The Quality Assurance Journal

Good Laboratory Practice (GLP). Guidelines for the Archiving of Electronic Raw Data in a GLP Environment†

Working Group on Information Technology (AGIT)*

Foreword

The aim of the present document is to provide guidance on the GLP-compliant archiving of electronic raw data. It will aid test facilities and promote the use of a common standard, but it should not be considered as a legal document. The present guidelines may evolve according to experience over the next few years and may also depend on interpretations made by other Organization for Economic Co-operation and Development (OECD) member countries.

The present guidelines were prepared by the Working Group on Information Technology (Arbeitsgruppe Informationstechnologie, AGIT). This group is made up of representatives from Swiss industry and from the Swiss GLP monitoring authorities, and its objective is to propose procedures that might appropriately be applied in test facilities to fulfil the regulatory requirements. However, the test facility management may use different approaches that are in compliance with the GLP principles.

Introduction

Computerized systems are used for the electronic acquisition, maintenance, modification, reporting, archiving and retrieval of electronic records. The benefits of computerized systems include the possibility of further processing and analysing electronic raw data.

A critical issue as regards electronic data systems is the long-term archiving and retrieval of electronic raw data. These guidelines are based on the Swiss Ordinance on GLP [1], the OECD GLP principles [2] and OECD Consensus Document No. 10 [3].

Other relevant guidelines, e.g. FDA 21 CFR Part 11 [4], are considered where appropriate. However, the scope and application of 21 CFR Part 11 is under discussion [5].

In the official GLP regulations, the meaning of electronic raw data is not specified in enough detail for it to be used easily in practice. The archiving of electronic raw data in conformity with GLP principles requires a comprehensive understanding of the nature of electronic raw data. Therefore, the intention of this document is to clarify important aspects of electronic raw data.

Scope

This document provides guidance on:

- Regulatory (GLP) requirements for electronic archiving
- The integrity of archived electronic raw data
- The availability of electronic raw data during the required retention period
- Long-term considerations of archiving to meet GLP requirements

The following items are not considered in depth in this document:

- Special requests from the registration authorities, such as specific data formats allowing reprocessing of data
- Special data formats to generate historical data pools, such as company-wide data warehousing

*Correspondence to: Dr Hans Peter Saxer, BUWAL, CH-3003 Bern, Switzerland.
E-mail: hanspeter.saxer@buwal.admin.ch

†Reprinted by kind permission of AGIT (Arbeitsgruppe Informationstechnologie) or the Working Group on Information Technology made up of representatives from Swiss industry and from the Swiss GLP monitoring authorities. This article was first released in May 2003 and can be accessed at http://www.glp.admin.ch/legis/ArchElectRawData1_0.pdf

DOI: 10.1002/qaj.244

Electronic Raw Data

Definition of electronic raw data

Raw data are defined in the Swiss Ordinance on GLP [1] as follows:

Raw data means all original test facility records and documentation, or verified copies thereof, which are the result of the original observations and activities in a study. 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… for at least 10 years.

OECD Consensus Document No. 10 does not give precise information on electronic raw data, so raw data should be defined for each computerized system [3].

Other countries, such as the USA, EU member states and Japan, have slightly different interpretations of electronic raw data, but do not give complete clarity and guidance on this complex topic.

For the purpose of the present guidelines, the following definition of the term electronic raw data and its various forms are given below.

Electronic Raw Data: Original test facility records generated by means of computerized systems and stored on digital media. In a broader sense this may include data processed subsequently, and stored on digital media, which are necessary for reconstruction and evaluation of the final results.

Binary Form: Refers to any digital encoded data, which need a decoding system to be read and worked on.

Human Readable Form: A file format that can be interpreted by standard software to view the content as text, figures, graphs, tables, etc.

Components of electronic raw data

Based on GLP requirements, raw data (including electronic raw data) have to be archived. No specific requirements regarding the data format are specified. However, in order to ensure readability throughout the retention period, it should be possible to retrieve the raw data in electronic and human readable form as required by 21 CFR Part 11 [4].

