Government of India
Ministry of Science & Technology
Department of Science & Technology
National Good Laboratory Practice (GLP) Compliance Monitoring Authority

DEFINITIONS OF GENERAL TERMS USED IN NGCMA

Document No.GLP-111
Issue No. 04
Issue Date: May 09, 2022

NATIONAL GLP COMPLIANCE MONITORING AUTHORITY
DEPARTMENT OF SCIENCE AND TECHNOLOGY
TECHNOLOGY BHAVAN, NEW MEHRAULI ROAD
NEW DELHI-110 016
https://dst.gov.in/ngcma

DEFINITIONS OF GENERAL TERMS USED IN NGCMA

Good Laboratory Practice

Good Laboratory Practice (GLP) is a quality system concerned with the organizational process and the conditions under which non-clinical health and environmental safety studies are planned, performed, monitored, recorded, archived and reported.

Organization for Economic Co-operation and Development (OECD) Principles of GLP

OECD Principles of GLP were developed by an international group of experts established under the Special Programme on the Control of Chemicals. These principles of GLP were adopted by the OECD Council in 1981, as an Annex to the Council Decision on the Mutual Acceptance of Data (MAD) in the Assessment of Chemicals [C(81)30(Final)].

The purpose of these Principles of GLP is to promote the development of quality test data. Comparable quality of test data forms the basis for the MAD among countries. The application of these Principles should help to avoid the creation of technical barriers to trade, and further improve the protection of human health and the environment.

Terms Concerning the Organization of a Test Facility

Test Facility (TF): The persons, premises and operational unit(s) that are necessary for conducting the non-clinical health and environmental safety study. For multi-site studies, those which are conducted at more than one site, the TF comprises the site at which the Study Director is located and all individual test sites, which individually or collectively can be considered to be test facilities.

Multi-site Study: Any study that has phases conducted at more than one site. Multi-site studies become necessary if there is a need to use sites that are geographically remote, organizationally distinct or otherwise separated. This could include a department of an organization acting as a test site when another department of the same organization acts as the TF.

A phase is a defined activity or set of activities in the conduct of a study.

Test site: The location(s) at which a phase(s) of a study is conducted.

Test Facility Management (TFM): The person(s) who has the authority and formal responsibility for the organization and functioning of the TF according to the OECD Principles of GLP.

Test Site Management (if appointed): The person(s) responsible for ensuring that the phase(s) of the study, for which he/she is responsible, are conducted according to the OECD Principles of GLP.

Sponsor: An entity which commissions supports and/or summits a non-clinical health and environmental safety study.

Study Director: The individual responsible for the overall conduct of the non-clinical health and environmental safety study.

Principal Investigator: An individual who, for a multi-site study, acts on behalf of the Study Director and has defined responsibility for delegated phases of the study. The Study Director's responsibility for the overall conduct of the study cannot be delegated to the Principal Investigator(s); this includes approval of the study plan and its amendments, approval of the final report, and ensuring that all applicable OECD Principles of GLP are followed.

Quality Assurance Programme: A defined system, including personnel, which is independent of study conduct and is designed to assure TFM of compliance with the OECD Principles of GLP.

Standard Operating Procedures (SOPs): Documented procedures, which describe how to perform tests, or activities normally not specified in detail in the study plan or test guidelines.

Master Schedule: A compilation of information to assist in the assessment of workload and for the tracking of studies at a TF.

Terms Concerning the Non-Clinical Health and Environmental Safety Study

Non-clinical health and environmental safety study, henceforth referred to simply as "study", means an experiment or set of experiments in which a test item is examined under laboratory conditions or in the environment to obtain data on its properties and/or safety, intended for submission to appropriate regulatory authorities.

Short-term Study: A study of short duration with widely used routine techniques.

Study Plan: A document, which defines the objectives and experimental design for the conduct of the study, and includes any amendments.

Study Plan Amendment: An intended change to the study plan after the study initiation date.

Study plan Deviation: An unintended departure from the study plan after the study initiation date.

Test System: Any biological, chemical or physical system or a combination thereof used in a study.

