SOP TITLE**: PROCEDURE FOR MANAGEMENT OF DATA INTEGRITY SYSTEM OF PHARMEVO SITE**

1. **Objective:**

The objective of this document is to develop a system for management of Data Integrity system of PharmEvo site in the light of applicable Data Integrity guidelines and ALCOA++ principles.

1. **Scope:**

This procedure is applicable to all the systems (manual or electronic) which produce, process, store or archive GMP data and related meta data generated in response to various GMP activities executed at PharmEvo (Pvt.) Ltd manufacturing site. Training and awareness of staff w.r.t DI principles, DI non-conformances & their classification, DIRA and periodic DI surveillance.

1. **Reference:**
   1. 21 CFR part 11 and EU Annex 11
   2. “Annex 4- Guideline on Data Integrity”.  
       WHO Technical Report Series No. 1033, 2021
   3. PIC/S guidance (PI 041-1, 2021)  
      (Good practices for Data Management & Integrity in   
      regulated GMP/GDP environments)
2. **Responsibility:**
   1. Deputy Manager DI & Compliance/designee is responsible to prepare, review and execute this SOP.
   2. Chief Operating Officer is responsible for assuring that system is in place for regulation of data integrity system at site; also responsible to approve the DI sop.
   3. Deputy Manager DI & Compliance/designee is responsible for assuring that appropriate training has been provided to the site team including non-management staff to create awareness of this system.
   4. HOD / DI representative is responsible for assuring that necessary resources have been provided for the compliance of this system.
   5. Deputy Manager DI & Compliance/designee is responsible for monitoring and evaluation of the laid down procedures with respect to data integrity and recommendations for its compliance.
   6. QA Department is responsible for controlling of this SOP.
3. **Definitions:**
   1. Data Integrity: Practices to ensure the originality and accuracy of real time data.
   2. ALCOA: A framework to achieve data integrity.
   3. US FDA: United States Food & Drug Administration.
   4. EU: European Commission
   5. GDocP Good Documentation Practices
   6. DIRA Data Integrity Risk Assessment
   7. Meta Data Meta data are those data which provide contextual information required  
       to understand other data.
   8. Raw Data The original record (data) which can be described as the first capture of  
       information, whether recorded on paper or electronically. Raw data can  
       also be referred as source data.
   9. Audit trail Audit trail is a form of Meta data containing information associated with  
       actions that relate to creation, modification or deletion of GxP records.
   10. Data Life cycle The sequence of stages that a particular data goes through from its initial   
        generation or capture to its eventual archival and or deletion/destruction at  
        end of its useful life.
4. **Materials & Equipment:**

N/A

1. **Precautions:**
   * 1. Being a fundamental part of Pharmaceutical Quality Management System, the good documentation practices (GDocP) is the key to assure the integrity of data. The application of GDocPs may vary depending on the medium used to record the data i.e. either physical or electronic record but the principles are applicable to both.
2. **Procedure:**
   1. **General Requirement:**
      1. Some key concepts of GDocPs are summarized by the acronym ALCOA (Attributable, Legible, Contemporaneous, Original, & Accurate); which provides a framework to achieve data integrity. To this list, Complete Consistent Enduring and Available can be added (ALCOA+). A brief summary of acronym ALCOA++ has been illustrated below:
      2. Together these expectations ensure that events are properly documented and the data can be used to support informed decisions.
      3. Following table provide the guidance how to implement the ALCOA requirements:
         1. **Attributable:**

|  |  |
| --- | --- |
| **Attributable** means information is captured in the record so that it is uniquely identified as having been executed by the originator of the data (who performed an action and when a person or computer system). | |
| **Expectation for Paper Record** | **Expectation for Electronic Record** |
| Attribution of action in paper records should occur, as appropriate through the use of:   * Initials * Full handwritten signature * Personal seal * Date and, when necessary time | Attribution of action in electronic records should occur, as appropriate through the use of:   * Unique user logons that link the user to actions that create, modify or delete data; * Unique electronic signatures * An audit trail that should capture user identification (ID) and date and time stamp; * Signatures, which must be securely and permanently linked to the record being signed. |

