Labfolder GmbH
Elsenstraße. 106, 12435 Berlin, Germany
www.labfolder.com

Contact| Labfolder Team
contact@labfolder.com
+49 (0) 30 91572642

Whitepaper:

Labfolder GLP Compliance

TABLE OF CONTENTS:

Background and Introduction

This White Paper summarizes how the Labfolder platform enables compliance with the requirements of the OECD Series on Principles of Good Laboratory Practice (GLP) and Compliance Monitoring.

As a quality assurance system, the GLP Principles have been introduced by the Organisation for Economic Co-operation and Development (OECD) with the intention to promote data quality and guarantee data integrity. Apart from other guidelines regarding quality research, the GLP Principles can be found in the member countries of the OECD (except the USA and Japan) for non-clinical, chemical and agrochemical research testing studies.

In particular, the GLP principles intend to provide a secure research environment that protects raw data from manipulation during and after testing procedures and incorporates all organizational structures of research procedures. Therefore GLP not only regulates the personnel working in a laboratory or other research facility, but also applies to computerized systems and their device-specific requirements used for research purposes.

As a result, computerized systems like Labfolder have to provide validated services to ensure accuracy, reliability and consistent intended performance, including the ability to ensure data quality and integrity, protecting stored records against manipulation or loss.

Overview of Labfolder's compliance with the GLP Principles

Labfolder is a management software, used for the electronic analysis and management of research data across scientific disciplines. For a computerized system with integrated archive facilities like Labfolder, the provision of services that are compliant with the GLP Principles is of utmost importance.

The Labfolder system has considered the GLP Principles during its development phase and continues to incorporate the regulations within its system life cycle to ensure continuous quality, integrity and security of research data stored in the electronic archive facilities..

Since the compliant adherence to GLP is not reclusively based on the software system itself but also depends on procedural controls (such as SOPs, well trained personnel, physical conditions of research facilities) within a laboratory or other research organizations using electronic management systems for research purposes, a software system cannot be certified to be compliant (and any software vendor claiming GLP-compliance is incorrect!). However, software

vendors can offer a system which meets the technical requirements for computerized systems and the management of electronic records set by the OECD in a compliant set-up.

The following section below gives a brief summary on how the Labfolder system complies with selected GLP Principles that are relevant for software systems used in laboratories or other research institutions. The Labfolder system provides a secure, GLP-compliant environment for research data by employing the following features:

Security

Labfolder incorporates state of the art enterprise security - both logical and physical - to protect research data, including:

- Access control: Password complexity requirements
- Back-up power: Daily back-ups of records
- High-security data center: Offsite back-ups on redundant servers with TÜV approved data security and ISO 27001 certificate for excellent data security
- Strict network firewalls: System access only allowed for verified IP addresses
- Multiple encryption: Storage encryption, encrypted communication and encryption during uploads and downloads
- System check-ups: System scanning and monitoring routines
- IT updates: Regular security and functionality updates
- Business infrastructure: Validation plan and continuity and disaster recovery procedures
- Physical protection programme: Secure data centre with regular stress testing of the infrastructure, climate protection procedures (e.g fire. water or other natural disasters), the provision of redundancies and emergency management

Confidentiality

The Labfolder system employs procedures that keep all stored records protected from disclosure to unauthorized parties, including:

- Admission control: Limited access to data only for account owner and authorised persons
- Data encryption: Encryption for identifiable data during uploads/downloads, transfer and storage
- Secure storage: Separate security locations on redundant servers with various security procedures in place (both physical and logical)
- Safe disposal: of data and media

- Confidentiality agreement: Records Management Section for staff working with sensitive research data, well trained personnel and internal security training

Authenticity

Labfolder guarantees the reliability of data transfers and the information exchange within research networks through:

- Multi-level authentication processes: Login/password combination and access rights management
- Secure user identification: Identification needed to access and to manage data
- Electronic signatures: Sign and witness functions for digital data
- Migration plan: Secure data transfer with encrypted coding

Integrity

Labfolder provides comprehensive protection of research data from unauthorised access and changes through:

- Access control: Restricted management rights to ensure data quality in a regulated environment
- Authority checks: Limited access to authorized individuals only
- Full audit trail: All activities within the system will be recorded
- Version control. Recording and monitoring of all activities, including IT related processes
- Logged data: Uploads and downloads are logged and “hashed” to verify data integrity
- Timestamps: Records and changes are provided with a system-created timestamp, recording person, date and time
- Electronic signatures: Option to sign and witness electronic documents
- Secure data transfer: Migration plan with encrypted coding
- Data retention: Long term retention of electronic records for at least 3 years until deleted by account owner
- Data availability: Stored records are available for collection, inspection and review by the agency/reviewing body
- Data deletion: Deletion of records can be controlled and prohibited by organizational policy
- Standard Operating Procedures: SOPs to ensure optimal system performance and uninterrupted services, including validation, operation and maintenance

This white paper at hand summarizes the sections of the OECD Series on Principles of Good Laboratory Practice (GLP) and Compliance Monitoring regulations which are relevant to electronic systems like Labfolder, also pointing out the Labfolder implementation to meet these technical requirements.

In addition to the selected GLP Principles (No 1, 10 and 15), there are several sections of the GLP regulations that do not apply (test sites and physical archives only) to the system and services provided by Labfolder..

However, this document does not give detailed information on GLP, nor does it provide legal advice for full compliance. The full text of GLP can be found on the OECD website at: http://www.oecd.org/env/ehs/testing/oecdseriesonprinciplesofgoodlaboratorypracticeglpandcompliancemonitoring.htm

NUMBER 1- OECD Principles of Good Laboratory Practice

SECTION II GOOD LABORATORY PRACTICE PRINCIPLES

3. FACILITIES

3.4 Archive Facilities

Labfolder implementation: As an archive facility Labfolder aims to support the promotion of quality test data, providing a powerful research tool that ensures a sound and reliable approach to the management of research studies.

In terms of data security, the Labfolder infrastructure employs redundant servers, daily back-ups and encrypted communication between any device in use and the Labfolder cloud, providing bank level security for all records. Strict access control with a login/password combination and an automated audit trail with system-created timestamps further protects all stored content.

In case of closure, the system also provides a business continuity and disaster recovery plan, including the safe transfer or record to a new archive facility. Labfolder offers a long term retention of electronic records with the secure storage of records for three years beyond the subscription period unless explicitly being deleted by the account owner. Deletion of records can be controlled by management rights control and prohibited by organizational policy.

4. APPARATUS, MATERIAL AND REAGENTS

1. Apparatus, including validated computerised systems, used for the generation, storage and retrieval of data, and for controlling environmental factors relevant to the study should be suitably located and of appropriate design and adequate capacity.
2. Apparatus used in a study should be periodically inspected, cleaned, maintained, and calibrated according to Standard Operating Procedures. Records of these activities should be maintained. Calibration should, where appropriate, be traceable to national or international standards of measurement.
3. Apparatus and materials used in a study should not interfere adversely with the test systems.