Raw Data: All original TF records and documentation, or verified copies thereof, which are the result of the original observations and activities in a study. Raw data may also include, for example, photographs, microfilm or microfiche copies, computer readable media, dictated observations, recorded data from automated instruments, or any other data storage medium that has been recognized as capable of providing secure storage of information for a time period.

Specimen: Any material derived from a test system for examination, analysis or retention.

Experimental Starting Date: The date on which the first study specific data are collected.

Experimental Completion Date: The last date on which data are collected from the study.

Study Initiation Date: The date the Study Director signs the study plan.

Study Completion Date: The date the Study Director signs the final report.

Terms Concerning the Test Item

Test Item: An article that is the subject of a study.

Reference Item ("Control Item"): Any article used to provide a basis for comparison with the test item.

Batch: A specific quantity or lot of a test item or reference item produced during a defined cycle of manufacture in such a way that it could be expected to be of a uniform character and should be designated as such.

Vehicle: Any agent who serves as a carrier used to mix, disperse, or solubilise the test item or reference item to facilitate the administration/application to the test system.

Terms Concerning Computerized Systems

Acceptance Criteria: The documented criteria that should be met to successfully complete a test phase or to meet delivery requirements.

Acceptance testing: Formal testing of a computerised system in its anticipated operating environment to determine whether all acceptance criteria of the test facility have been met and whether the system is acceptable for operational use.

Authorisation concept: An authorisation concept is a formal procedure to define and control access rights to and privileges in a computerized system.

Back-up: Provisions made for the recovery of data files or software, for the restart of processing, or for the use of alternative computer equipment after a system failure or disaster.

Change Control: Ongoing evaluation and documentation of system operations and changes to determine whether a validation process is necessary following any changes to the computerised system.

Change Management: Change management is the process of controlling the life cycle of changes.

Commercial off-the-shelf (COTS) product: Software or hardware is a commercial off-the-shelf (COTS) product if provided by a vendor to the general public, if available in multiple and identical copies, and if implemented by the test facility management without or with some customization.

Computerised System: "A computerized system is a function (process or operation) integrated with a computer system and performed by trained personnel. The function is controlled by the computer system. The controlling computer system is comprised of hardware and software. The controlled function is comprised of equipment to be controlled and operating procedures performed by personnel." PIC/S PI 11-3 "Good Practices for Computerised Systems in Regulated GxP Environments"

Configuration: A configuration is an arrangement of functional units and pertains to the choice of hardware, software and documentation. It affects function and performance of the system.

Configuration Management: Configuration management comprises those activities necessary to be able to precisely define a computerised system at a certain time point.

Controlled function: Is a process or operation integrated with a computer system and performed by trained people.

Corrective and Preventive Actions: The concept of corrective and preventive actions focusses on the systematic investigation of the root causes of identified problems or risks in an attempt to prevent their recurrence or to prevent occurrence.

Customized computerised system: A computerised system individually designed to suit a specific business process.

Data approval: Data approval means locking data after collection, verification and e.g. transformation to make data suitable for use in records.

Data capture: Data capture are actions that typically take place to plan, collect, and verify data and associated metadata elements.

Data migration: Data migration is the activity of e.g. transporting electronic data from one computer system to another, transferring data between storage media or simply the transition of data from one state to another [e.g. conversion of data to a different format]. The term "data" refers to "raw data" as well as "metadata".

Deviation (incident) management: Deviation (incident) management comprises those activities to identify, document, evaluate and when appropriate, investigate in order to determine the originating causes of deviation (incident) to prevent recurrence.

Electronic record: Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

Hybrid solution (system): Co-existence of paper and electronic record and signature components. Examples include combinations of paper (or other non-electronic media) and electronic records, paper records and electronic signatures, or handwritten signatures linked to electronic records.

Life cycle: An approach to computerised system development that begins with identification of the user's requirements, continues through design, integration, qualification, user validation, control and maintenance, and ends when use of the system is retired.

Life cycle model: A life cycle model describes the phases or activities of a project from conception until the product is retired. It specifies the relationships between project phases, including transition criteria, feedback mechanisms, milestones, baselines, reviews, and deliverables.