* + - 1. **Legible & Enduring:**

|  |  |
| --- | --- |
| **Legible** the term legible, traceable and permanent refer to the requirements that data are readable, understandable and allow a clear picture of the sequencing of steps or events in the record to that all GXP activity conducted can be fully reconstructed by people reviewing these record at any point during the record retention period. (Must be readable throughout the entire lifecycle). | |
| **Expectation for Paper Record** | **Expectation for Electronic Record** |
| Legible, traceable and permanent controls for paper records include, but are not limited to:   * Use of permanent, indelible ink; * No use of pencil or erasures; * Use of single-line cross-outs to record changes with name, date and reason recorded (i.e., the paper equivalent to the audit trail). * No use of opaque correction fluid or otherwise obscuring the record; * Controlled issuance of bound, paginated notebooks with sequentially numbered pages (i.e. that allow detection of missing or skipped pages); * Controlled issuance of sequentially numbered copies of blank forms (i.e. that allow all issued forms to be accounted for); * Archival of paper records by designated Quality assurance personal in secure and controlled paper archives. * Preservation of paper/ink that fades over time where their use is unavoidable. | Legible, traceable and permanent controls for electronic records include, but are not limited to;   * Designing and configuring computer systems and writing SOPs, as required, that enforce the saving of electronic data at the time of activity and before proceeding to the next step of the sequence of events (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); * Use of secure time-stamped audit trails that independently record operator actions and attribute action to the logged-on individual: * 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 trail or enable overwriting and deletion of data), only to persons independent of those responsible for the content of the electronic records; * 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; strictly controlled configuration and use of data annotation tools in a manner that prevents data in displays and printouts from being obscured; * Validated backup of electronic records to ensure disaster recovery; * Validated archival of electronic records by independent. Designated archivist(s) in secure and controlled electronic archives. |

* + - 1. **Contemporaneous & Consistent**

|  |  |
| --- | --- |
| **Contemporaneous** – Data recorded at the time they are generated or observed or activity performed | |
| **Expectation of Paper Record** | **Expectation for Electronic Record** |
| Contemporaneous is recording of actions in paper records should occur, as appropriate through use of:   * Written procedures, training, review and audit and self-inspection controls that ensure personnel record data entries and information at the time of the activity directly in official controlled documents (e.g. laboratory logbooks, batch records, case report forms); * Procedures requiring that activities be recorded in paper records with the date of the activity (and time as well, if it is a time-sensitive activity); * Good document design, following chronological order and sequencing of steps to encourage good practices in documentations and ensure consistency of data as well; availability of blank forms/ documents in which the activities are recorded should be ensured; * Recording of data with time of activities using synchronized time sources (facility and computerized system clocks) which cannot be changed by unauthorized personal. Where possible data and time recording of manual activities (e.g. weighing) should be done automatically. | Contemporaneous recording of actions in electronic records should occur, as appropriate through use of:   * Configuration settings, SOPs and controls that ensure that data recorded in temporary memory are committed to durable media upon completion of the step or event and before proceeding to the next step or event in order to ensure the permanent recording of the step or event at the time it is conducted; * Secure system time/date stamps that cannot be altered by personal; * Procedures and maintenance programs that ensure time/date stamps are synchronized across the GXP operations; * Controls that allow for the determination of the timing of one activity relative to another (e.g. time zone controls); * Availability of the system to the user at the time of the activity. |