Electronic raw data are considered as the data themselves and their related meta-data. The data represent the core data elements (measured values), whereas meta-data are considered as the attributes of the measured values (e.g. study number, time, sample identification) and technical properties (e.g. field properties, table relationships, keys etc.).

Additionally, all changes to electronic raw data have to be recorded in an audit trail specifying the original and modified data, the reason for the change, the date and time, and the identity of the person changing the data.

In analogy to the requirement for handwritten signatures in paper-based systems, an electronic signature is required for electronic raw data generation [1,4]. Currently, specific controls for electronic signatures have only been described in FDA Guidelines no. 21 CFR Part 11 [4]. Further *legal* regulations for digital signatures are described in the Swiss Ordinance on Electronic Certification [6].

Critical issues concerning raw data

For each computerized system, the electronic raw data have to be defined with respect to the measured values, their meta-data, audit trail specifications and electronic signatures.

To be able to generate electronic raw data in a human readable form the relationship between the data components as defined has to be maintained during the whole life cycle of the electronic raw data (recording, changes, maintenance and archiving).

For the time being, paper records cannot be avoided, even for the most sophisticated electronic raw data acquisition system:

- Contingency concept for raw data recording (system failure)
- Paper based raw data records, e.g. ECGs, photos, notes, X-ray films, correspondence etc.

- Computer system validation and system documentation records.

When paper based raw data have to be scanned or entered manually into a computerised system, the paper based raw data represent the original raw data and should be handled and archived as required by GLP principles. However, if the transformation of the paper based raw data into an electronic form is performed by validated procedures the electronic form obtained can be considered as a certified copy.

The question of whether printouts of electronic raw data can be considered as the raw data is discussed in FDA regulations [4,5].

Specific electronic data formats

Both analogue and digital recording systems are now available on the market.

- Digital systems (digital cameras, NMR/MS/UV/VIS spectrometers, radioluminographs, digital voice-recorders etc.) store information in structured files, which can be handled like other digital electronic records. However, 'off the shelf' audio or video systems do not support electronic signatures, audit trails etc. and should be addressed accordingly.
- Analogue systems (voice-recorders, video-recorders etc.) store information unstructured on magnetic tape and cannot be considered as electronic raw data in the sense used in the GLP principles. Such data media should be archived as described in principle 10 of the Swiss GLP Ordinance [1].

Roles and Responsibilities

Test facility management

The test facility management should:

- Designate personnel with specific responsibility for the management of the electronic archives. Such personnel should be suitably qualified, and have relevant experience and appropriate training to perform their duties in accordance with the GLP Principles. If parts of the archiving process are not covered by the personnel of the test facility, the test facility management has to ensure that GLP principles are fulfilled by the service provider, e.g. via a service level agreement. The test facility management has to ensure that all personnel involved are qualified and properly trained for the specific purpose.
- Ensure that appropriate facilities, equipment, and materials and SOPs are available and that electronic archiving systems are suitable for their intended purpose and are validated, operated and maintained in accordance with the principles of GLP.
- Establish procedures for all aspects of the life cycle of archived electronic raw data, i.e. archiving, amending, maintaining, migration, reformatting, conversion, retrieval and deletion.

Study director

The study director should ensure the proper archiving of all data related to the study, including any electronic raw data [2]. The final report should specify where all data related to the study are to be stored.

Archivist/IT Personnel

The archivist is responsible for all aspects of electronic archiving. He/she should have full control of all activities within the archiving process. If there is external IT involvement (service provider), the archivist has to ensure that the procedures are followed as described in the relevant service level agreements or contracts. The IT person(s) involved have to fulfil GLP requirements such as maintaining job descriptions, training records and CVs etc.

Quality assurance unit (QAU)

The QAU is responsible for inspecting all aspects of archiving for compliance with GLP. This includes the inspection of archiving procedures for electronic raw data, IT infrastructure,

electronic archives, archived studies and documents concerning the personnel. If there is external IT involvement, their activities should be included in test facility based inspections. All findings should be reported to the test facility management.