Operating System: A programme or collection of programmes, routines and sub-routines that controls the operation of a computer. An operating system may provide services such as resource allocation, scheduling, input/output control, and data management.

Peripheral Components: Any interfaced instrumentation, or auxiliary or remote components such as printers, modems and terminals, etc.

Process: A process is a series of actions designed to produce a specified result. A process defines required activities and the responsibilities of the personnel assigned to do the work. Appropriate tools and equipment, procedures and methods define the tasks and relationships between the tasks.

Qualification: Action of proving that any equipment including software operates correctly and is fit for its purpose.

Recognised Technical Standards: Standards as promulgated by national or international standard setting bodies (ISO, IEEE, ANSI, etc.)

Regulated record: Is one required to be maintained or submitted by GLP regulations. A regulated record may be held in different formats, for example, electronic, paper, or both.

Risk: Combination of the probability of occurrence of harm and the severity of that harm.

Risk analysis: Estimation of the risk associated with the identified hazards. It is the qualitative or quantitative process of linking the likelihood of occurrence and severity of harms.

Risk assessment: Risk assessment consists of the identification of hazards and the analysis and evaluation of risks associated with exposure to those hazards. Risk assessment is followed by risk control.

Risk control: Process through which decisions are reached and protective measures are implemented for reducing risks to, or maintaining risks within, specified levels.

Risk identification: A systematic use of information to identify hazards referring to the risk question or problem description. Information can include historical data, theoretical analysis, informed opinions, and the concerns of stakeholders.

Risk management: The concept of quality risk management is described as "a systematic process" for the assessment, control, communication and review of risks to the quality.

Risk mitigation: Actions taken to lessen the probability of occurrence of harm and the severity of that harm.

Security: The protection of computer hardware and software from accidental or malicious access, use, modification, destruction or disclosure. Security also pertains to personnel, data, communications and the physical and logical protection of computer installations.

Software: A programme acquired for or developed, adapted or tailored to the test facility requirements for the purpose of controlling processes, data collection, data manipulation, data reporting and/ or archiving.

Source Code: An original computer programme expressed in human-readable form (programming language) which must be translated into machine-readable form before it can be executed by the computer.

User requirement specifications: User requirement specifications define in writing what the user expects the computerised system to be able to do.

User review: Review of user access rights and privileges

Validation: Action of proving that a process leads to the expected results. Validation of a computerised system requires ensuring and demonstrating the fitness for its purpose.

Validation strategy: The validation strategy defines in a document the process and all activities related to each stage of validation of computerised system.

Terms Concerning Data and Data Integrity

Data: Data are quantitative or qualitative facts, figures and statistics collected for reference or analysis. These include all original records and verified copies of original records, including raw

data and metadata and all subsequent transformations that are generated or recorded at the time of the GLP activity, and allow complete reconstruction and evaluation of the GLP activity.

Data can have different formats (e.g. analogue, digital) and structure, layouts (e.g. on paper or on screen), sources (e.g. chromatography charts, text, image, video, etc.), and media used to store or present (paper, DVD, photo film, tape, electronic files, etc.).

Raw data: The Principles of GLP define raw data as all original test facility records and documentation, or verified copies thereof, which are the result of the original observations and activities in a study and allow complete reconstruction and evaluation of the GLP activities. Raw data also may include, for example, photographs, microfilm or microfiche copies, computer readable media, dictated observations, recorded data from automated instruments, or any other data storage medium that has been recognized as capable of providing secure storage of information for a time period.

Record: A record is a piece of information (e.g. data). The term original record is used to describe the first source of information or data capture. Original records are generally raw data. If an original record meets the definition of raw data, but is not considered as such, this must be justified.

Verified copy: A verified copy is a faithful representation of the original at the time the copy is generated. A verified copy may be stored in a different format or document type to the original.

Derived data: Derived data are obtained and reconstructed from raw data (e.g. final concentrations as calculated by a spreadsheet relying on raw data obtained from an instrument; result tables as summarized by a Laboratory Information Management System (LIMS), etc.). Derived data are obtained by data processing.