* + - 1. **Original**

|  |  |
| --- | --- |
| **Original**- 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. (Original record or a certified copy) | |
| **Expectation for Paper Record** | **Expectation for Electronic Record** |
| Controls for review of original paper records include, but are not limited to;   * Written procedure and training and review and audit and self-inspection controls to ensure that personnel conduct and adequate review and approval of original paper records, including those used to record the contemporaneous capture of information, * Data review procedures describing review of relevant metadata. For example, written procedures for review should require that personnel evaluate changes made to original information on paper records (such as changes documented in cross-out or data correction) to ensure these changes are appropriately documented, and justified with substantiating evidence and investigated when required. * Documentation of data review. For paper records this is typically signified by signing the paper records that have been reviewed. Where record approval is a separate process this should also be similarly signed. Written procedures for data review should clarify the meaning of the review and approval signatures to ensure that the people concerned understand their responsibility as reviewers and approvers to assure the integrity, accuracy. Consistency and compliance with established standards of the paper records subject to review and approval; * A procedure describing the actions to be taken if data review identifies as error or omission. This procedure should enable data corrections or clarification to be made in a GXP compliant manner, providing visibility of the original record and audit-trailed traceability of the correction, using ALCOA principles. | Controls for review of original electronic records include, but are not limited to;   * Written procedures and training and review and audit and inspection controls that ensure personnel original electronic records. Including human readable source records of electronic data; * Data review procedures describing review of original electronic data and relevant metadata. For example, written procedures for review should require that personnel evaluate changes made to original information in electronic records (such as changes documented in audit trails or history fields or found in other meaningful metadata) to ensure these changes are appropriately documented and justified with substantiating evidence and investigated when required; * Documentation of data review. For electronic records, this is typically signified by electronically signing the electronic data set that has been reviewed and approval. Written procedures for data review should clarify the meaning of the review and approval signatures to ensure that the personnel concerned understand to assure the integrity, accuracy, consistency and compliance with established standards of the electronic data and metadata subject to review and approval; * A procedure describing the actions to be taken if data review identifies and error or omission. This procedure should enable data corrections or clarifications to be made in a GXP compliant manner, providing visibility of the original record and audit trailed traceability of the correction, using ALCOA principles. |

|  |  |
| --- | --- |
| **Retention of Original Records or True Copies.** | |
| Controls for retention of original paper records or true copies of original paper records include, but are not limited to;   * Controlled and secure storage areas, including archives, for paper records; * A QA Person designated for archiving GXP paper records * Indexing of records to permit ready retrieval; * Periodic tests at appropriate intervals based upon risk assessment, to verify the ability to retrieve archived paper or static format records; * Written procedures, training review and audit, and self-inspection of processes defining conversion, as needed of an original paper record to true copy. | Controls for retention of original electronic or true copies of original electronic records include, but are not limited to.   * Routine back –up copies of original electronic records stored in another location as a safeguard in case of disaster that causes loss of the original electronic records; * Controlled and secure storage areas, including archives for electronic records; * A designated electronic archivist, should be suitably qualified and have relevant experience and appropriate training to perform their duties; * Indexing of records to permit ready retrieval; * Periodic tests to verity the ability to retrieve archived electronic data from storage locations. The ability to retrieve archived electronic data from storage locations should be tested during the validation of the electronic archive. * Written procedures, training. Review and audit and self-inspection of processes defining conversion. As needed, of original electronic records to true copy. |

|  |
| --- |
| **Accurate –** The term “accurate” means data are correct, truthful, complete, valid and reliable. For both paper and electronic records, archiving the goal of accurate data requires adequate procedures, processes, system and control that comprise the quality management system. The quality management system should be appropriate to the scope of its activities and risk based.  Controls that assure the accuracy of data in paper & electronic records include, but are not limited to;   * Qualification, calibration and maintenance of equipment, such as balances and PH meters, that generate printout; * Validation of computerized system that generate, process, maintain, distribute or archive electronic records; * System must be validated to ensure their integrity while transmitting between/among computerized systems; * Validation of analytical methods; * Validation of production processes; * Review of GXP records; * Investigation of deviations and doubtful and out-of-specification results; and * Many other risk management controls within the quality management system. |

* + - 1. **Accurate:  
           
         8.2 Data Integrity Surveillance:**Surveillance of functional GMP or related areas of PharmEvo factory premises with respect to Data Integrity principles shall be done as per following:
    1. Inspection of functional GMP or related areas shall be performed Quarterly by Deputy Manager Data Integrity & Compliance/designee by employing the “Data integrity Compliance Monitoring Checklist” (CDG/5/003). Prior to this inspection, a schedule shall be prepared as per format (CDG/5/002) “Quarterly Data Integrity Compliance Monitoring Schedule”.
    2. While preparing Quarterly Data Integrity Compliance Monitoring Schedule (CDG/5/002), a unique number will be assigned to each individual planned inspection and the same number will be assigned to the report prepared against the respective inspection. Each Number will consist of “9” digits as “DI/QX/001,

