Agaram TECHNOLOGIES

How Logilab SDMS helps Laboratories to enable GLP Compliance

White Paper

Part 4

V. Raghavan

Agaram Technologies Private Limited

25 – Sep - 2020

TABLE OF CONTENTS

GLP Principles During Operational Phase of Logilab SDMS

Accuracy checks

GLP lays down a very important principle that the data captured or entered in the system must be accurate. In order to ensure accuracy, GLP necessitates computerized system must have the capability to validate, verify and filter the data for accuracy. Logilab SDMS ensures that users can verify the data that is captured from the instruments can go through a workflow process. Using the workflow tool users will be guided to follow the review and approval processes so that data errors can be avoided.

Logilab SDMS also supports electronic signature. Authorised users can place electronic signatures on appropriate records with the username, password and the reason with a date and time stamp is recorded. This will ensure that users can be fixed with the responsibility to carry out necessary checks during the data transaction process.

Scheduling certain type of files generated in Lab process using file type watcher. This will ensure filtering out of unwanted data or files.

Users can identify or provide additional metadata for instrument generated data by entering batch numbers, sample types, projects, sample ids. Whatever metadata that is suitable for the instrument data, it can be tagged in meaningful names. This improves the accuracy of the data. The instrument data can be searched easily using the specific tag name.

Data Storage and Access

GLP requires that electronic data capture, storage, backup and retrieval must not violate data integrity principle. Easy accessibility, readability, restorability, security, accuracy must be ensured for data/records in a continuous manner.

The core functionality of Logilab SDMS is Scheduler. The Scheduler can capture data generated by instruments automatically. It can be configured with respect to time. Live-capture module is used as and when data is generated being used by any other software.

All the data is being stored in a secured FTP server which is the backbone for the entire system for file storage. The changes made to the files in the source will be captured with proper version control. Automated removal of files from local clients can be configured based on file deletion policy.

It is very easy to search (wider search criteria), view (using preview facility), retrieve and navigate the data (including all the versions) inside the SDMS Explorer which is similar Windows Explorer. SDMS Explorer is easily accessible by authorised personnel using role-based access control. Also, data can be logically separated by creating multiple FTP storage systems.

Printouts

GLP principles require the Laboratory to have the facility to print the audit trail and data records at any point of time. Logilab SDMS supports easy readability of data in PDF format and printing. Human Readable data is also a mandatory process as per 21 CFR Part 11.

Whenever there is a report generated by an instrument software, users can store this report in a human readable format. Logilab SDMS provides a virtual PDF printer. Once the users have finalised the data inside the instrument software, Logilab virtual PDF printer can be used to generate a human readable PDF format of the report and then send to printer for printing on a paper if required.

Audit trails

GLP principles requires the computerized system to have n audit trail module which can provide documentary evidence of activities that have affected the content or meaning of a record at a specific time point. Audit trail for a computerized system should be enabled, appropriately configured and reflect the roles and responsibilities of study personnel. The ability to make modifications to the audit trail settings should be restricted to authorised personnel.

Audit trails module records each and every user & system action namely uploads, downloads Logins, Logoffs, failed logins, password policy, etc. Audit Trail has features to

filter data based on user-based or module-based, time-based, type of audit trails. The audit trail settings are carried out only by Administrator users. Auditors can review specific audit trails and record/mark them. Audit trails can be exported such that Auditors can take them away as part of their audits.

The Audit Trail module records data with Time stamp, who did what and when and why at any point in time. Any communication failures that happen with respect to instrument are also audit-trailed inside the system.

Change management and configuration management

According to GLP Principles, Laboratories should have appropriate procedures for configuration management and change management in the operational phase. Both change and configuration management should be applied to hardware and software.
Agaram follows Support Agreement (SLA) with Laboratory customers with all necessary precautions and information is prepared in collaboration with them so that business continuity, reliability and responsiveness are ensured. Agaram's helpdesk support will ensure that issues encountered after go-live are properly recorded, segregated as issue or change, responded and resolved in collaboration with Agaram's Quality Assurance and Product Development team. The changes or bug-fixes or patch/upgrades are deployed in the production after Testing by QA and then by Users' signoff.

Periodic review

Agaram' s support team as well as Marketing team periodically takes customer inputs and feedback for the software product performance in terms of functionalities, issues/bugs, reliability and security. The market information as well as regulatory compliance requirements are also considered during the periodic review by Product Development to incorporate new changes, fixes, patches and upgrades of the product.

Security

According to GLP Principles, physical and logical security of the hardware and software are paramount importance and Logilab SDMS has the functionality to configure Users, their access rights restrictions and password policies.

Logilab SDMS has got its own built-in security module where Admin Users will be able to create users, groups and provide rights for users to access various parts of the applications, functionalities of the application or only view the data.