Labfolder implementation:
(1): As a validated computerised system, Labfolder uses redundant servers that are located in Germany. These servers operate under the strictest international data protection laws.
(2): As part of the Labfolder IT development cycle, the Labfolder system undergoes regular system scanning and monitoring, according to national and international standards. These scheduled unit and integration tests also include all newly integrated features with the continuous integration system running whole test suite on any code change. The dedicated test system is the exact copy of the original production system. Records of these test inspections are kept for further review.
to (3): Labfolder does not interfere adversely with the test system. The Labfolder system is designed to support research projects.

7. STANDARD OPERATION PROCEDURES

7.4. Standard Operating Procedures should be available for, but not be limited to, the following categories of test facility activities. The details given under each heading are to be considered as illustrative examples.

2. Apparatus, Materials and Reagents
b) Computerised Systems
Validation, operation, maintenance, security, change control and back-up.
3. Record Keeping, Reporting, Storage, and Retrieval
Coding of studies, data collection, preparation of reports, indexing systems, handling of data, including the use of computerised systems.

Labfolder implementation:

(7.4.2b): As a computerised system, Labfolder employs Standard Operation Procedures (SOPs) that are compliant with the Principles of GLP. Procedures of validation, operation and maintenance are in place to guarantee optimal system operation and data integrity

In terms of system validation, Labfolder accounts for a closed, validated system as stated in Subpart B – Electronic Records, Section 11.10 Controls for closed systems of CFR Part 11 and Annex 11. The Labfolder system meets all set classifications by the FDA, requiring a login and password to use the electronic lab notebook. No matter from which device a user wants to access Labfolder, a login is required each time. In addition, the IP addresses of the devices in use are stored for every session. With all these security measures in place, the Labfolder-system guarantees authenticity, integrity and confidentiality of electronic records managed by the Labfolder software.

Regular maintenance procedures - including software tests, system scanning and monitoring with message alerts - and Disaster Recovery Plans arrange for a smooth system operation. Labfolder employs various state of the art enterprise security features, a compilation that provides maximum data security for all Labfolder accounts. Within the archive facilities, Labfolder uses storage encryption as well as encryption during upload and download of data. Redundant servers, daily automated back-ups and strict network firewalls keep all records safe and provide maximum data protection against unauthorized access. An integrated Source Code Management System generates a full audit trail with detailed index of all actions performed.

(7.4.3): As part of SOPs, Labfolder employs strict access controls for accessing, sharing and changing records with all activities requiring a specific login/password authentication. In addition, the Labfolder system annotates all records - including new records as well as changes to existing records - with a unique time-stamp which cannot be manipulated by any user. A system-created audit trail generates a detailed report, providing documentary evidence of the operation, procedure and persons managing stored records.

8. PERFORMANCE OF THE STUDY

8.3 Conduct of the Study

3. All data generated during the conduct of the study should be recorded directly, promptly, accurately, and legibly by the individual entering the data. These entries should be signed or initialled and dated.
4. Any change in the raw data should be made so as not to obscure the previous entry, should indicate the reason for change and should be dated and signed or initialled by the individual making the change.

5. Data generated as a direct computer input should be identified at the time of data input by the individual(s) responsible for direct data entries. Computerised 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 having made those changes, for example, by the use of timed and dated (electronic) signatures. Reason for changes should be given.

Labfolder implementation:
(8.3.3): Labfolder allows for the accurate recording of research data in compliance with set research regulations. Before entering data into the electronic lab notebook, each Labfolder user has to verify his/her identity, using registered login details. The Labfolder system also annotates each entry with a unique timestamp. In addition, digital signatures can be added to each entry.

(8.3.4): The Labfolder system allows for changes to raw data, always retaining a copy of the original entry. Thus record changes do not obscure previously recorded information. A system-created timestamp records all activities, including details on date and time. Any changes made to an existing entry are saved and marked with an additional timestamp and optional signature.

(8.3.5): All data entered or generated within Labfolder is provided with a timestamp, identifying the user/author, time of data entry or alteration to existing entries. Additionally, an automated audit trail records all data-related activities. In case of altering entries, an original copy of the record is kept without obscuring the original data. All changes are saved in the generated audit trail, also allowing for digital signatures to identify the person making these changes. In addition, reasons for change can be given,

10. STORAGE AND RETENTION OF RECORDS AND MATERIALS

10.1 The following should be retained in the archives for the period specified by the appropriate authorities:

a) The study plan, raw data, samples of test and reference items, specimens, and the final report of each study;
b) Records of all inspections performed by the Quality Assurance Programme, as well as master schedules;
e) Validation documentation for computerised systems;

Labfolder implementation:
(10.1 a & b): In the cloud version of Labfolder, all records - including study plans, raw data, reports among others - are stored for three years beyond the subscription period unless

explicitly being deleted by the user. On local server installations, retrieval throughout the records retention period is within the responsibility of the hosting organization.

(10.1e): Validation documentation for Labfolder are retained in our archive for an unlimited period of time.

NUMBER 10 - GLP Consensus Document The Application Of The Principles Of GLP To Computerised Systems Environment Monograph No 116.

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.

Labfolder implementation: This principle lies beyond the scope of Labfolder and reaches out to the sole responsibilities of the respective management unit of a test facility. However, as an archive facility and powerful research tool the Labfolder system supports the promotion of quality test data and offering a reliable management facility of research studies.

Overall, the Labfolder system is developed, validated, operated and maintained in accordance with the GLP Principles. Amongst other principles our management ensures that all Labfolder personnel is qualified and experienced in regards to software development and laboratory research. Our Labfolder IT personnel are well trained in the fields of software design, implementation of cryptographic methods and regulations. Labfolder personnel who are not familiar with the system and the requirements are being provided with manuals and training. Due to regular check-ups and maintenance work the Labfolder system is kept in adequate condition.

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.

Labfolder implementation: All Labfolder personnel are qualified and experienced in regards to software development and laboratory research. The Labfolder IT personnel are well trained in the fields of software design, implementation of cryptographic methods and regulations, including GLP compliance. For all personnel using the Labfolder system, Labfolder provides guidelines and training to ensure compliance with the GLP Principles.

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.

Labfolder implementation: However, Labfolder incorporates a Quality Assurance (QA) Programme, assuring that established policies and procedures are maintained at all stages of system operation. In order to guarantee GLP- compliance, designated QA personnel monitor the Labfolder system on a regular basis. Labfolder also provides training and manuals to all personnel not familiar with the GLP Principles

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.

Labfolder implementation: This principle is partly beyond the scope of Labfolder, being part of the responsibilities by the Quality Assurance Unit provided by the institution using the Labfolder system for research purposes.

However, all Labfolder personnel are qualified to perform assigned task in alliance with the GLP Principles. The Labfolder management as well as the IT personnel are both well trained in reference to set regulations. Team members who are not familiar with the system and the requirements are being provided with manuals and specific training courses by Labfolder.

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.

Labfolder implementation: All redundant Labfolder servers are exclusively located in Germany and operate under regulated EU and German data security and privacy laws. The data centre employs a specific climate management plan with an optimal cooling system, power supply with dual protection and emergency generators, and a planned network infrastructure to handle high volume of traffic.