Where:

* + - 1. DI Stands for Data Integrity
      2. QX stands for particular quarter in which monitoring will be performed as Q1 for 1st quarter, Q2 for 2nd quarter and so on.
      3. 001 is the sequential number that will be followed as 001, 002, 003, ……. for each individual inspection of different departments. The sequential number will start from 001 for every quarter.
    1. Periodic DI monitoring of each department/function shall be performed in the presence of system owner and observations must be acknowledged by the user available at the time of review/monitoring.
    2. Observations from the periodic DI monitoring shall be accounted over Data Integrity Compliance Monitoring Report (CDG/5/004). HOD of concerned department shall acknowledge the observations mentioned on the report.
    3. Commensurate with the observations, an appropriate corrective/preventive action plan shall be developed through CDG/5/005 (Corrective & Preventive action plan for Data Integrity monitoring).
    4. The summary of Quarterly Data Integrity monitoring shall be discussed in the Management Review meeting.
  1. **Data Integrity Risk Assessment (DIRA):**
     1. Data Integrity Risk Assessment shall be carried out in order to identify and assess areas of risk associated with creation, processing, movement and management of GMP data.
     2. DIRA shall cover systems and processes that produce or store GMP data; how the system is acquiring and processing data and the inherent risks (procedure & practices). Examples include but not limited to paper based records employed for data capture (logbooks, standalone formats, batch records, reports), electronic records generated by computerized systems of CFR compliant manufacturing equipment, HPLC’s and other laboratory instruments, Data loggers etc.,
     3. Risk assessment of systems with regards to DI may be performed pro-actively (where the function is expecting a potential DI impact); or as a result of observations made during Quarterly DI monitoring or after implementation of DI CAPA’s in order to determine the residual risk. DIRA shall be conducted by a team comprising of area manager/HOD & DI representative and shall be documented using any standard FMEA template.
     4. In case risk assessment identifies areas for remedial actions specially where remedial action requires capital investment; then risk reducing short-term measures shall be implemented in order to provide acceptable data governance in the interim.
     5. Review of Data Integrity risks shall be performed once in a fiscal year. DI representative & departmental head/designee shall review the process and previously identified DI risks. In case of any changes in the system/process, the associated DI risks shall be assessed and documented as per template CDG/5/007 (DI risk review format).
  2. **Data Integrity Training & Awareness:**
     1. Training on Data integrity SOP shall be carried out once a month and shall comprise of management and non-management staff on an alternate basis.
     2. Refresher training on Data integrity policy shall be imparted to all site staff on annual basis.
     3. Data integrity awareness session to elaborate the core concept of data integrity shall be delivered once a month. Nominations prior to the session shall be taken by departmental managers.
     4. In case of DI SOP training, the SOP version shall be pre-approved. While in case of DI awareness session, the training material shall also be controlled and pre-approved.
  3. **Data Integrity Non-conformances:**

8.5.1 Non-conformances to Data Integrity principles (critical-major) if identified during  
 quarterly DI monitoring shall be properly investigated, documented as per CDG/5/006  
 (investigation form for Data Integrity non-conformance) and shall be dealt as per  
 DI policy of PharmEvo manufacturing site. Observations categorized as Minor, shall be taken on  
 the CAPA plan as per CDG/5/005.

8.5.2 A committee comprising of site’s HR representative, DI representative and HOD of concerned  
 department shall initiate an investigation over DI non-conformance; conclusion of investigation  
 shall be discussed with senior management and further actions shall be taken accordingly.

8.5.3 Reports of DI non-conformances shall be retained and a unique number shall be granted   
 for the purpose of tracking as “DI-NC-001-XXXX”.  
 where,   
 DI stands for Data Integrity  
 NC stands for Non-conformance  
 001 is the sequential number of each non-conformance  
 XXXX is the year during which the non- conformance was reported.

* 1. **Classification of Data Integrity Non-conformances:**

8.6.1 **Critical :** Critical Data integrity non-conformance can be defined as a state where it is observed that  
 data has been falsified or fabricated during QC testing, critical product / process parameter  
 or related documentation or due to negligence in the aforesaid tasks; that in-turn has a potential for  
 producing product which fails to meet marketing authorization specification at release or within  
 shelf-life.