Also, password policies, which correspond to 21 CFR Part 11 and Eudralex Annex 11 can be setup inside the Logilab Security module with full control over the access to functionalities and data. This will ensure different operations will be performed based on the restrictions/privileges setup on the individual users as per company policies.

Data Integrity

Data Integrity is defined as, “the completeness, consistency, and accuracy of data. Complete, consistent, and accurate data should be Attributable, Legible, and contemporaneously recorded, Original or a true copy, and Accurate.”. Data integrity is a very important aspect of GLP principle and the computerized system must be able to provide the users facility to achieve this.

Logilab SDMS helps Laboratory users to achieve this by:

1) **Attributable**: Logilab SDMS captures instrument data along with meta data with information like which instrument, which user, on what data and at what time.

2) **Legible**: The data handled by SDMS is always electronic, easily accessible and human readable.

3) **Contemporaneous**: Data and meta data are captured and stored as and when generated (along with exact data and time stamp) and not the data generated at a different point of time. SDMS’s mobile capability further enhances as the user does not need computer (PC or desktop) but simply using mobile device.

4) **Original/true data**: Logilab SDMS helps users to e-sign the data and metadata as true and original

5) **Accurate**: Data capture is automated and there is no human intervention required in Logilab SDMS system. This is achieved by the heart of the SDMS system called 'Data Scheduler'.

Incident Management

GLP principles requires laboratories that during the daily operation of the system, records should be maintained of any problems or inconsistencies detected and any remedial action taken.

Logilab SDMS has an audit trail module which records each and every user & system action namely uploads, downloads Logins, Logoffs, failed logins, password policy, etc. The Audit Trail module records data with Time stamp, who did what and when and why at any point in time. Any communication failures that happen with respect to instrument are also audit-trailed inside the system. This helps easy trouble-shooting of any issues encountered.

Electronic Signature

According to GLP, an electronic signature function of a computerized system should be addressed in the requirements for the system by the Laboratory for electronic records and validated and described in the system procedures.

It should be possible to associate all changes to data with the persons making those changes by use of timed and dated (electronic) signatures. Reasons for change should be given. Password re-entry should be considered as a minimum requirement for an electronic signature and Reasons for change should be entered. It can be considered as equivalent to hand-written signature.

Logilab SDMS has the functionality to incorporate electronic signature for the changes of system parameters. The users who make the changes must enter username, password and reasons for the changes. They are recorded in the audit trail module of the application.

There is also a workflow to configure who is the reviewer and who is the approver of the electronic data generated. Electronic signature is also recorded during review and approval process.

Data approval

As mentioned earlier, Logilab SDMS has a workflow using which reviewer and approvers can be configured. The corresponding users can either review or approve the instrument generated data and metadata which helps to validate and improve accuracy and accountability. This is a very important requirement of GLP.

Data archival

GLP has specified data archival as one of the requirements for laboratories and the computerized system must support the users to decide and carryout which data can be archived for a specified period clearly separated from the current data.

Using Logilab SDMS Scheduler, the archive policy can be implemented by scheduling the archival of data (i.e. file move) to the desired location. The retention period setting up (i.e. retaining the files to a specified period and removing them after that) can be setup by configuring the File delete options in the Scheduler.

Business continuity and disaster recovery

GLP requires the Laboratories to document the Business continuity and disaster recovery plans and follow them judiciously to avoid stoppage of operations in the event of any system failures.

Agaram recommends to the customer to provision proper load balancing and backup servers to take care of the system failures. Automatic switching to the backup server is highly recommended. Logilab SDMS fully supports high availability feature.

References

1) OECD SERIES ON PRINCIPLES OF GOOD LABORATORY PRACTICE AND COMPLIANCE MONITORING

NUMBER 10

GLP CONSENSUS DOCUMENT - THE APPLICATION OF THE PRINCIPLES OF GLP TO COMPUTERISED SYSTEMS

ENVIRONMENT MONOGRAPH NO. 116

Published by:

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, Paris.

2) Series on Principles of Good Laboratory Practice and Compliance Monitoring

No. 17

Advisory Document of the Working Group on Good Laboratory Practice

Application of GLP Principles to Computerised Systems

Published by:

Environment Directorate

ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, Paris.

Appendix

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

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

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

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

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

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

Eudralex Annex 11: EudraLex : The Rules Governing Medicinal Products in the European Union - Volume 4. Good Manufacturing Practice - Medicinal Products for Human and Veterinary Use
Annex 11: Computerised Systems
Published by EUROPEAN COMMISSION, HEALTH AND CONSUMERS DIRECTORATE-GENERAL, Public Health and Risk Assessment - Pharmaceuticals

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

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

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

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

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

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

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

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

21 CFR Part 11: It is the part of Title 21 of the Code of Federal Regulations that establishes the United States Food and Drug Administration (FDA) regulations on electronic records and electronic signatures (ERES). Part 11, as it is commonly called, defines the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records (Title 21 CFR Part 11 Section 11.1 (a)).

(Concluded)