With regular maintenance procedures scheduled, including system scanning and monitoring, Labfolder ensures optimal system operation and performance under any conditions and circumstances, reducing the likelihood of an unexpected breakdown and, as a consequence, loss of data. In addition, daily back-ups guarantee maximum data safety and secure storage facilities. Even in the case of a possible device failure or other incidents, the abfolder system provides for the secure retention of all stored data.

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.

Labfolder implementation: Labfolder is a software that allows its clients to archive, manage and share research data. The Labfolder system offers web applications for all major browsers and operating systems via selected networks. In reference to peripheral components, Labfolder employs a high-tech data centre for back-up and redundant storage, providing the following services for the secure retention of electronic storage media:

- Connection to multi-redundant, carrier-neutral 75 Gbit/s internet backbone
- Uninterruptible Power Supply (n+1 UPS) and redundant power supply
- Climate management and air conditioning (n+2)
- Argon fire extinguishing facility with early warning system
- Fire/alarm control panel

For all hardware devices used to run the Labfolder software the sole responsibility lies with the owner/operator/user.

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.

Labfolder implementation: Labfolder applies encrypted communication between any device in use and the Labfolder cloud. The encryption via SSL (256-bit) ensures maximum data security, anytime and anywhere. Automated system scans and monitoring procedures during the system life-cycle are in place to prevent interruptions and failure of service, simultaneously guaranteeing a reliable and secure business continuity of Labfolder.

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.

Labfolder implementation: As part of the Labfolder Standard Operation Procedures (SOPs), Labfolder adopts a set of standard maintenance policies. For prevention, Labfolder employs regular system monitoring with direct message alerts to inform Labfolder IT personnel in charge about any incident corrupting the system. Additionally, automated software tests are scheduled and performed on a regular basis to ensure a smooth operation of all software components involved in the Labfolder system. Precautionary measures also include scheduled maintenance activities to software parts that do not possess suitable backups or alternatives, reducing the risk of breakdown or system-failure.

In reference to curative procedures, Labfolder adopts assigned contingency plans for any fault being detected within the system. In case of an incident/bug detection, Labfolder IT personnel takes immediate action and programs a new software test to target the reported bug/incident. The new test is then implemented into the regular testing system as an additional part of the regular software scan cycle. Immediate access to Labfolder IT personnel allows for a quick fix of the reported incident, being classified as a high priority task to re-establish full services and system operation.

Both programmes - preventative and curative - guarantee permanent system-performance with the intention to protect all data stored in the electronic lab notebook against manipulation and/or loss. All preventative procedures are being recorded, including all Labfolder IT personnel involved. In terms of documentation, an automatically generated audit trail records the overall software performance alongside possible incidents and inconsistencies that may occur during system operation.

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.

Labfolder implementation: The Standard Operation Procedures (SOPs) of Labfolder also include procedures that apply in case of disaster recovery. In case of recovery mode, Labfolder maintains back-up copies and - if necessary - performs a validation of the system.
Daily backups and redundant servers allow for the quick retrieval of all original records stored in the Labfolder system. Clients also have the option to download all documents to PDF for paper based back-up (or printing). Labfolder's Disaster Recovery Programme is well documented and ensures continued data integrity and full recovery of stored records. All Labfolder personnel involved are familiar with the Contingency Plan.

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 the 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

Labfolder implementation: Labfolder's definition of raw data relates to all original laboratory records and documentation collected as part of a particular study, including gathered research data directly entered into a computer or imported via a mobile device (e.g. image). For example, various (digital) text and table formats, photographs, dictated observations, recorded data imported from mobile devices, or any other data storage medium. In addition, raw data also incorporates the documentation of the procedures and circumstances under which the study was conducted.

In reference to data retention, Labfolder allows for continued access to and retention of raw data for a period of three years beyond the subscription period unless explicitly being deleted by the user without integrity risks. The system also provides all records - including changes to existing entries - with a system - created timestamp. The subsequently generated audit trail can not be manipulated and contains valuable information such as date and time of data submission or entry alteration. Besides, digital signatures indicate the person submitting or

changing an entry. All in all Labfolder supplies well documented processes that ensure data integrity and prevent manipulation or loss of research data.

In terms of transfer, Labfolder offers a migration plan and guidance in support of safe and secure data transfer to new storage facility. For full details, view GLP 15, Section 7.5.

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.

Labfolder implementation: The principle concerning physical security is beyond the scope of Labfolder. As a validated software system Labfolder provides digital (logical) data security. In terms of physical security, the regulations of the respective institute/organization using Labfolder for research purposes apply.

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.

Labfolder implementation: In order to provide maximum data security, Labfolder incorporates state of the art enterprise security features that prevent unauthorised access to clients' accounts, including the following:

- Access control with login/password combination for authentication
- Strict controls for data access, data sharing and data management
- Access management and restrictions according to assigned roles
- Change control & management permissions
- Regular system scanning and monitoring
- Strict network firewalls
- Storage encryption
- Encryption during uploads and downloads
- Session timeout

As part of the Labfolder software development lifecycle, Labfolder ensures software quality control, only using approved versions and validated software. Labfolder has implemented further security control features in order to check external sources and detect suspicious behaviour. For example, multiple logins, subsequent logins from alternating locations amongst others. Unauthorized use can further be detected and prevented by monitoring and restricting IP addresses for system access.

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.

Labfolder implementation: Labfolder ensures that persons who develop, maintain, or use the electronic lab notebook are aware of and respect all GLP Principles, including data integrity, authenticity and confidentiality. All Labfolder personnel have the education, training, and experience to perform their assigned tasks according to security regulations that may apply. For new team members who are not familiar with the Labfolder system, the requirements and the applied security regulations, Labfolder offers manuals and on-the-job training to ensure GLP-compliance. Labfolder provides information for clients on GLP-compliance. However, the respective management or individual is responsible for following these regulations

To further ensure data integrity, all records are stored and processed at high-security redundant servers located in Germany with back-up power and strict access control. In addition, Labfolder employs the following features:

- Version control for all entries.
- All activities, including data access, management and changes are time- and date-stamped and logged to a dedicated server.
- All uploaded records are logged and "hashed" to verify integrity.
- Full storage encryption and encryption during data uploads and downloads
- All records are maintained for at least three years beyond the subscription period unless explicitly being deleted by the user.
- System scanning and monitoring to prevent system failure and compromising of data.
- Rights management and restricted permissions according to role

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.

Labfolder implementation: As part of the Labfolder Recovery Plan, all data is automatically backed-up daily to multiple remote servers, ensuring maximum data safety and integrity of all records. In case of an incident, such as PC crash, device failure or disk corruption, Labfolder allows for the full recovery of all data concerned. All back-up copies are treated with care and the standard safety guidelines apply, ensuring that studies implementing Labfolder for research purposes are not irretrievably affected.

7. VALIDATION OF COMPUTERIZED 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 preplanned 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.