Metadata: Metadata are data providing information used for the identification, description, and relationships of data. Metadata give data meaning, provide context, define structure, and enable retrievability across systems, and usability, authenticity, and auditability across time. For electronic data, parts of the metadata can be generated in audit trails. Metadata form an integral part of the data. Without the context provided by metadata, the data have no or limited meaning. The degree of metadata missing reduces the ability to interpret the data.

Audit trail: The audit trail is a form of metadata that contains information associated with actions that relate to the creation, modification or deletion of electronic data. An audit trail provides an automated secure way of recording life cycle details such as creation, additions, deletions or alterations of information in an electronic record without obscuring or overwriting the original record. An audit trail facilitates the reconstruction of the history of such events relating to the record, including the ‘who, what, when and why’ of the action.

Data structure: Data can have different structures.
Static format: A static record format, such as a paper or electronic record, is one that is fixed and allows no interaction between the user and the record content. For example, all paper records are static records. Electronic records that do not contain any link to other records that allow

interaction are also static records. A printout from a basic electronic balance, where no electronic data is stored, is an example of a static record from an electronic system.

Dynamic format: Records in a dynamic state are mostly electronic records that allow for an interactive relationship between the user and the record content. Examples of a dynamic format include chromatography data maintained as electronic records to allow the user to zoom on the baseline, to view the integration more clearly, or to have direct access via electronic links to the sequence of analysis, the table of results, the audit trails and the methods of acquisition and integration. Records electronically signed are also dynamic records as they contain a link with the authentication of the signature.

File structure: The way in which most of the electronic data are structured within the GLP environment will depend on what the data will be used for and the end user will almost always have this dictated to them by what software / computerized system is available.

*Flat files***:** A flat file consists of a single table of data, has no internal hierarchy and allows the user to specify data attributes i.e. its data structure is self-contained and limited. Flat files can be thought of as being similar to the files in a file cabinet drawer, a collection of single records each containing standalone data. The most commonly known flat file would be a .csv or .xls file or a Microsoft Word™ text only document.

Relational databases: Relational databases are a collection of tables linked together using a common piece of data, such as a study number, and can be arranged to highlight specific information for ad hoc queries. A relational database is a scalable and query friendly tool that provides the ability to capture a wide variety of data types. Relational databases are usually not used to record raw data. Relational databases store different components of associated data and metadata in different places. Each individual record is created and may be retrieved by compiling the data and metadata for review using a database reporting tool. For example, electronic records in a database format allows the user to track, trend and query data.

Electronic signature: An electronic signature is a signature in digital form that represents the hand-written ('wet') signatory. Different types of systems exist from simple ones (e.g. internal user identification with password) to complex systems of signatures (e.g. with an external, certified electronic signature service that provides with timestamp and encrypted information behind the signature). To be considered as an electronic signature in legal terms, the associated level of control required is defined where relevant by local regulation.

Data integrity: Data integrity is the degree to which data are complete, consistent, accurate, trustworthy and reliable and that these characteristics of the data are maintained throughout the data life cycle. Assuring data integrity requires appropriate quality and risk management systems, including adherence to sound scientific principles, good documentation practices and training of personnel.

Data quality: Data quality is the assurance that the data produced are generated according to applicable standards and fit for intended purpose. Data quality is assured by appropriate study design that accurately and scientifically addresses the experimental question and hypotheses

being studied and by the availability of adequate resources. Data quality affects the value and overall acceptability of the data in regard to decision-making or onward use.

