Chapter 10. Storage and retention of records and materials

Key message: *Before collecting data from in vitro methods it is important to assess the format of collection, the complexity involved and requirements for traceability, storage, verification and transmission of data.*

Key content: *The chapter gives insight on what key records and materials to archive and retain. It also details adequate document and record management of processes and the traceability of origin of materials.*

Guidance for improved practice: *Data integrity arrangements must be in place and structured methods and essential process components are described for both paper-based and electronic data to ensure that the collected in vitro method data are attributable, legible, contemporaneous, original and accurate.*

Recommendations *are detailed for the necessary procedures related to retention, archiving, retrieval, backup and restoration for all target groups involved in the in vitro method lifecycle.*

It is imperative that the historical data, paper-based or in the form of electronic data, are effectively managed so as to prevent any data integrity issues as this data may be requested when submitting the method for formal validation.

As compliance with the Principles of Good Laboratory Practice (GLP) is required by law for non-clinical safety studies in many (OECD) countries, it is important that newly developed *in vitro* methods are suitable to be performed in a GLP environment, and so avoid lengthy adaptation where possible (Coecke et al., 2016[1]). Studies which support validations may or may not be subject to verification depending on compliance monitoring authorities' programmes[1].

As the ultimate goal is to develop an *in vitro* method which will be formally validated for its future use in a regulatory environment following a quality system (e.g., GLP), it is essential to have some knowledge of the regulatory requirements specifically relating to the storage and retention of data, records and materials as the *in vitro* method should be designed so as to be easily transferrable into a GLP facility. In the early stages of method development there are less formal requirements for storage and retention of records and materials than in the later stages and in general facilities will follow internal policies regarding storage and retention of data, records or materials. The development phase should be used to define the raw data, preferably described in the *in vitro* method itself, and any data (e.g., metadata), records or materials, to be retained when used in a regulatory environment.

Before beginning to collect raw data from *in vitro* test procedures, it is important to assess the format of collection, the complexity involved and requirements for traceability, storage, verification and transmission of data. Specific standards may apply for data from regulatory testing and manufacturing (Coecke et al., 2005[2]); (FDA, 2003[3]); (OECD, 1999[4]). Data from material provided by tissue donors may also be subject to the requirements of data management and control under local, regional, national or international rules and regulations such as the EU Directive on Data Protection[2] (national and regional rules should be consulted as these may vary). It should be ensured that data reported accurately reflects the results obtained during experimental work, by performing adequate quality control of the data.

GLP test facilities should comply with the GLP principles with regards to storage and retrieval of records and data. The use of computerised systems and the generation of electronic data are now common across all aspects of a GLP study, through planning, performing, monitoring, recording and finally archiving. GLP data integrity requirements apply equally to paper and electronic data, and staff should be trained in data handling and data integrity and specifically with regards to ensuring electronic data integrity (Section 10.1).

Data may be generated in many ways, by recording manual observation, by printouts of simple equipment (e.g., balance) or by data generated using complex computerised systems. The more complex and configurable the system, the higher the risks to data integrity, however systems with lower complexity should not be overlooked. For instance, it may be relatively trivial to perform repeat measurements until the "correct" result is obtained (e.g., pH measurements). It is also important that all data is retained and archived.

Many electronic records are important to retain in their dynamic (electronic) format, to enable interaction with the data. Data must be retained in a dynamic form where this is critical to its integrity or later verification. This should be justified based on risk.

Stored data should be secured by both physical and electronic means against loss, damage and/or alteration. Stored data should be verified for restorability, accessibility, readability and accuracy. Verification procedures of stored data should be risk-based. Access to stored data should be ensured throughout the retention period (OECD, 2016[5]).

10.1. Data integrity

Data integrity arrangements must be in place throughout the *in vitro* method lifecycle to ensure that the accuracy and completeness of the data. The lifecycle includes all phases in the life of the data, records and materials, from their initial creation or purchase through processing, use, retention, archival and retrieval, and eventual destruction (if applicable). It is vital that formal records used to confirm the results and how they were obtained are held in a stable/secure form, duplicated (i.e., backed-up) and location which is documented and traceable and for which there is a minimum storage period. Disposal after such storage periods should be recorded and a summary report of the destroyed data and the means of destruction should be prepared and held.

If data is translated between different recording methods, systems and/or databases and, in particular critical phases like manual or semi-automatic transfer (e.g., Excel™ files to database, combination of information obtained from two or three databases to one database), correct resolution of pre- and post-translation data should be reviewed and confirmed by a qualified person. For handwritten data translated into an Excel™ sheet, it is also advisable for the changes to be verified by the same person who has made the observations. These issues are of special concern where data are exchanged between countries. When data translation occurs between different software or database systems, their compatibility and inability to be altered in translation should be tested and will need to involve appropriate validation procedures.

The acronym ALCOA (Attributable, Legible, Contemporaneous, Original, Accurate) has been widely associated with data integrity (FDA, 2007[6]); (WHO, 2016[7]). The Good Automated Manufacturing Practice (GAMP) guide "A Risk-Based Approach to GxP Compliant Laboratory Computerized Systems" includes an appendix (Appendix 3) on data integrity, which used the term "ALCOA +" described as **A**ttributable, **L**egible, **C**ontemporaneous, **O**riginal, **A**ccurate, complete, consistent, enduring, and available (Table 10.1).