Labfolder implementation:
Labfolder is an electronic lab notebook, used as a viable research tool for data management and as a collaboration platform for laboratory research. As a validated computerized system, Labfolder can provide objective evidence that all related software specifications conform to user needs and purposes. The Labfolder system is compliant to the GLP Principles and ensures that particular requirements implemented through software can be consistently fulfilled. In alliance with recognized quality and technical standards, the Labfolder software has been intensively tested and approved before being released to customers. All testing procedures have been well planned and documented, including test set-ups and outcomes. The Source Code Management System in place generates a detailed index of all actions performed.

Furthermore our data center has been awarded the following certificates for approved security provision from recognised quality and technical standards:

- TÜV approved secure information management system
- ISO 27001 for excellent data security
- Trusted Cloud for maximum availability, confidentiality and integrity
- 5 stars in the eco Datacenter Star Audit, the security and quality certificate for internet data centres.

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.

Labfolder implementation: These principles do not apply to the Labfolder system as the software has been designed in alliance with the GLP Principles. As far as the implementation of

new features to the Labfolder system are concerned, all new components also provide GLP-compliance.

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.

Labfolder implementation: Labfolder employs change control to ensure that data modification is well documented. Audit trails are in place to identify the person submitting and changing an entry. System-generated timestamps record date and time of all activities necessary to submit, change or delete electronic records. The generated audit trails are retained for at least xx years and are available for agency review.

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.

Labfolder implementation: Embedded support mechanisms, such as regular maintenance, software tests and overall performance assessment monitor the operation of the Labfolder system. The procedures in place to verify that Labfolder is fully functioning and providing reliable and responsive services to clients. Additionally, Labfolder offers continuous customer support to ensure that clients needs are met, incidents or interruptions are immediately eliminated and full services are provided 24/7.

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.

Labfolder implementation: All Labfolder policies are described in Standard Operating Procedures (SOPs) which are part of Labfolder's documentation system, including mandatory principles that apply to all activities related to the Labfolder system in use. These policies comprise liability, user responsibility, maintenance and staff performance and responsibilities. All development, validation, operation and maintenance procedures are well documented, assuring users that the Labfolder system is reliable and not outside its service interval. Labfolder also provides records of system calibration, demonstrating that the respective SOPs have been followed and that system performance was adequate within its specifications.

b) Application Description

For each application there should be documentation fully describing:

Labfolder implementation:

- The name of the application software or identification code and a detailed and clear description of the purpose of the application.
    - Labfolder is a digital lab notebook and collaboration platform for laboratory research. The Labfolder software presents a powerful research tool that allows scientists to archive, manage and share their research data with others.

- The hardware (with model numbers) on which the application software operates.
    - The Labfolder software operates on PCs, Macbooks, tablets and other hardware, including mobile devices (iOS and Android)

- The operating system and other system software (e.g., tools) used in conjunction with the application.
    - The Labfolder webapp is accessible for all the major browsers and operating systems, Older versions may not have all the features available, lacking the required capabilities.

The full list of browser support is available at https://www.labfolder.com/browser-support
    - Integrated software tools, such as Dropbox, Mendeley and Figshare can be used in conjunction with the Labfolder system.

- The application programming language(s) and/or database tools used.
    - Information on this matter is only available upon request, being subject to corporate privacy.

- The major functions performed by the application
    - Labfolder is a digital lab notebook and collaboration platform for laboratory research. The Labfolder software presents a powerful research tool that allows scientists to archive, manage and share their research data with others.

- An overview of the type and flow of data/database design associated with the application.
    - Labfolder allows for the import/export of various text and table formats, media and other files.

- File structures, error and alarm messages, and algorithms associated with the application.
    - In case of system interruption or failure, the Labfolder system generates error and alarm messages for clients.

- The application software components with version numbers.
    - Information on this matter is only available upon request, being subject to corporate privacy.
- Configuration and communication links among application modules and to equipment and other systems.
    - Configuration and communications between Labfolder and other devices is securely encrypted via SSL (256-bit).

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.

Labfolder implementation: Information on this matter is only available upon request, being subject to corporate privacy.

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 archiving and retrieval of all documents, software and computer data.
- Procedures for the monitoring and auditing of computerised systems.

Labfolder implementation: Labfolder's Standard Operating Procedures (SOPs) include all procedures concerning the operation,and performance of the Labfolder system with the aim to guarantee data integrity, to ensure data safety and to minimize the risk of systematic error. The Sops include the following procedures:

- Operational procedures concerning the Labfolder systems, including training and responsibilities of assigned Labfolder IT personnel.
- Safety and security procedures to guarantee maximum data integrity and to prevent unauthorised access to accounts.
- Procedures and authorisation for programme changes and the recording of changes.
- Development and testing procedures for software updates and the implementation of new features, including the documentation.
- Monitoring and scanning procedures for the surveillance of the Labfolder system, testing its performance and correct functioning.
- Maintenance procedures for the Labfolder systems and any associated equipment.
- Back-up procedures for all stored data and contingency plans in the event of a breakdown.
- Data management procedures, also including archive processes and retrieval of all research data.
- Procedures for the monitoring and auditing of computerised systems.

Upon performance, all Labfolder SOPs are well documented and retained for further review.

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.

Labfolder implementation: The GLP Principles are applied to all data stored in the Labfolder archive. Labfolder uses the same level of access control and care for all data types, requiring a login/password combination.for user authentication. If needed, the Labfolder system also provides an index for electronic data obtained from more than one study.

Labfolder allows for long-term access to data, providing storage even for records that must be retained for longer periods of time.The Labfolder servers ensure the long-term integrity of data without loss or deterioration of stored records. In addition, the Labfolder system also allows for a quick retrieval of archived data.

Labfolder promotes safe storage of research data, restricting access to archive facilities with implemented procedures such as access control, full audit trail and restricted management rights. In case of system retirement, Labfolder has specific transfer procedures in place, ensuring the continued readability and use of data

In terms of permanent data deletion, the deletion of research data is possible after authorization and can be further controlled by organizational policy. By default, all data is only available to the authors or the respective project owner with the possibility to grant access to other users/fellow

researchers. Therefore records stored in the electronic lab notebook cannot be deleted without management authorization and/or permission.

Supporting data of the Labfolder system concerning development, validation, operation, maintenance and monitoring records will be kept for (enter period of time).

NUMBER 15 - Establishment and Control of Archives that Operate in Compliance with the Principles of GLP

4. ROLES & RESPONSIBILITIES

4.3 Archive Contracting Facility

If a sponsor or test facility management uses a contract archive for the storage of records and/or materials for a GLP study, the contracting parties should ensure compliance with the relevant sections of the Principles of GLP.

Labfolder implementation: The Labfolder system presents an archive contracting facility, supporting documentation, archiving processes and management of quality test data. Labfolder operates in compliance with GLP Principles and provides a reliable research tool for the management of sensitive research data. Amongst other procedures, the Labfolder system generates a full audit trail and records all activities related to stored entries, including up- and downloads of data as well as changes to existing records. In terms of data security and integrity, Labfolder relies on encrypted communication, redundant servers and daily back-ups, all procedures that ensure maximum data safety and integrity. Additionally, access control with a login/password combination and restricted management rights further ensure GLP-compliance.

