GRRMDP

Global Regulatory requirements for Good Manufacturing and Distribution practices in Pharmaceutical /Biopharma industries

RESPONSIBILITIES OF AN EMPLOYEE RELATED TO DATA RELIABILTY

- Every employee has a duty to engage in conduct to ensure that all stakeholders can trust employee decisions that are based on data and information that are accurate, truthful and complete.
- Every employee has a duty to perform their GXP functions in an ethical manner that meets company requirements and industry standards as articulated in the company requirements, and in accordance with all relevant laws, regulations and legislative directives of regulatory authorities.
- In order to verify paper records of GXP activities, the company shall establish and maintain Signature and Initial Logs (Table 1) for employees that work in GXP areas that include a handwritten specimen of the signature/initials of each employee. After reading and understood the responsibilities related to Data Reliability, each employee shall sign in the Signature and Initial Log.
- Every employee is required to collect, analyze, report and retain information and data in a manner that accurately, truthfully and completely represents what actually occurred, in either paper or electronic format or both, in accordance with company policies and procedures and applicable laws.
- Each employee shall receive annual refresher training on the Code of Conduct for Data Integrity.
- Every employee shall adhere to the requirements of the established documentation systems and are not permitted to record any raw data on unofficial, unauthorized or uncontrolled record.
- Employees must sign or initial on original records with date and time in a contemporaneous manner.
- Employees shall never record and signature or initials of another person or pre-date or back date entries on any record.

RESPONSIBILITIES OF AN EMPLOYEE RELATED TO DATA RELIABILTY

- Employees shall not discard, destroy or modify the raw data or original records in any way (other than at the end of prescribed retention period as provided by approved procedures).
- Employees shall not delete raw data or alter original records in a manner that obscures or obliterates the original entries. If changes are needed to correct errors, the original entries shall be retained along with entries that identify the person making the correction, and the date and reason for the correction.
- In order to verify paper records of GXP activities, the company shall establish and maintain Signature and Initial Logs for employees that work in GXP areas that include a handwritten specimen of the signature/initials of each employee.
- Employees must sign or initial original records in a contemporaneous manner, and must enter the date (and time if required by procedure) to accurately reflect who performed or witnessed the activity or who entered results or verified the accuracy of entries.

- Employees shall never record the signature or initials of another person or pre-date or back date entries on any record (either paper or electronic).

- Employees who enter data or verify accuracy of data or perform other activities including GXP data shall contemporaneously enter data in accordance with established policies and procedures.
- Employees shall not engage in any conduct that calls into question the reliability of data (such as falsifying data, making unauthorized changes, destroying, deleting or over-writing data.)

- Employees shall never record the signature or initials of another person or pre-date or back date entries on any record (either paper or electronic).

RESPONSIBILITIES OF AN EMPLOYEE RELATED TO DATA RELIABILTY

- Employees who perform review of batch production and control records as a condition of batch release shall adhere to established procedures and shall confirm that the records supporting batch release have been verified by second person for accuracy, truthfulness and completeness.
- If electronic data acquisition systems for GXP data are established, it must be ensured that the systems are configured, validated, and maintained in accordance with established industry standards intended to assure data integrity.
- The business processes shall include the establishment of written procedures that govern the collection, analysis, reporting and retention of electronic data including:
    - ✓ Procedural controls covering the use, correction, and movement of data, ensuring that data can be traced through every phase of its lifecycle. If the transfer of data is authorized, it must be controlled in a manner that provides traceability and retention for a period of time prescribed by applicable laws, regulations or legislative directives or longer if required by company policies and procedures.
    - ✓ Security controls to prevent and detect data deletion, over-writing, manipulation and/or omission of data.
    - ✓ Secure date and time stamps to permit detection and to prevent manipulation of records.
    - ✓ Secure data retention storage locations to prevent data from being saved to unauthorized file storage locations including removable devices.
    - ✓ System and procedural controls to provide for the reporting and evaluation of all data generated.

- Electronic records shall be attributable, legible, contemporaneous, traceable, time/date stamped and permanent.

RESPONSIBILITIES OF AN EMPLOYEE RELATED TO DATA RELIABILTY

- The company shall maintain and review audit trails for electronic GXP data that is required by company procedures or regulatory requirement.
- Reviews shall include periodic review of system audit trail logs against entries in transactional logs to verify that all events and data (including meta data) are being accurately and completely captured, reported and retained.
- Employees who enter data or verify data accuracy or perform other activities involving GXP data (such as collection, analysis, reporting or retention functions) shall contemporaneously enter data in accordance with established policies and procedures.
- Employees shall accurately enter and completely report all required data.
- Employees shall not engage in any conduct that calls into question the integrity of data (such as falsifying data, making unauthorized changes, or destroying, deleting or over-writing data).
- Employees shall provide factual information about any incident or event for which he/she may have firsthand knowledge about what happened.
- Employees who review or evaluate electronic data shall follow established procedures and verify that all required data and information have been included in relevant records and reports.
- Employees shall always enter data and information in a manner that accurately, truthfully and completely represents what actually occurred, and includes all testing results (if applicable).
- Any computer data acquisition system's Security measures shall include strict controls to prevent unauthorized access to computer system including use of unique user names and passwords or other biometric means to identify authorized users such as facial recognition, fingerprint readers, and iris scanners.
- Employees shall notify the Management if they become aware or have reason to suspect that other have falsified data, made unauthorized changes, caused

destruction or have indulged in any other conduct that calls into question the integrity of data.

- An employee shall not delay, deny or limit access to records or refuse to permit inspection by duly authorized officials of regulatory authorities, except as may be specified in a written procedure [e.g., to immediately notify executive management when an inspector arrives].
- Computer security measures shall include strict controls to prevent unauthorized access to computer system including use of unique user names and passwords or other biometric means to identify authorized users such as facial recognition, fingerprint readers, and iris scanners.
- Employees shall not disclose and/or share their user name and /or passwords with others, or use the username or password of another person to access computer files.
- Every employee is responsible to his/her own conduct in order to maintain a bond of trust between the company and its stakeholder, namely the patients, health care providers and regulators.
- Employees shall have the option of reporting such issues anonymously if they so choose and if local laws permit.
- Employees shall notify responsible management of the company if they become aware of any potential data integrity issue regardless of its cause.
- For example, employees shall immediately notify management if they are aware of or have reason to suspect others have falsified data, wrongful acts, made unauthorized changes, omissions, destroyed data or other conduct that calls into question the integrity of data.

GRRMDP

Global Regulatory requirements for Good Manufacturing and Distribution practices in Pharmaceutical /Biopharma industries

RESPONSIBILITIES OF AN EMPLOYEE RELATED TO DATA RELIABILTY

Table 1

Sl No	Name of Employee	Employee Code No.	DOJ	Dept.	Designation	Training	Signature / Date	Remarks