GENERAL DISTRIBUTION

OCDE/GD(95)115

OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING

NUMBER 10

GLP CONSENSUS DOCUMENT

THE APPLICATION OF THE PRINCIPLES OF GLP TO COMPUTERISED SYSTEMS

ENVIRONMENT MONOGRAPH NO. 116

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Paris 1995

OECD SERIES
ON
PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING

Number 10

GLP Consensus Document

THE APPLICATION OF THE PRINCIPLES OF GLP TO COMPUTERISED SYSTEMS

ENVIRONMENT MONOGRAPH NO. 116

Environment Directorate

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Paris 1995

FOREWORD

Within the framework of the third OECD Consensus Workshop on Good Laboratory Practice held 5th to 8th October 1992, in Interlaken, Switzerland, a working group of experts discussed the interpretation of the GLP Principles as applied to computerised systems. The working group was chaired by Dr. Theo Helder of the Dutch GLP Compliance Monitoring Authority. The Rapporteur was Mr. Bryan Doherty (Chairman of the Computing Committee of the British Association for Research Quality Assurance). Participants in the Working Group were from both national GLP compliance monitoring authorities and from testing laboratories in the following countries: Austria, Belgium, Denmark, Finland, France, Germany, Japan, the Netherlands, Switzerland, United Kingdom, United States. That Working Group was unable to reach consensus on a detailed guidance document in the time available to it. It did, however, develop a document entitled "Concepts relating to Computerised Systems in a GLP Environment", which set out the general principles and described the issues involved for each. That document was circulated to comments to Member countries.

In light of the comments received, the Panel on Good Laboratory Practice at its fifth meeting in March 1993, agreed that further work needed to be done and called for a second working group meeting to be held. Under the chairmanship of Dr. Helder, and with Mr. Doherty as rapporteur, that group met in Paris from 14th to 16th December 1994. Participants representing government and industry from Canada, Denmark, France, Germany, Japan, the Netherlands, Sweden, the United Kingdom and the United States took part.

The draft Consensus Document developed by the working group was based on the document emanating from the Interlaken workshop, comments from Member countries thereto and a document developed by a United Kingdom joint government-industry working party. It was subsequently reviewed, modified and endorsed by the Panel and the Joint Meeting of the Chemicals Group and Management Committee of the Special Programme on the Control of Chemicals. The Environment Policy Committee thus recommended that this document be derestricted under the authority of the Secretary-General.

GLP CONSENSUS DOCUMENT:

THE APPLICATION OF GLP PRINCIPLES TO COMPUTERISED SYSTEMS

Throughout recent years there has been an increase in the use of computerised systems by test facilities undertaking health and environmental safety testing. These computerised systems may be involved with the direct or indirect capture of data, processing, reporting and storage of data, and increasingly as an integral part of automated equipment. Where these computerised systems are associated with the conduct of studies intended for regulatory purposes, it is essential that they are developed, validated, operated and maintained in accordance with the OECD Principles of Good Laboratory Practice (GLP).

Scope

All computerised systems used for the generation, measurement or assessment of data intended for regulatory submission should be developed, validated, operated and maintained in ways which are compliant with the GLP Principles.

During the planning, conduct and reporting of studies there may be several computerised systems in use for a variety of purposes. Such purposes might include the direct or indirect capture of data from automated instruments, operation/control of automated equipment and the processing, reporting and storage of data. For these different activities, computerised systems can vary from a programmable analytical instrument, or a personal computer to a laboratory information management system (LIMS) - with multiple functions. Whatever the scale of computer involvement, the GLP Principles should be applied.

Approach

Computerised systems associated with the conduct of studies destined for regulatory submission should be of appropriate design, adequate capacity and suitable for their intended purposes. There should be appropriate procedures to control and maintain these systems, and the systems should be developed, validated and operated in a way which is in compliance with the GLP Principles.

The demonstration that a computerised system is suitable for its intended purpose is of fundamental importance and is referred to as computer validation.

The validation process provides a high degree of assurance that a computerised system meets its pre-determined specifications. Validation should be undertaken by means of a formal validation plan and performed prior to operational use.

The Application of the GLP Principles to Computerised Systems

The following considerations will assist in the application of the GLP Principles to computerised systems outlined above :

1. Responsibilities

a) *Management* of a test facility has the overall responsibility for compliance with the GLP Principles. This responsibility includes the appointment and effective organisation of an adequate number of appropriately qualified and experienced staff, as well as the obligation to ensure that the facilities, equipment and data handling procedures are of an adequate standard.