4.8 Information Technology (IT) Personnel

IT personnel involved in archiving operations (such as ensuring the integrity of electronic records) should be adequately trained and their activities should conform to GLP requirements. Since activities pertaining to archiving are the primary responsibility of the archivist, these IT personnel ideally should work under the direction and supervision of the archivist. Because it is recognised that such organisational structures are not feasible in modern companies, the co-operation between the archivist and IT personnel should be ensured in other ways, for instance in SOPs or written service level agreements.

Labfolder implementation: Labfolder employs IT personnel for all archiving operations and software development procedures. All IT personnel is well trained and experienced in the fields of software design, implementation of cryptographic methods with all actions being compliant to GLP. New team members obtain hands on training-sessions and training manuals, including an introduction to the GLP Principles (as pointed out in GLP No. 10, 1 a&d).

5. ARCHIVE FACILITIES

The archive facility should be suitably designed and constructed to accommodate the archived records and materials. This may be one or more buildings, rooms, safes or lockable cabinets or other locations that provide suitable security. The archive facility should be physically secure to prevent unauthorised access to the retained records and materials. The use of locks or electronic entry systems is required. The components that provide storage of unique electronic records should also be physically secure. The computerised archive facility should have processes to prevent unauthorised access and virus protection.

The building(s) or room(s) that house the archive should be constructed to withstand the elements of local weather, etc. Consideration may need to be given to specific local conditions such as a risk of flooding. The archive design should protect the contents from untimely deterioration for example by leakage of running water pipes in the archive areas. The risk of fire and explosion should be minimised. In most circumstances it will be necessary that an automated fire and/or smoke detection system be installed. Management may also consider an automated fire suppression system that minimises the risk of damage. If there is a risk of flooding, a water detector and/or water drain should be considered.

The archive facility should be designed to prevent the entry of rodent and insect pests. Where appropriate, pest control procedures should be in place.

Where necessary, back-up electrical power should be provided for all temperature-critical equipment (e.g., refrigerators and freezers).

Labfolder implementation: This principle is beyond the scope of the electronic software system provided by Labfolder and does only apply to physical archives. However, Labfolder can provide guidelines and training for clients to ensure compliance.

As a provider of computerised archive facilities for research data, Labfolder ensures that all entered data is kept safe and secure - without loss or deterioration. The Labfolder system presents a centralised, secure repository for the storage and retrieval of scientific data and employs several safety procedures and processes to prevent unauthorised access and virus protection. In compliance with GLP Principles, Labfolder controls data management and

modifications, recording all logins and logouts in an audit trail. In case of system-failure, Labfolder

5.1 Archive Conditions

Storage conditions should be designed to preserve and not adversely affect the quality and integrity of retained records and materials. Special storage conditions may be required to maintain the integrity of some retained record(s) and material(s) for the specified retention period(s). For example, it might be appropriate to store wet tissues, blocks and reserve samples of test items separate from paper and histology slides.

Special storage conditions may be required for particular materials. Examples are materials required to be stored frozen, refrigerated, desiccated, etc., or free from dust or magnetic interference in the case of electronic media. The need for special storage conditions should be defined in relevant test facility Standard Operating Procedures.

If special storage conditions have been defined, environmental monitoring procedures should be implemented within archive storage areas to confirm that specified conditions of storage are being achieved. Where continuous (automated) monitoring systems are used (which may also act as alarms that are activated in the event that defined conditions are outside specified limits), these systems should be regularly maintained, tested, and verified, and records thereof retained, as required by the Principles of GLP.

Labfolder implementation: This principle is beyond the scope of the electronic software system provided by Labfolder and does only apply to physical archives. However, Labfolder can provide guidelines and training for clients to ensure compliance.

As an electronic repository for research data, Labfolder stores all entered records on a secure cloud and redundant servers. Strict security measures ensure maximum data protection and integrity. With monitoring procedures scheduled on a regular basis, the Labfolder system guarantees excellent storage conditions as previously pointed out in GLP No 1, 6c, 3.4, 7, 10 and No 10, 3a, 4 and 6.

5.2 Disaster Recovery

Test facilities and contract archives should have procedures in place to minimise damage to archived records and materials caused by adverse events. Some of the more common adverse events to be considered include fire, electrical failure, extreme weather-related damage, flooding, theft, and sabotage.

The procedures may cover protective measures that may be implemented, as well as the recovery and/or restoration of lost or damaged records and materials and re-establishment of security. The plan should include useful and emergency contacts, the location of necessary equipment, and the records that should be made (e.g., documentation of the event and the steps taken to resolve and/or restore).

Labfolder implementation: Labfolder employs a specific Disaster Recovery Program with measures to be taken in the event of partial or total failure of the Labfolder system. The Labfolder Contingency Plan is well documented, validated and ensures continued data integrity that will not compromise the research project. The allocated procedures for the recovery depend on the criticality of the system, but it is essential that back-up copies of all software are maintained. Labfolder informas all clients about the Disaster Recovery Program before the initial sign-up to the electronic lab notebook. Disaster recovery is also pointed out in detail in GLP No 1,7 and No 10, 4.

6. SECURITY

6.1 Physical and Operational Security

The archive facility should be both physically and operationally secure to prevent unauthorised access and changes to or loss of retained records and materials. Test facility management should ensure security by implementing appropriate measures that should be described in the test facility's SOPs.

The security controls necessary to restrict access to electronic records will usually be different from those applied to other record types. Since many electronic storage media can be reused (e.g. overwritten), measures should be implemented to ensure that records cannot be altered or deleted.

Labfolder implementation: A wide array of security procedures are used to protect all research data stored in Labfolder's archive facilities from corruption or unauthorised access, modification or loss. Corruption of hardware and software by viruses or other maleficent agents are also covered by the operational security procedures employed by Labfolder. All security measures are described in the SOPs as pointed out under GLP No 1,7 and No 10, 6.

As an electronic repository for digital data, Labfolder implements specific security measures to prevent unauthorized manipulation of records. In order to maintain data integrity and provide maximum data protection, access to Labfolder requires authentication via a unique login/password combination. Access to records - including alteration and deletion - can be

controlled, granted and revoked anytime by the author or organization which controls and owns these records.

For all physical security aspects of the test facility, the respective Test Facility Management is responsible to ensure GLP compliance.

6.2 Access to the Archive

With normal archive operations, access to the archive should be controlled and restricted to the archivist and archive staff. For emergency access (especially during off-hours or for safety reasons), emergency personnel may enter and/or operate the archive unaccompanied. Otherwise visitors should be accompanied by the archivist or a member of the archive staff. The procedures for access to archive storage areas should be documented. The record of such visits should be retained. For electronic archives the above mentioned restrictions might not be applicable, but as a minimum deletion or alteration of electronic records in electronic archives should be avoided. Management might authorise read-only access on electronic records to a broader community.

Labfolder implementation: As an electronic archive Labfolder provides centralised, secure repository for the storage and retrieval of scientific data. All entries as well as changes to existing records are tracked in a full audit trail and obtain a timestamp provided by the server-system which cannot be manipulated by others. The deletion of documents is possible after authorization, and can be further controlled by granting restricted access rights by organizational policy.