Data life cycle: The data life cycle includes 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 approval*: Data approval is the act of authorizing data after collection, processing or verification to record that data are suitable for their intended use.
- *Transcription*: Transcription is the process where data are manually copied from a source into another record of data set. Transcription can occur when: o the same information is recorded in different records (for example, the date of arrival of the test item is recorded in multiple records such as logbooks or proformas); o data are entered into a computerized system for calculations. Transcription of manual records into an electronic system constitutes an example of a hybrid system.
- *Data processing*: Data processing is a sequence of operations performed on data in order to extract, present, calculate or obtain derived data in a defined format. Examples might include calculations in a spreadsheet, statistical analysis of individual test system data to present trends, or conversion of a raw electronic signal to a chromatogram and subsequently a calculated numerical result.
- *Data migration*: Data migration is the process of moving electronic data between different data storage types, computerized systems, or simply the transition of data from one format to another. This may include changing the format of data, but not the content or meaning, to make it usable or visible on an alternative computerized system.
- *Computerized system transaction*: A computerized system transaction is a single operation or sequence of operations performed as a single logical unit of work. The operation(s) that constitute(s) a transaction may not be saved as a permanent record on durable storage until the user commits the transaction through a deliberate act (e.g. pressing a save button, see also "data approval"), or until the system forces the saving of data.
- *Data retention*: Data retention is the storage of data which may be for the purpose of archiving (protected data for long-term storage) or back-up (electronic data or for the purposes of disaster recovery).
- *Back-up*: A data back-up is a copy of current data, metadata and system configuration settings maintained for the purpose of recovery including disaster recovery. Back-up allows for provisions made for the recovery of data files or software, for the restart of processing, or for the use of alternative computer equipment following a system failure or disaster.
- *Archive*: Archive means a designated area or facility (e.g. cabinet, room, building or computerized system) for the secure storage and retention of records and materials.

Data governance: Data governance is the sum total of arrangements to ensure that data (irrespective of the format in which they are captured, generated, recorded, processed, retained, archived and used) are attributable, legible, contemporaneous, original (or verified copy), accurate, complete, consistent, enduring and accurate (ALCOA+) throughout their life cycle. These arrangements can consist of a single standalone system or across a combination of systems within a test facility.

Terms Concerning GLP Compliance Monitoring

GLP Compliance Monitoring: The periodic inspection of TF(s) and/or auditing of studies for the purpose of verifying adherence to OECD Principles of GLP.

National GLP Programme: The particular scheme established by Government of India to monitor GLP compliance by TF(s) within its territories, by means of inspections and study audits.

National GLP Compliance Monitoring Authority (NGCMA): The authority set up by Government of India responsible for monitoring the GLP compliance of TF(s) within its territories and for discharging other functions related to GLP as may be nationally determined.

NGCMA Secretariat: The Secretariat of the NGCMA, located in Department of Science and Technology, Government of India.

GLP Inspector: A person, having the required qualification and training (as prescribed by the NGCMA), who performs the TF inspections and study audits on behalf of the NGCMA.

NGCMA categorizes its inspectors as:

a) **Lead Inspector**: The one who leads the inspection team during the inspection of the TF. He/ She prepare the agenda for the inspection, assign responsibilities to the inspection team members, lead the opening and the closing conferences and prepare the inspection report.

b) **Fellow Inspector**: Inspectors other than the lead inspector are fellow Inspectors. Their tasks during the inspection will be delegated by the lead inspector and will provide inputs for preparing the inspection report and will sign the inspection report.

c) **Technical Expert**: Head, NGCMA may appoint technical experts (Serving/ Retired) from Government departments/laboratories/universities, etc. for helping inspection teams from time to time in areas requiring specialized technical inputs, for making an assessment about GLP compliance. These experts shall have an exposure to OECD Principles of GLP. Their tasks during the inspection will be delegated by the lead inspector and they will provide inputs for preparing the inspection report and will sign the inspection report.

d) **Observer**: Inspectors under training are called observers and their task during each inspection will be identified by the lead inspector in consultation with Head, NGCMA. Observers will not need to sign the inspection report.

GLP Compliance Status: The level of adherence of a TF to the OECD Principles of GLP as assessed by the NGCMA.

GLP Certified Test Facility: A TF which has been granted GLP-compliance certificate by the NGCMA. All GLP certified TF(s) have to maintain their certification by paying prescribed annual certification fee.

Regulatory Authority: Any authority in any country or territory with legal responsibility for according market approval to chemicals and other aspects of the control of chemicals or items which are synthetic, of natural or biological origin and, in some circumstances, may be living organisms.

Study Audit: A comparison of raw data and associated records with the interim or final report in order to determine whether the raw data have been accurately reported, to determine whether testing was carried out in accordance with the study plan and SOPs, to obtain additional information not provided in the report, and to establish whether practices were employed in the development of data that would impair their validity.