Management is responsible for ensuring that computerised systems are suitable for their intended purposes. It should establish computing policies and procedures to ensure that systems are developed, validated, operated and maintained in accordance with the GLP Principles. Management should also ensure that these policies and procedures are understood and followed, and ensure that effective monitoring of such requirements occurs.

Management should also designate personnel with specific responsibility for the development, validation, operation and maintenance of computerised systems. Such personnel should be suitably qualified, with relevant experience and appropriate training to perform their duties in accordance with the GLP Principles.

b) *Study Directors* are responsible under the GLP Principles for the overall conduct of their studies. Since many such studies will utilise computerised systems, it is essential that Study Directors are fully aware of the involvement of any computerised systems used in studies under their direction.

The Study Director's responsibility for data recorded electronically is the same as that for data recorded on paper and thus only systems that have been validated should be used in GLP studies.

c) *Personnel*. All personnel using computerised systems have a responsibility for operating these systems in compliance with the GLP Principles. Personnel who develop, validate, operate and maintain computerised systems are responsible for performing such activities in accordance with the GLP Principles and recognized technical standards.

d) *Quality Assurance* (QA) responsibilities for computerised systems must be defined by management and described in written policies and procedures. The quality assurance programme should include procedures and practices that will assure that established standards are met for all phases of the validation, operation and maintenance of computerised systems. It should also include procedures and practices for the introduction of purchased systems and for the process of in-house development of computerised systems.

Quality Assurance personnel are required to monitor the GLP compliance of computerised systems and should be given training in any specialist techniques necessary. They should be sufficiently familiar with such systems so as to permit objective comment; in some cases the appointment of specialist auditors may be necessary.

QA personnel should have, for review, direct read-only access to the data stored within a computerised system.

2. Training

The GLP Principles require that a test facility has appropriately qualified and experienced personnel and that there are documented training programmes including both on-the-job training and, where appropriate, attendance at external training courses. Records of all such training should be maintained.

The above provisions should also apply for all personnel involved with computerised systems.

3. Facilities and Equipment

Adequate facilities and equipment should be available for the proper conduct of studies in compliance with GLP. For computerised systems there will be a number of specific considerations:

a) *Facilities*

Due consideration should be given to the physical location of computer hardware, peripheral components, communications equipment and electronic storage media. Extremes of temperature and humidity, dust, electromagnetic interference and proximity to high voltage cables should be avoided unless the equipment is specifically designed to operate under such conditions.

Consideration must also be given to the electrical supply for computer equipment and, where appropriate, back-up or uninterruptable supplies for computerised systems, whose sudden failure would affect the results of a study.

Adequate facilities should be provided for the secure retention of electronic storage media.

b) *Equipment*

i) *Hardware and Software*

A computerised system is defined as a group of hardware components and associated software designed and assembled to perform a specific function or group of functions.

Hardware is the physical components of the computerised system; it will include the computer unit itself and its peripheral components.

Software is the programme or programmes that control the operation of the computerised system.

All GLP Principles which apply to equipment therefore apply to both hardware and software.

ii) *Communications*

Communications related to computerised systems broadly fall into two categories: between computers or between computers and peripheral components.

All communication links are potential sources of error and may result in the loss or corruption of data. Appropriate controls for security and system integrity must be adequately addressed during the development, validation, operation and maintenance of any computerised system.

4. Maintenance and Disaster Recovery

All computerised systems should be installed and maintained in a manner to ensure the continuity of accurate performance.

a) *Maintenance*

There should be documented procedures covering both routine preventative maintenance and fault repair. These procedures should clearly detail the roles and responsibilities of personnel involved. Where such maintenance activities have necessitated changes to hardware and/or software it may be necessary to validate the system again. During the daily operation of the system, records should be maintained of any problems or inconsistencies detected and any remedial action taken.

b) *Disaster Recovery*

Procedures should be in place describing the measures to be taken in the event of partial or total failure of a computerised system. Measures may range from planned hardware redundancy to transition back to a paper-based system. All contingency plans need to be well documented, validated and should ensure continued data integrity and should not compromise the study in any way. Personnel involved in the conduct of studies according to the GLP Principles should be aware of such contingency plans.

Procedures for the recovery of a computerised system will depend on the criticality of the system, but it is essential that back-up copies of all software are maintained. If recovery procedures entail changes to hardware or software, it may be necessary to validate the system again.