7. ARCHIVING PROCEDURES

7.1 Standard Operating Procedures

The following issues should be addressed in the Archive Standard Operating Procedures, where applicable:

- Access to the archives
- Definition and description of the archive
- Indexing procedures, including electronic records
- Conditions under which records and materials should be stored
- Procedures for the receipt of records and materials to be archived
- Procedures for accessing, removal and return of records and materials
- Responsibilities of the archivist and archiving staff
- Security of the archive facility and the records and materials retained

- Climate control
- Retention period
- Disposal of archived records and materials
- Contract archiving services, if applicable
- Transfer to sponsors or third parties, if applicable
- Disaster recovery
- Training requirements for the archivist and archiving staff
- Frequency of archiving non-study specific records
- Periodic refreshing of electronic records

Labfolder implementation: Labfolder's Standard Operating Procedures contain various practices to ensure maximum data security and integrity, promoting secure and quality research management. In short, Labfolder addresses the following:

All of the mentioned procedures above are also mentioned in Labfolder's implementation of the GLP Principles No 1 and 10.

- Access control with restricted access, requiring a unique login/password combination
- Definition and description of the electronic archive facilities provided by Labfolder
- Full audit trail with indexing procedures, including timestamps and electronic signatures
- Procedures for accessing, removal and return of records and materials
- Security procedures to prevent data from unauthorised access, corruption, modification or loss
- Indication of retention period for stored records
- Information on disaster recovery procedures
- Requirements for Labfolder personnel, including training and GLP awareness
- Periodic refreshing of electronic records

The SOPs are also pointed out in great detail in the Labfolder implementation of GLP Principles No 1 and No 10..

7.2 Records and Materials to be retained

Records to be retained include paper records, photographs, microfilms or microfiches, computer media, dictated observations, recorded data from automated instruments, or any other storage medium containing the data generated in the conduct of a non-clinical health or environmental safety study.

Materials to be retained include wet tissues, paraffin blocks, specimens, slides, smears, test materials / retention samples, etc. Records and materials may be study-specific, or relate to more than one study.

Labfolder implementation: Labfolder retains all (digital) data that is stored in the electronic archive. Upon entry, the original record is kept with altered versions being stored as copies of the original file. Therefore record changes do not obscure previously recorded information. All activities are recorded in an audit trail, providing a system-created timestamp - and electronic signatures - for all entries.

7.2.2 Facility records and materials

These are records and materials that are generated by a test facility/site, and may be specific to one or more studies performed at the facility/site. Such records and materials may be inspected for the reconstruction of a study and for the general assessment of the continuing compliance of a test facility with Principles of GLP. Management should address in an SOP how and by whom the archiving of these records and materials should be carried out.

The following are examples of facility records and materials that should be retained:

- Records of all inspections performed by the Quality Assurance
- Master Schedules
- Organisational charts
- Floor/site plans
- Records of qualifications, training, experience and job descriptions of personnel
- Records and reports of the maintenance and calibration of apparatus
- Validation documentation for computerised systems
- Historical files of all Standard Operating Procedures
- Environmental monitoring records
- Samples of test and reference items, if used for more than one study
- Certificates of Analysis, if used for more than one study

Labfolder implementation: This principle only partly accounts for Labfolder. As an electronic archive facility, most of the examples mentioned above do only account for physical test sites.

In terms of validation documentation, Labfolder retains all records that validate the system for archive and research purposes. SOPs are also available, providing information on security procedures to ensure maximum data protection and integrity.

7.3 Indexing

The Principles of GLP requires that records and materials retained in the archives be indexed so as to facilitate orderly storage and rapid retrieval. The system of indexing employed should facilitate the retrieval of all information required to reconstruct a study from both the study and the facility records.

Labfolder implementation: The Labfolder system provides an audit trail and complex index of all records. This allows for the quick and complete retrieval of research data and for the historical reconstruction if needed.

7.4 Placement of Records and Materials into the Archives

On completion (including termination) of a study the Study Director is responsible for ensuring that all study documentation, data and related records and materials are archived in a timely manner. The Study Director retains responsibility for the integrity of study documentation, data and related records and materials until they are accepted into the archive. Test facility management is responsible for maintaining the integrity of the records and materials once they are transferred to the archives. Test facility management should ensure that a time period for the transfer of material from the Study Director to the archivist is defined that is in compliance with national regulatory requirements, where existent.

Prior to transferring records and materials to the archive, the Study Director is responsible for establishing an inventory to be archived, confirming completeness of records and materials, and ensuring that these records and materials are transferred in their entirety to the archive.

The archivist or archive personnel should check the completeness of records and materials upon their arrival by comparison with the inventory list and acknowledge receipt.

Test Facility Management should ensure that non study specific (facility) records such as maintenance records, staff training records, organisational charts, etc. are archived on a regular basis defined by test facility SOP. Procedures for archiving these records and materials should be similar to those employed for study records and materials.

In multi-site studies, procedures for archiving records and materials generated at individual test sites should be agreed upon and documented prior to/ or at the initiation of the study.
The Principal Investigator should notify the Study Director of the transfer of study materials to the archive.

7.5 Transfers

On occasion it may be necessary to transfer archived records and materials from one archive to another at a different physical location. The archivist transferring the records and materials, including electronic records, should ensure that there is a documented agreement and transfer plan between test facility management, management at the receiving facility and the sponsor before any transfer occurs. The documentation should include details of the records and materials to be transferred, the contact details/address of the receiving facility, and the means of transfer between locations.

Records and materials to be transferred should be clearly described in appropriate chain of custody documentation prepared by the archivist. The transportation of the material, and associated paperwork, between the two locations should be undertaken in such a way as to minimise the risk of loss or damage of the records and materials.

The recipient of the transferred records and materials should check that they correspond with the associated chain of custody documentation, and once accepted, the recipient becomes responsible for ensuring that anything is maintained and preserved appropriately. All parties involved in the transfer should retain copies of the chain-of-custody documentation. Transfer of archived materials between computerised archive systems should be documented and conducted according to a migration plan.

Labfolder implementation: Labfolder presents an electronic archive facility for the secure storage of digital data. With most of this principle relating to physical archives, Labfolder can only provide a documented agreement and secure transfer plan for the migration of electronic data files. As a computerized archive system Labfolder offers a migration plan that minimises the risk of damage, manipulation or loss of electronic records during migration to a new storage location. For the physical transfer of research data - such as print outs, laboratory equipment and others - the sole responsibility lies with the respective test facility management. However, Labfolder can provide guidelines and training for clients to ensure compliance.

7.6 Retention Period

Retention periods should be, and in some countries are, defined by regulatory (receiving) authorities.

The retention period defines the minimal period of time that data must be retained and must be available for review if the safety studies that support the registration of new products or marketed products need to be verified. It is strongly recommended that records and other sustaining material associated with such safety studies be retained for as long as regulatory authorities might request GLP audits of the respective studies.