The QAU should be qualified in terms of IT knowledge and properly trained in the corresponding archive systems to be able to inspect electronic archiving procedures.

Archiving of Electronic Raw Data

Electronic archiving

The archiving of electronic raw data means the process of protection against loss, modification, and unauthorized access. The availability of controlled amendment procedures and readability should be assured at any time during a predefined retention period.

Timing of archiving

Electronic raw data should be archived after completion of the study (final report signed by study director) as for all other study raw data (paper, slides etc.).

Archiving options

Off-line archiving

Electronic raw data should be stored on read-only data media (e.g. CD-Rom, DVD) and archived within the test facility archives.

The stored electronic raw data should be well protected against accidental data changes and physically separated from the productive system. The types of medium selected should provide long-term readability (magnetic media are less favourable in this respect). Due to the physical separation of the data media, the maintaining of the overall index and the amending procedures may be difficult to handle. In addition, direct access to the data for any form of data warehousing or data mining is not feasible.

On-line archiving

On-line archiving can be achieved either using a dedicated electronic archive system (physically separated) or a productive system, by marking the electronic raw data explicitly as archived (logically separated). In any case the archived electronic raw data should have read-only status for all system users. It must be ensured that archived electronic raw data are never changed even not by the system administrator.

The requirements for archived systems with respect to physical access to the system, restricted numbers of system administrators, system maintenance, and data protection will be more easily achievable using a dedicated electronic archive system. In both options, historical electronic data are directly accessible for further evaluation purposes.

Archiving process

The archiving process should fulfil the following requirements:

- For each study, the order of the study director to archive study data should include a full index of all necessary information about the electronic raw data.
  For a file system, the index should include file name, file identification, location, application version, etc.
  For a database system, key attributes are needed as index, e.g. study number, instrument, application version, date, sample number, etc.
- The status of the electronic raw data should be changed from 'productive' to 'archive' (off-line or on-line).
- In case of physical separation of the electronic archive the electronic raw data should be moved from the source to the archive destination.
- The proper and secure transfer of electronic raw data to the archive has to be verified and documented.
- The index of the archive inventory should be kept up to date.

- The archivist should give confirmation to the study director that the archiving process has been completed.

It is recommended that (as for paper records) all information be frozen at the time of archiving. For on-line archiving, it is important to freeze historical results and report formats, including company name, department names, user names, etc.

The archiving process for electronic raw data should be described in an SOP and performed by validated procedures.

Interactions between the study director, the archivist and IT personnel involved at any stage of the archiving process should be documented.

Operation of Electronic Archives

Requirements for storage conditions

The usual storage requirements for paper archives also apply to electronic archives. In addition, the following should be ensured:

- Storage conditions are appropriate with respect to the particular sensitivity of the media to heat, humidity, and electromagnetic radiation.
- If data media are not stored in the regular paper GLP archives, such media should be stored in a fire-proof lockable cabinet identified as GLP archives, with access to authorized persons only.
- It is recommended that security copies (backups) of archived electronic raw data be kept off-site. The storage conditions should be equivalent to those required for GLP archives.

Regular activities

The usual archiving requirements for paper archives also apply to electronic archives. In addition, it should be ensured that the following activities are carried out and documented:

- An index of all data media, with the table of contents, and associated software versions should be maintained and the index kept up to date.
- Any checking in and checking out of data and/or data media (who, what, when) should be documented by an audit trail of the electronic archive system.
- It should be checked that user access to the archived data is restricted to read only, to prevent any changes.
- The readability of the archived data should be checked at appropriate intervals.
- Depending on the storage media used, these should be renewed and reformatted at appropriate intervals.

Change management for archived electronic raw data

Long-term access to archived data requires processes to copy, convert or migrate archived data to newer technologies. When there are software changes in the productive systems, or a system will be retired, procedures have to be in place to initiate a risk assessment of the readability and retrieval of archived data. Based on the result of the risk assessment, the test facility management should take a decision on any change management necessary for the archived data. A general SOP should be established for the following procedures, and the procedures should be recorded and documented.