Table 10.1. Terms associated with ALCOA

	Criteria	Description / Explanation	Comments
A	Attributable	Who performed an action and when? If a record is changed, who did it and why? Link to the source data.	**Who did it? Source data**
L	Legible	Data must be recorded permanently in a durable medium and be readable.	**Can you read it? Permanently recorded**
C	Contemporaneous	The data should be recorded at the time the work is performed and date / time stamps should follow in order.	**Was it done in "real time"?**
O	Original	Is the information the original record or a certified true copy?	**Is it original or true copy?**
A	Accurate	No errors or editing performed without documented amendments.	**Is it accurate?**

Comparisons are often made between secure electronic data and data that are available in paper format. The comparison results in similar conclusions that electronic data are more secure, more difficult to manipulate or change, and any changes are easier to detect

(assuming that the software is technically compliant to 21 Code of Federal Regulations (CFR) Part 11 and technical controls are appropriately implemented). On the other hand, changes to paper data, such as a printed chromatogram, are simpler to make, but may be much harder to detect.

The same principles should be applied when using either paper-based and electronic systems, or a combination of both. It should be assured that the data is unchanged from the source, and has not been modified, altered or destroyed. To ensure data integrity for both systems, the following components of this process should be taken into consideration.

1. **Documentation and result reporting**

   - Records must be clear and accurate.
   - All activities should be recorded at the time they are performed.
   - Records should also be chronological, traceable, and readily retrievable.
   - Original documents must be clearly identifiable (e.g., time stamps, watermarks) and standardised, predefined; authorised forms and templates should be used wherever possible and applicable.
   - Records should be signed and dated allowing for clear identification. The use of pencil either for recording data or signing/dating records should not be allowed. Recording of original (raw) data on loose notes or scrap sheets of paper should not occur. For electronic data, an audit trail recording who does what and when should be implemented.
   - Any corrections written on documents should be signed, dated and justified (i.e., indicate the reason for change) by a trained staff member, and must not obscure the original data.
   - Transcriptions, if performed need to be attached to the original results (full traceability) and reviewed.
   - Chronology of recorded data must be ensured.

2. **Effective review and verification**

   - A clear definition and understanding of raw data should be ensured.
   - There needs to be traceability to the testing method used, source data and verification of raw data.
   - SOPs need to be in place for data handling, record retention and good documentation practices and deviation handling etc.

3. **Additional considerations for electronic data**

   - If a system is required to maintain electronic data, it should be managed by unique user identity and password combination. If the system does not permit this, a paper-based log must be in place to record who uses the generic user and password combination, or who uses the unprotected equipment.

- Paper records can be reviewed for any changes or crossings out/deletions plus the signature/date and the reason for doing so. This is to be replicated in an electronic system in the same way by use of an electronic log (audit trail).
- Electronic records must be traceable to the operator who produced the records. Where there are multiple users, each user should be provided with a unique username/password combination and shared logins should not be allowed.
- There must be a periodic user account review procedure.
- There should be procedures in place for assigning access rights to each user.
- The level of access should be in line with the tasks that have to be performed.

4. Data storage

- Data must be stored in a safe and secure place for paper-based systems and in protected folders for electronic systems.
- An approach must be in place to ensure that data are protected against loss, damage or overwriting.
- Access to stored paper or electronic records must be restricted and tightly controlled and documented, e.g., original electronic data files may be saved as read-only, so as to avoid manipulation or loss of these files.
- Electronic records must be held in a format that is not readily corruptible and protected from deliberate or accidental alteration (e.g., CFR 21 part 11, GLP: see OECD GLP Guidance Document 17).

10.2. Retention and archiving

In a regulatory GLP environment the archiving retention time is sometimes defined in national legislation. However, where there is no retention time specified, the OECD recommends that records and materials should be retained for as long as receiving authorities might request GLP audits of the respective studies and at least three inspection cycles so that inspectors can evaluate the GLP compliance of the test facility and the respective studies (OECD, 2007[8]).

Retention arrangements must be designed to protect data, records and materials from deliberate or accidental changes, manipulations or deletions thus ensuring integrity throughout the retention period. Archiving is defined as the long-term retention of completed data and relevant metadata, records or materials. Archived data, records or materials may need to be stored for many years and must be permanently locked so that no changes can be made without detection. In the case of paper records, archive design and conditions must protect contents from untimely deterioration. In addition to this, they should be easily retrieved for regulatory inspections.

The archives must be designed so as to allow for the archiving of documents and records and also for the archiving of study samples and materials (e.g., slides, specimens, test items and reference material) under suitable storage conditions (OECD, 2007[8]). The OECD Principles of GLP state that: "a sample for analytical purposes from each batch of test item should be retained for all studies except short-term studies". The same rules

apply to these archives as apply to the paper based archive, i.e., access restrictions, retrieval and removal of items, etc.