When performing routine test facility inspections that include the carrying out of study audits,

monitoring authorities and/or their inspectors will normally select studies completed or performed since the previous inspection or, in some countries, the two previous inspections. If the retention periods have not been defined by an applicable regulatory authority, it is highly recommended that records and materials should be retained for at least three inspection cycles so that inspectors can evaluate the compliance of the test facility with the Principles of GLP. For those studies that will not be submitted to regulatory authorities it may be acceptable (if justified) to dispose of the study specific records and materials after this period.
The Principles of GLP state: “a sample for analytical purposes from each batch of test item should be retained for all studies except short-term studies”. Samples of test and reference items may however be discarded when the quality of the material no longer permits evaluation. Obviously the storage conditions should be optimal for these samples. 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.

Perishable specimens, such as blood smears, freeze-dried preparations and wet tissues, may also be discarded when they can no longer be read or evaluated. For non-perishable specimens the general guidance will apply.

Electronic media may be discarded when the media itself no longer permits evaluation (due to hardware or software issues) provided the disposal is authorized, documented, and electronic records are migrated and any record losses documented.

Labfolder implementation: Labfolder’s retention period for the storage of research data is (enter period of time). In the cloud version, records are stored for three years beyond the subscription period unless explicitly being deleted by the user. On local server installations, retrieval throughout the records retention period is within the responsibility of the hosting organization.

7.7 Retrieval

Appropriate procedures should be established for retrieval of archived records and materials. These procedures should define the circumstances under which they may be removed from the archive (e.g. for inspection/ regulatory purposes, by sponsor, etc.). The procedures should also describe in detail who is permitted to withdraw records and materials, who can authorise removal of records and materials and the timeframe within which records and materials should be returned to the archives.

Viewing electronic records without the possibility of alteration or deletion of the archived electronic record or replicating within another computerized system does not constitute “retrieval” of a record.

The Principles of GLP require that movement of records and materials in and out of the archives should be properly recorded. There should be mechanisms in place to enable the archivist to track the movement of records and materials from and back to the archive and to identify any records and materials not returned within the specified timeframe. On return to the archive, the records and materials should be verified by the archivist or a designated member of the archive staff to be complete and unaltered.

Management should be informed of any discrepancies.

Labfolder implementation: In general, access to data stored in Labfolder requires a clear authentication via a unique login/password combination, only known to the respective author/account owner. Additionally, the author/owner can assign administrative roles and share controlled access rights with others. Read/write access to records as well as the possibility to sign can be managed, granted and revoked at any time by the account owner, allowing to enforce authority checks and access control for stored data.

7.8 Disposal of Records and Materials

Test facility management's and, if applicable, the sponsor's authorisation should be obtained before the disposal of any archived records and materials. The reasons for disposal should be recorded. It may be appropriate to inform QA. The disposal of archived records and materials should be documented.

Labfolder implementation: All records stored in the Labfolder system have only one original author/owner that cannot be changed during the entire lifecycle of a document. In order to maintain data integrity, every single record as well as changes to a record are tracked in a full audit trail with an automatically generated timestamp which cannot be manipulated by others. The deletion of documents is possible after explicit authorization, and can be further controlled by organizational policy.

8. ARCHIVING ELECTRONIC RECORDS

Requirements for the archiving of electronic records are the same as those for other record types, but there are additional features, which are addressed below. It is therefore important that management ensures that appropriate Standard Operating Procedures are established for the archiving of electronic media in a secure GLP environment.

8.1 Decision to Retain Records Electronically

The decision to retain records in electronic form has important implications. The long-term retention of electronic records may influence the choice of storage medium since deterioration of storage media can lead to permanent loss of records. Computer technology is developing rapidly and devices capable of reading storage media in common use today may not be available in the future. Electronic records should be stored in a format that is readable for the duration of the applicable record retention period.

Labfolder implementation: Labfolder's retention period for the storage of research data is (enter period of time). In the cloud version, records are stored for three years beyond the subscription period unless explicitly being deleted by the user. On local server installations, retrieval throughout the records retention period is within the responsibility of the hosting organization (as stated under GLP Principle No 15, 7.6).

8.2 Storage Media

Records may be migrated from a computerised system onto a storage medium, e.g. magnetic tape, diskette, CD or optical disk that can be placed in a physical archive. Archive procedures should include the consideration of additional controls for the migration of electronic records from old to new media of these records. Consideration should be given to future access to the data or records stored on these media. There may be a need for special storage conditions, e.g. protection from magnetic fields.

Labfolder implementation: Labfolder allows for the migration of electronic records to other storage mediums. In terms of data transfer, Labfolder offers guidance and a migration plan that minimises the risk of damage, manipulation or loss of electronic records during migration to a new storage location. However, this sole responsibility during data migration lies with the account author/owner. After the successful transfer, guidelines of the new storage medium apply.

8.3 Defined Archive Area on a Computerised System

Electronic records may be moved from the production part of a computerised system to a discrete, secure archive area on the same computer system (physically separated, e.g. file record systems), or explicitly marked as archived (logically separated, e.g., database record systems). Records should be "locked" such that they can no longer be altered or deleted without detection. Records archived in this way must be under the control of a designated archivist and be subject to equivalent controls to those applied to other record types.

Labfolder implementation: Archive facilities provided by Labfolder are under special protection. Audit trail and full versioning record all data-related activities. All uploaded records are logged

and “hashed” to verify integrity, ensuring that records cannot be altered or deleted without detection and the permission of the account owner/author. The archivist is employed by test site management, thus the responsibilities lie beyond the scope of services provided by Labfolder. However, Labfolder can provide guidance and training to ensure GLP-compliance.

8.4 Dedicated Electronic Archive System

Records may be migrated from the computer system that captured or manipulated them into a separate dedicated electronic archive system. All data associated with the reconstruction of the study needs to be migrated. This includes, but is not limited to raw data, metadata, audit trails, e-signatures and associated hardware and software that allow availability of all records in the future.

Where ideally the archivist should be the system-owner for the electronic archive system, it is recognised that the electronic archive system is likely to be managed by information technology (IT) personnel. The archivist, being ultimately responsible for managing the archive, has an important role in helping to ensure that regulatory requirements are met. Test facility management should, therefore, take care that the co-operation and co-ordination between the archivist and information technology personnel is ensured.

These IT staff should follow procedures agreed with the archivist and/or test facility management.

Labfolder implementation: In case of data migration, Labfolder offers a migration plan to ensure the safe transfer of all records to a new archive facility. Labfolder IT personnel is available for advice and guidance during the whole migration process. In close collaboration with the archivist and the test site facility management Labfolder ensures an uninterrupted transition of data as well as compliance with regulatory requirements.

8.5 Maintenance and Preservation of Electronic Records

Electronic records are at risk without a preservation process to ensure that these records are available in the future. Procedures should be in place to ensure that essential information remains complete and retrievable throughout the specified retention period. If the record medium requires processing in order to render the retained records into a readable format, then the continued availability of appropriate equipment should be ensured. If availability cannot be guaranteed, the possibility of migrating data from one medium to another should be considered.