Copying archived data

The copying of archived data is considered to have the least influence on their integrity. This should be carried out if there is a need to copy electronic data from their current storage medium to a new medium, i.e. change of medium (tape to CD), medium refreshment (tape to tape, CD to CD) or a change in the location of the archives (server to server). Depending on the operating system, the file size and structure may be changed, e.g. FAT to NTFS; however, data integrity is not affected by copying.

Suitable methods and utilities, validated for the intended purpose should be used. The time schedule for a media refresh should be

appropriate to specifications of medium degradation, ensuring the minimum loss of records kept in long-term storage. In any case the replication should not result in any loss of content, structure, or context of the archived data.

Converting archived data

It may be necessary to convert archived data when there are changes in the version of software. This involves the transfer of archived data from one application environment to another, newer application environment with little or no change of information that would compromize the content, structure, and context of the archived data preserving its authenticity. In most cases the only difference is the underlying binary structure (bit stream) of the electronic stored data. However a pilot conversion and validation should be performed prior to the conversion of archived data.

Where the format of the archived raw data and/or the functionality of the application exclude data conversion, migration strategies may have to be considered. In any case, the decision to carry out data conversion or the migration of archived data should be taken by the test facility management.

Migrating archived data

Data migration is the process of transferring electronic data from one computer platform to another in an environment that does not provide automatic conversion between the platforms. Migration is considered to have the greatest impact on the archived data. It requires the development of software or procedures to interpret the data structure of the legacy system and convert them to the format of the new system. The main objective of a migration strategy should be to preserve the integrity and usefulness of the data. Data that have migrated should be readable, identifiable, retrievable, intelligible, and authentic. The processing of the migrated data within the new system should lead to the same results as before. However, there is a considerable risk that some information may be lost during migration, as a result of incompatibilities between the systems. It is an essential objective of the validation of the migration process to determine this unavoidability loss. The impact of this loss on further outcome of data interpretation has to be known.

In the procedure for system migration, the following steps have to be carried out and documented:

- Analyse the original computer environment and data, to give the mapping content, structure, and context of data.
- Understand the impact and risk of the loss of data or of data attributes, and minimize any such risk as much as possible.
- Engineer the new environment to preserve the best level of data content, data structure, and data context after migration.

Retrieval of electronic raw data

For audits and inspections carried out by the authorities or by QAUs, electronic raw data and audit trails should be made available in a human readable form in good timely manner.

If regulatory and/or internal requirements make further data processing/interpretation necessary, the electronic raw data should be copied to a productive system. Data processing should be performed only on the copied data. If the new evaluation results in a different interpretation, an amendment process should be initiated. All data generated during such a process should be archived in addition to the original raw data.

Electronic raw data deletion

It is recommended that the archivist notifies the test facility management after the defined retention period, which is at least 10 years according to the Swiss GLP Ordinance. It should be taken into account that regulatory authorities usually require longer periods of data retention for registered products.

The test facility management should decide on the further retention of the electronic raw data or initiate their deletion. In any case, this decision should be documented.

Critical Issues

Retirement of a computerized system

If the archived electronic raw data are only interpretable by the original application software the following options should be considered prior to the retirement of the computerized system:

Data migration to a follow-up system

Data migration is considered as the preferred option, keeping both the electronic raw data and the possibility of generating a human readable form.

Maintaining of retired systems

If the result of the risk assessment concludes that an unacceptable change of data integrity may occur after data migration, or if a follow-up system is not available, the conservation of the computerized system (hardware and/or software) may be appropriate. However, this option is considered as unsuitable for long-term storage of electronic raw data, since maintaining outdated systems involves increasing effort, cost, and risk during the retention time.