8.6.2 **Major :** It can be described as a data integrity failure resulting from bad practices (due to  
 negligence in the assigned tasks) or poor documentation / record management practices. Data being misreported, e.g. original results ‘in specification’; but altered to give a more  
 favorable trend.  
 Reporting of a ‘desired’ result rather than an actual out of specification result when reporting  
 data which does not relate to QC tests, critical product or process parameters and thus has no  
 impact on product or patient safety.

8.6.3  **Other Deficiency (opportunity for failure due to absence of required data control  
 measures) – Minor** Badpractices or weak data controls which may result in probability for data integrity  
 issues or loss of traceability in documentation; limited failure in otherwise acceptable system.

* 1. **Considerations for Electronic records:**

8.7.1 Electronic records are considered equivalent as paper records and the conditions of ALCOA and  
 ALCOA plus principles are equally applicable on electronic records.  
  
8.7.2 Electronic data/records includes chromatograms obtained from HPLCs; data derived from FTIR,   
 UV spectrophotometers or other laboratory instruments with a stand-alone computerized system,  
 audit trails of change/modification/deletion of data from laboratory instruments, Data loggers,  
 manufacturing equipment or computerized systems (SAP, LIMS spectrum etc.,).  
  
8.7.3 Electronic data may be reviewed by DI representative during Quarterly DI monitoring or it may be  
 reviewed during DI or product related investigations. Departmental HOD’s/Managers may also  
 review audit trails on need basis.

* 1. **Operating Procedure for Quarterly Data Integrity Monitoring:**
     1. DM Data Integrity & Compliance / designee will develop schedule for quarterly Data Integrity compliance monitoring and get it approved preferably at start of each quarter.
     2. COO will approve the schedule of quarterly DI inspection.
     3. DM Data Integrity & Compliance / designee will circulate the approved schedule among the relevant stake holders.
     4. Departmental Head will nominate a representative to escort the DM Data Integrity & Compliance / designee for quarterly monitoring of identified system / function / department.
     5. DM Data Integrity & Compliance / designee will inspect the identified system / function / department against the format (CDG/5/003) “Data integrity Compliance Monitoring Checklist”.
     6. DM Data Integrity & Compliance / designee will collect the evidence & discuss the observation with the departmental Manager/representative and record on the Data Integrity Compliance Monitoring Checklist (CDG/5/003).
     7. Departmental Manager shall review the findings as observed by DM Data Integrity & Compliance / designee.
     8. In case of disagreement on any observation, guidance shall be taken by COO on the matter.
     9. DM Data Integrity & Compliance / designee will present the Data Integrity Compliance Monitoring Report (CDG/5/004) to the head of department within 15 days of monitoring/inspection.
     10. Respective HOD will acknowledge the report.
     11. COO will approve the report.
     12. Respective auditee will develop the Corrective and Preventive Action (CAPA) Plan for Data Integrity Monitoring (CDG/5/005) and get authorized by head of department. CAPA plan shall be  
         submitted to DI department within 15 days of receipt of audit report.
     13. DM Data Integrity & Compliance / designee will review & approve the CAPA plan.
     14. After approval of CAPA plan, respective departmental manager/designee shall be responsible to follow the CAPA plans and ensure closure of CAPA’s within the proposed timelines.
     15. DM Data Integrity & Compliance / designee shall be responsible to monitor and track status of open/closed CAPA’s with respect to each quarter.

1. **Training:**

Training on SOP will be imparted prior to the implementation of SOP and will be documented in QAG/5/142.

1. **Attachments:**

10.1. Quarterly Data Integrity Compliance Monitoring Schedule CDG/5/002

10.2. Data Integrity Compliance Monitoring Checklist CDG/5/003

10.3. Data Integrity Compliance Monitoring Report CDG/5/004

10.4. Corrective and Preventive Action (CAPA) Plan for

Data Integrity Monitoring CDG/5/005

10.5. Investigation Form for DI non-conformance CDG/5/006

10.6 DI risk review format CDG/5/007

1. **Distribution List:**
2. **SOP Review History:**