Technical Committee (TC) on GLP: The Committee set up by the NGCMA to help the NGCMA in evaluating the competence of TF(s) by reviewing the inspection reports and giving recommendations on the grant of GLP-compliance certificate to the TF(s) or otherwise.

Legislation Committee: The Committee set up by the NGCMA to formulate legislation on GLP in India.

Test Facility Inspection: An on-site examination of the TF(s) procedures and practices to assess the compliance with OECD Principles of GLP. During inspections, the management structures and operational procedures of the TF are examined, key technical personnel are interviewed, and the quality and integrity of data generated by the TF are assessed and reported.

a. **Pre-Inspection:** A pre-inspection is carried out for new applicants, to establish whether the facility is ready for a final inspection.

b. **Final Inspection**: A final inspection is an inspection carried out, when a satisfactory Action Taken Report (ATR) to the pre-inspection is submitted by the TF. The final inspection is a complete facility inspection including study audits for detailed assessment of the TF, in accordance with OECD Principles of GLP and guidelines of the NGCMA, if any.

c. **Surveillance Inspection:** An inspection to ascertain on a regular basis (18±3months from the grant of GLP certificate), whether a GLP certified test facility continues to comply with the OECD Principles of GLP.

d. **Extension in Scope inspection:** An inspection done for a GLP certified TF wishes to extend the scope of its GLP certification during a GLP certification cycle. It includes facility inspection for the additional scope(s) applied by the TF and study audits for studies of each of the scopes/ areas of expertise.

e. **Re-certification inspection:** This refers to a GLP-inspection done after every three years, in case the TF continues to apply for re-certification at least six

months before the expiry of its existing GLP certificate. The re-certification inspection is similar to final inspection and includes a complete facility inspection and study audits for detailed assessment of the TF, in accordance with OECD Principles of GLP and Guidelines of the NGCMA, if any.

f. **Verification Inspection:** An inspection performed to verify the corrective actions mentioned in the ATR submitted by TF on major deviations observed during all inspections except pre-inspection. Verification inspection would be done more than once, at the discretion of NGCMA.

g. **Inspection/ Joint Inspection/ Study Audit on request of a Regulatory Authority/ Other Compliance Monitoring Authority**: Inspections/study audits conducted at the request of the Indian Regulatory Authorities (RA) or Compliance Monitoring Authorities (CMA)/ RA of OECD MAD adherent countries. Joint inspection alongwith the concerned RA or CMA may also be conducted, where applicable.

h. **Surprise Inspection:** Inspections undertaken without prior intimation to the certified TF under National GLP Programme to evaluate continued compliance to OECD Principles of GLP. These inspections shall be undertaken only with the approval of Chairman, GLP Authority.

Action Taken Report (ATR): Corrective actions taken by the TF towards the findings of an inspection, indicated by the inspection team during the closing conference.

Suspension of TF: Discontinuation of GLP certification of a TF for a defined period, as applicable.

Voluntary Withdrawal of GLP certificate: When a GLP certified TF no longer wishes to continue conducting GLP studies in accordance with OECD Principles of GLP, it voluntarily requests to NGCMA in writing that its GLP certification may be terminated. This is referred as "Voluntary withdrawal". Accordingly, the TF is placed under "Voluntary withdrawal category" by NGCMA and the status is published on NGCMA website.

Forced Withdrawal of GLP Certificate: When a GLP certified TF remains in "Suspended status" for three months and has not met the condition(s) for lifting the suspension even after three months, the GLP certificate of the TF is withdrawn by NGCMA. This is referred to as "forced withdrawal". The TF shall not claim GLP certification after forced withdrawal.

Complaint: Expression of dissatisfaction, other than an appeal, by any person or organization, against NGCMA or a Good Laboratory Practice (GLP) certified or applicant TF.

Complainant: Any individual/ organization/ body that is making a complaint.

Grievance: Expression of a real or imagined cause for complaint.

Appeal: A formal written request by a GLP certified or applicant TF for reconsideration of any adverse decision made by NGCMA related to the TF's certification status.

Appellant: A GLP certified or applicant TF filing an appeal.

Hearing: The process where the Complaints/ Grievances/ Appeal Committee hears oral arguments on an appeal presented by an appellant.