5. Data

The GLP Principles define raw data as being all original laboratory records and documentation, including data directly entered into a computer through an instrument interface, which are the results of original observations and activities in a study and which are necessary for the reconstruction and evaluation of the report of that study.

Computerised systems operating in compliance with GLP Principles may be associated with raw data in a variety of forms, for example, electronic storage media, computer or instrument printouts and microfilm/fiche copies. It is necessary that raw data are defined for each computerised system.

Where computerised systems are used to capture, process, report or store raw data electronically, system design should always provide for the retention of full audit trails to show all changes to the data without obscuring the original data. It should be possible to associate all changes to data with the persons making those changes by use of timed and dated (electronic) signatures. Reasons for change should be given.

When raw data are held electronically it is necessary to provide for long term retention requirements for the type of data held and the expected life of computerised systems. Hardware and software system changes must provide for continued access to and retention of the raw data without integrity risks.

Supporting information such as maintenance logs and calibration records that are necessary to verify the validity of raw data or to permit reconstruction of a process or a study should be retained in the archives.

Procedures for the operation of a computerised system should also describe the alternative data capture procedures to be followed in the event of system failure. In such circumstances any manually recorded raw data subsequently entered into the computer should be clearly identified as such, and should be retained as the original record. Manual back-up procedures should serve to minimise the risk of any data loss and ensure that these alternative records are retained.

Where system obsolescence forces a need to transfer electronic raw data from one system to another then the process must be well documented and its integrity verified. Where such migration is not practicable then the raw data must be transferred to another medium and this verified as an exact copy prior to any destruction of the original electronic records.

6. Security

Documented security procedures should be in place for the protection of hardware, software and data from corruption or unauthorised modification, or loss. In this context security includes the prevention of unauthorised access or changes to the computerised system as well as to the data held within the system. The potential for corruption of data by viruses or other agents should also be addressed. Security measures should also be taken to ensure data integrity in the event of both short term and long term system failure.

a) *Physical Security*

Physical security measures should be in place to restrict access to computer hardware, communications equipment, peripheral components and electronic storage media to authorised personnel only. For equipment not held within specific ’computer rooms’ (e.g., personal computers and terminals), standard test facility access controls are necessary as a minimum. However, where such equipment is located remotely (e.g., portable components and modem links), additional measures need to be taken.

b) *Logical Security*

For each computerised system or application, logical security measures must be in place to prevent unauthorised access to the computerised system, applications and data. It is essential to ensure that only approved versions and validated software are in use. Logical security may include the need to enter a unique user identity with an associated password. Any introduction of data or software from external sources should be controlled. These controls may be provided by the computer operating system software, by specific security routines, routines embedded into the applications or combinations of the above.

c) *Data Integrity*

Since maintaining data integrity is a primary objective of the GLP Principles, it is important that everyone associated with a computerised system is aware of the necessity for the above security considerations. Management should ensure that personnel are aware of the importance of data security, the procedures and system features that are available to provide appropriate security and the consequences of security breaches. Such system features could include routine surveillance of system access, the implementation of file verification routines and exception and/or trend reporting.

d) *Back-up*

It is standard practice with computerised systems to make back-up copies of all software and data to allow for recovery of the system following any failure which compromises the integrity of the system e.g., disk corruption. The implication, therefore, is that the back-up copy may become raw data and must be treated as such.

7. Validation of Computerised Systems

Computerised systems must be suitable for their intended purpose. The following aspects should be addressed:

a) *Acceptance*

Computerised systems should be designed to satisfy GLP Principles and introduced in a pre-planned manner. There should be adequate documentation that each system was developed in a controlled manner and preferably according to recognised quality and technical standards (e.g. ISO/9001). Furthermore, there should be evidence that the system was adequately tested for conformance with the acceptance criteria by the test facility prior to being put into routine use. Formal acceptance testing requires the conduct of tests following a pre-defined plan and retention of documented evidence of all testing procedures, test data, test results, a formal summary of testing and a record of formal acceptance.

For vendor-supplied systems it is likely that much of the documentation created during the development is retained at the vendor’s site. In this case, evidence of formal assessment and/or vendor audits should be available at the test facility.

b) *Retrospective Evaluation*

There will be systems where the need for compliance with GLP Principles was not foreseen or not specified. Where this occurs there should be documented justification for use of the systems; this should involve a retrospective evaluation to assess suitability.

