct data?
B.	Are procedures in place to independently review original paper records?
C.	Are deviations and out of specification results investigated?
D.	Are laboratory instruments calibrated and maintained?
E.	Are secondary checks performed to check the accuracy of critical data?
F.	Are staffs pressured into meeting production targets, leading to compromised accuracy of records?
Electronic	
G.	Do interface contains built in checks for the correct and secure entry and processing of data?
H.	Does your system perform a check on the accuracy of critical data and configurations?
I.	Are system periodically reviewed?
J.	Are interfaces validated to demonstrate security and no corruption of data?
K.	Is archived data protected against unauthorized amendments?
L.	Linking paper print-outs to electronic records

7.0 ANNEXURES:

Not Applicable

8.0 DISTRIBUTION:

- Controlled Copy No. 01 — Corporate Quality Assurance
- Controlled Copy No. 02 — Quality Assurance, Central Warehouse & Central Stability
- Controlled Copy No. 03 — Corporate Information & Technology
- Controlled Copy No. 04 — Corporate Accounts
- Controlled Copy No. 05 — Corporate Purchase

- Controlled Copy No. 06 Corporate Human Resource
- Controlled Copy No. 07 Corporate Health & Medical Services
- Controlled Copy No. 08 Corporate Pharmacovigilance
- Controlled Copy No. 09 Corporate Environment, Health & Safety
- Controlled Copy No. 10 Corporate PPIC
- Controlled Copy No. 11 Corporate DRA
- Master Copy Corporate Quality Assurance

9.0 REFERENCES:

- WHO TRS No. 996 Annex-5 Guidance on Good Data and Record Management Practices (May 2016)
- Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments (Draft PIC/s Guidance August 2016)
- Data Integrity and Compliance with cGMP, Guidance for Industry (US FDA Draft Guidance April 2016)
- MHRA GxP Data Integrity Definitions and Guidance for Industry (Draft Version for consultation July 2016)

10.0 REVISION HISTORY:

CHANGE HISTORY LOG

Revision No.	Change Control No.	Details of Changes	Reason for Changes	Effective Date	Updated By