Maintaining electronic raw data only in human readable form

If neither of the above options can be applied, the storage of electronic raw data in human readable form might be a least desired alternative. However, acceptance of this approach by the different registration authorities cannot be considered as certain. In the case of system retirement the amount of archived electronic raw data that has to be transferred into a human readable form may create a substantial effort. Therefore it may be appropriate to store at the time of archiving both the binary and human readable form of the electronic raw data.

References

1. Ordinance relating to Good Laboratory Practice of 2 February 2000 [RS 813.016.5] as last amended on 16 November 2001.
2. OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring No. 1: OECD Principles of Good Laboratory Practice (as revised in 1997). Environment Directorate, OECD, Paris, 1998.
3. OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring No. 10: GLP Consensus Document. The Application of the Principles of GLP to Computerised Systems. Environment Monograph No. 116; Environment Directorate, OECD, Paris, 1995.
4. Electronic Records; Electronic Signatures; 21 CFR Part 11 (Rule 11), US Food and Drug Administration, 20 March 1997.
5. Guidance for Industry – Part 11, Electronic Records; Electronic Signatures – Scope and Application, Draft Guidance, February 2003.
6. Verordnung über Dienste der elektronischen Zertifizierung [RS 784.103] vom 12. April 2000 (Stand am 23. Mai 2000)

Literature

Einsatz computergestützter Systeme bei GLP-Prüfungen; Vorschläge der Projektgruppe GLP und EDV des Arbeitskreises GLP im Verband der Chemischen Industrie e.V.: Pharm. Ind. 59, 1, 24–29. 2, 116–120 (1997).

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

Good Automated Laboratory Practices (GALP), US Environmental Protection Agency, 1995.

Good Automated Manufacturing Practice (GAMP), GAMP Forum, 8 November 1999: Complying with 21 CFR Part 11: Electronic Records and Electronic Signatures.

Definition of Raw Data, British Association of Research Quality Assurance, November 1994.

Archiving Electronic Data: 1.Transfer to Archives, 2.Data Maintenance, 3.Long Term Considerations, British Association of Research Quality Assurance (October/December 1994).

Working Group on Information Technology (AGIT)

The Working Group on Information Technology (AGIT) was founded on 27 March 1998 with the

objective of discussing relevant problems of Good Laboratory Practice (GLP) in the field of information technology between industry and the monitoring authorities.

The AGIT intends to set up guidelines based on legislative requirements and practical experience to support test facilities introducing information technology tools to computerized systems in practice. OECD Consensus Document number 10 on the application of the principles of GLP to computerized systems is used as a basis for the discussions.

The members of the AGIT are representatives from the Swiss GLP monitoring authorities (Gérard Donzé, Swiss Federal Office of Public Health; Hansruedi Hartmann, Swissmedic, Swiss Agency for Therapeutic Products; Hans Peter Saxer, Swiss Agency for the Environment, Forests and Landscape), and representatives from industry (Peter Esch, Novartis Pharma AG; Stephan Hassler, Syngenta Crop Protection AG; Uwe Timm, F. Hoffmann-La Roche AG; Bruno Eschbach, PDS Pathology Data Systems AG; Leo Hutter, RCC Ltd.).

The AGIT has selected the following topic to be discussed in the near future:

- Acquisition, handling, and documentation of electronic raw data in a GLP environment.

For the convenience of users, AGIT publications are available on the Swiss GLP Home Page www.glp.admin.ch, subtopic legislation.

Furthermore, links and references to guidelines, laws and regulations, definitions, relevant literature, training courses, workshops etc. are given on the Swiss GLP Home Page.

AGIT Publications (as of May 2003):

GUIDELINES FOR THE VALIDATION OF COMPUTERISED SYSTEMS (Version 01, June 2000)

GUIDELINES FOR THE MANAGEMENT OF ELECTRONIC SOPS IN A GLP ENVIRONMENT (Version 01, July 2001)

GUIDELINES FOR THE ARCHIVING OF ELECTRONIC RAW DATA IN A GLP ENVIRONMENT (Version 01, May 2003)