The storage conditions should be optimal for these samples and often these archives will require dedicated storage facilities, e.g., low temperature storage such as -20°C, liquid nitrogen storage or storage of items under inert conditions. Where special storage equipment is required, the rules governing the control and maintenance of this equipment must be applied. Where computerised systems are used, these systems must also follow the facility's policy regarding the use of computerised systems, including qualification and validation of such systems (OECD, 2016[5]).

Samples of test and reference items or specimens may however be discarded when the quality of the material no longer permits evaluation. Obviously, the storage conditions should be optimal for these samples. It is also good practice to refer to the storage devices' history to determine equipment failures, power outages, moves, that could possibly impact sample integrity. When samples of test and reference items or specimens are disposed of before the end of the required retention period, the reason for disposal should be justified and documented (e.g., the reason might be perishable specimens such as blood smears, freeze-dried preparations and wet tissues).

Data is generated during the experimental phase of studies and during this phase the integrity of the data must be ensured until final archiving of the study. This data will usually be required for further analysis and as such will not be formally archived until the completion of the study. It is important that access to this data, both electronic and hard copies, is controlled until the final archiving upon completion of the study. It is recommended, where possible or feasible, that the electronic data is set as read-only or that an audit trail is provided, detailing who did what and when.

The GLP Principles for archiving must be applied consistently to electronic and non-electronic data. It is therefore important that electronic data is stored with the same levels of access control, indexing and expedient "retrieval" as non-electronic data. Electronic archiving should be regarded as an independent procedure which should be validated appropriately. A risk assessment should be applied when designing and validating the archiving procedure. Relevant hosting systems and data formats should be evaluated regarding accessibility, readability and influences on data integrity during the archiving period.

When electronic archiving is performed, the archiving system, both hardware and software, must be designated as a computerised system and validated as such so as to ensure the integrity of data stored electronically over its life-time. If the data storage media, the data formats, the hardware or software of the archiving system changes during the archiving period, the system should be revalidated so as to ensure that there is no negative influence on the accessibility, readability and integrity of the archived data and that the ability to retrieve the data has not been compromised. Where problems with long-term access to data are envisaged or when computerised systems have to be retired, procedures for ensuring continued readability of the data should be established. This may, for example, include producing hard copy printouts or converting data to a different format or transferring data to another system. If migration of data including conversion to a different data format or printing is relevant, the requirements of this guidance for data migration should be met. Risk assessment, change control, configuration management and testing regime should be considered as relevant standard procedures when changes in the archiving system are required. As content and integrity of any electronic data should be preserved during the archiving period, the complete information package should be

identified and archived (e.g., raw data, meta-data necessary to understand correctly the meaning of a record or to reconstruct its source, electronic signatures, audit trails, etc.).

10.2.1. Retrieval

Each facility should have in place procedures concerning the retrieval of archived records and materials. The procedures should detail who may retrieve records and materials, for how long and the return of records and materials to the archive. All steps mentioned above need to be documented and traceable.

In the case of electronic records, viewing the records without the possibility of alteration or deletion of the archived version does not constitute "retrieval" of a record. Most systems available nowadays support read-only access, without the possibility to change or delete the archived record.

10.3. Backup and restore

When storing electronic documents, including electronic archives, periodic backups should be performed. These backups do not constitute archived records, however as they may be required to be restored in the case a system failure, the same rules regarding access to the archived electronic records should be applied to access to the backup(s). In general backups are foreseen for short term storage and not long term storage or archiving and therefore the long-term readability of these archives is usually not an issue; however the restoration of the backups should also be checked on a regular basis.

Data generated during the experimental phase of the study should also be covered by the backup and restore policy of the facility.

Notes

1. See: http://www.oecd.org/env/ehs/testing/glp-frequently-asked-questions.htm
2. See: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046

References

Coecke, S. et al. (2005), "Guidance on good cell culture practice: A Report of the Second ECVAM Task Force on good cell culture practice", *ATLA Alternatives to Laboratory Animals*, Vol. 33/3, pp. 261-287. [2]

Coecke, S. et al. (2016), "Practical Aspects of Designing and Conducting Validation Studies Involving Multi-study Trials", in *Advances in Experimental Medicine and Biology, Validation of Alternative Methods for Toxicity Testing*, Springer International Publishing, Cham, http://dx.doi.org/10.1007/978-3-319-33826-2_5. [1]

FDA (2007), *Computerized Systems Used in Clinical Investigations*, Food and Drug Administration, United States. [6]

FDA (2003), *Part 11: Electronic Records; Electronic Signatures – Scope and Application*, Food and Drug Administration, United States. [3]

OECD (2016), *Application of Good Laboratory Practice Principles to Computerised Systems*, OECD Series on Principles on Good Laboratory Practice and Compliance Monitoring, No. 17, OECD Publishing Paris. [5]

OECD (2007), *Establishment and Control of Archives that Operate in Compliance with the Principles of GLP*, OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 15, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264084995-en. [8]

OECD (1999), *Quality Assurance and GLP*, OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring, No. 4, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264078598-en. [4]

WHO (2016), *Guidance on good data and record management practices*, WHO Technical Report Series, No. 996. [7]