Retrospective evaluation begins by gathering all historical records related to the computerised system. These records are then reviewed and a written summary is produced. This retrospective evaluation summary should specify what validation evidence is available and what needs to be done in the future to ensure validation of the computerised system.

c) *Change Control*

Change control is the formal approval and documentation of any change to the computerised system during the operational life of the system. Change control is needed when a change may affect the computerised system's validation status. Change control procedures must be effective once the computerised system is operational.

The procedure should describe the method of evaluation to determine the extent of retesting necessary to maintain the validated state of the system. The change control procedure should identify the persons responsible for determining the necessity for change control and its approval.

Irrespective of the origin of the change (supplier or in-house developed system), appropriate information needs to be provided as part of the change control process. Change control procedures should ensure data integrity.

d) *Support Mechanism*

In order to ensure that a computerised system remains suitable for its intended purpose, support mechanisms should be in place to ensure the system is functioning and being used correctly. This may involve system management, training, maintenance, technical support, auditing and/or performance assessment. Performance assessment is the formal review of a system at periodic intervals to ensure that it continues to meet stated performance criteria, e.g., reliability, responsiveness, capacity.

8. Documentation

The items listed below are a guide to the minimum documentation for the development, validation, operation and maintenance of computerised systems.

a) *Policies*

There should be written management policies covering, *inter alia*, the acquisition, requirements, design, validation, testing, installation, operation, maintenance, staffing, control, auditing, monitoring and retirement of computerised systems.

b) *Application Description*

For each application there should be documentation fully describing:

* The name of the application software or identification code and a detailed and clear description of the purpose of the application.
* The hardware (with model numbers) on which the application software operates.
* The operating system and other system software (e.g., tools) used in conjunction with the application.
* The application programming language(s) and/or data base tools used.
* The major functions performed by the application
* An overview of the type and flow of data/data base design associated with the application.
* File structures, error and alarm messages, and algorithms associated with the application.
* The application software components with version numbers.
* Configuration and communication links among application modules and to equipment and other systems.

c) *Source Code*

Some OECD Member countries require that the source code for application software should be available at, or retrievable to, the test facility.

d) *Standard Operating Procedures (SOPs)*

Much of the documentation covering the use of computerised systems will be in the form of SOPs. These should cover but not be limited to the following:

* Procedures for the operation of computerised systems (hardware/software), and the responsibilities of personnel involved.
* Procedures for security measures used to detect and prevent unauthorised access and programme changes.
* Procedures and authorisation for programme changes and the recording of changes.
* Procedures and authorisation for changes to equipment (hardware/software) including testing before use if appropriate.
* Procedures for the periodic testing for correct functioning of the complete system or its component parts and the recording of these tests.
* Procedures for the maintenance of computerised systems and any associated equipment.
* Procedures for software development and acceptance testing, and the recording of all acceptance testing.
* Back-up procedures for all stored data and contingency plans in the event of a breakdown.
* Procedures for the archiving and retrieval of all documents, software and computer data.
* Procedures for the monitoring and auditing of computerised systems.

9. Archives

The GLP Principles for archiving data must be applied consistently to all data types. It is therefore important that electronic data are stored with the same levels of access control, indexing and expedient retrieval as other types of data.

Where electronic data from more than one study are stored on a single storage medium (e.g., disk or tape), a detailed index will be required.

It may be necessary to provide facilities with specific environmental controls appropriate to ensure the integrity of the stored electronic data. If this necessitates additional archive facilities then management should ensure that the personnel responsible for managing the archives are identified and that access is limited to authorised personnel. It will also be necessary to implement procedures to ensure that the long-term integrity of data stored electronically is not compromised. Where problems with long-term access to data are envisaged or when computerised systems have to be retired, procedures for ensuring that continued readability of the data should be established. This may, for example, include producing hard copy printouts or transferring the data to another system.

No electronically stored data should be destroyed without management authorization and relevant documentation. Other data held in support of computerised systems, such as source code and development, validation, operation, maintenance and monitoring records, should be held for at least as long as study records associated with these systems.

Definition of terms[1]

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.

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.

Computerised System: A group of hardware components and associated software designed and assembled to perform a specific function or group of functions.

Electronic Signature: The entry in the form of magnetic impulses or computer data compilation of any symbol or series of symbols, executed, adapted or authorized by a person to be equivalent to the person's handwritten signature.

Hardware: The physical components of a computerised system, including the computer unit itself and its peripheral components.

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

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

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 (Application): 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.

Software (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.

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.

Validation of a Computerised System: The demonstration that a computerised system is suitable for its intended purpose.

[1] Further definitions of terms can be found in the "OECD Principles of Good Laboratory Practice".