If electronic record migration is necessary, the process of migration should be fully documented, and validated to ensure complete and accurate migration of the original records before they are lost or destroyed. If it is impossible to migrate the records to new electronic media it may be necessary to migrate to paper records. Duplication of electronic archives should be considered as part of an archive preservation plan.

Labfolder implementation: Labfolder's retention period for the storage of research data is (enter period of time). In the cloud version, records are stored for three years beyond the subscription period unless explicitly being deleted by the user. On local server installations, retrieval throughout the records retention period is within the responsibility of the hosting organization (as stated under GLP Principle No 15, 7.6).

In case of data migration, Labfolder provides full documentation of the transfer process, assuring that all original records have been successfully and securely transferred to a new electronic archive system.

9. QUALITY ASSURANCE

Archive facilities and processes constitute an important component of a GLP compliant test facility. These aspects should, therefore, be subject to routine quality assurance (QA) inspections and audits. When archived records and materials are transferred, the transfer process should be monitored by the conduct of directed QA inspections.

Labfolder implementation: To ensure the provision of data quality and integrity, the Labfolder system is subject to regular monitoring and scanning processes. In case of data migration, the transfer process is available for QA review.

10. CONTRACT ARCHIVE SERVICES

The Principles of GLP require that a test facility has an archive to provide secure storage of records and materials. This will usually consist of archive facilities within the test facility itself, but the use of contract archive facilities is not precluded. In this situation, the guidance contained within this document should equally apply to the contract archive facilities. Contract archive facilities are involved in processes dealing with GLP studies and thus should be subject to inspections by Quality Assurance Programs, and by Monitoring Authorities, to assess the compliance with the GLP Principles. The following factors need to be considered when using contract archive facilities:

10.1 Contracts and/or Service Level Agreements

There should be a formal agreement that details the level and conditions of service to be provided by the contract archive facility. This agreement should cover the description of the records and materials to be archived, the transportation of records and materials to the archive, chain of custody, access to stored records and materials by the contract archive, services provided (e.g. regular check of containers for wet tissues), safety, storage conditions, duration of storage, method of retrieval/access and method of return/disposal, QA activities and responsibilities, and other considerations as addressed in this document. The contract archive organisation should follow relevant SOPs, either their own, or, in their absence, those provided by test facility management. This should be specified in the agreement.

Labfolder implementation: Labfolder provides a formal service level agreement that details the level and conditions of service to be provided by the contract archive facility. Apart from Labfolders's general SOPs the agreement contains valuable information on access control, data storage and retrieval as well as standard regulations and responsibilities associated with the secure and responsible archive facility management.

Additionally, a Terms of Use outline is available for potential and existing clients, providing important information on liability, confidentiality and user obligations amongst others.The full agreement is available at https://www.labfolder.com/terms-use.

In terms of security, Labfolder also offers a security statement, providing an overview of the system's security procedures which can be obtained at https://www.labfolder.com/security.

10.2 Access Arrangements

Procedures should define how, and when, stored records and/or materials can be accessed by the depositor of the records and/or materials. Any such access should be approved and documented.

Labfolder implementation: Labfolder employs strict access arrangements to ensure maximum protection and integrity of sensitive research data. Access to a Labfolder account requires a login/password combination, only known to the account owner. Access control features allow the owner/author to control, grant and revoke access to stored records. A system-generated audit trail records all activities and provides all entries and record changes with an automatic timestamp to prevent manipulation or loss. Deletion of records can be controlled and prohibited by organizational policy.

10.3 Conditions of Storage

The conditions of storage and the procedures followed by the contract archive facility should be the same standard as those expected of a test facility archive which is operated in compliance with the Principles of GLP. This will include the appointment of a suitably qualified archivist, written and approved SOPs describing archiving related activities and the provision of suitable storage areas to prevent deterioration or loss of stored records and materials.

Labfolder implementation: The archive facilities provided by Labfolder are compliant with the Principles of GLP. Qualified Labfolder personnel is in charge of all archiving activities. Approved SOPs are in place to provide information on archiving activities, storage conditions and safety procedures. Storage conditions and other archive-related policies are also pointed out under GLP Principle No 1, Section 7 and 10; No 10, Section 6 and 8; No 15 Section 5, 6 and 7.

10.4 Inspections

Periodically the contract archive facility should be inspected by Quality Assurance from or on behalf of the test facility or the sponsor, where applicable, to ensure that the conditions of the service level agreement are being met and that the systems and procedures operated by the contract archive facility comply with their SOPs and the Principles of GLP.

Labfolder implementation: Test facilities or the sponsor have the option to monitor and scan the Labfolder system with the intention to ensure GLP- compliance as well as conformity to the established SOPs. The close inspection is also used to certify that the conditions of the service level agreement between both parties are met.

11. CLOSURE OF AN ARCHIVE

11.1 Principle

The OECD Principles of Good Laboratory Practice (in Section 10.4) state: If a test facility or an archive contracting facility goes out of business and has no legal successor, the archive should be transferred to the archives of the sponsor(s) of the study(s)".

Labfolder implementation: In case of closure, the Labfolder system - including all stored information - will be transferred to a succeeding electronic archive facility. In close collaboration with the new archive facility the data transfer will be arranged. Of course, these procedures will be conducted with the utmost safety concerns to ensure a safe and reliable transition of sensitive research data.

11.2 Measures to be Taken

If a test facility or test site no longer intends to operate the archive in compliance with the Principles of GLP or goes out of business, the following measures have to be taken:

- The applicable national GLP compliance monitoring authority should be informed in a timely manner by the test facility.
- Test facility management should ensure that sponsors are informed as soon as possible once a decision is made to close the archive or if the facility goes out of business. Sponsors should ensure that all study-related records and materials are transferred to an alternate GLP compliant archive and retained for the period specified by the appropriate authorities.
- For non study specific (facility) records or records which relate to studies of more than one sponsor and that should be retained according to the Principles of GLP test facility management should agree with the sponsors on how to ensure that these records and materials are archived in a GLP compliant archive after the closure of the test facility or archive for the period specified by the appropriate authorities. Access of the sponsors to these study- related records and materials should be agreed upon and documented.

Labfolder implementation: The mentioned principles above relate to the responsibilities of the test facility or test site using Labfolder as contracting archive facility. Thus, this principle is beyond the scope of Labfolder. However, Labfolder can provide consultation and guidelines for clients to ensure compliance during all processes mentioned above.

11.3 Inspections by Monitoring Authorities

After the transfer to a new archive facility has taken place the GLP monitoring authority will normally inspect the new archive. In case records or materials are transferred to facilities located in another country, the GLP monitoring authority in that country should also be informed.

Labfolder implementation: After the transfer of data from Labfolder to a new archive medium, the sole responsibility lies with the new archive facility management. Therefore this principle is beyond the scope of Labfolder. However, Labfolder can provide consultation and guidelines for clients to arrange an inspection by Monitoring Authorities and to ensure GLP-compliance.

If you have any questions about how the Labfolder ELN is GLP compliant please do not hesitate to contact us anytime at feedback@labfolder.com.