Supporting tools for GLP / 21 CFR Part 11

Clarity provides the following tools to enable laboratories to comply with laboratory management regulations and general GLP practices such as 21 CFR Part 11. This document serves as a quick overview of the tools available in Clarity, for detailed descriptions of compliance with different regulations' sections refer to D128 datasheet. How to set up Clarity in Regulated Environment is described in M132 manual.

Clarity Features

1. **Certificate of Software Validation** (labeled as D021 Datasheet) certifies that Clarity was developed, tested, and structurally validated following a Certified Quality System conforming to GLP/GMP, GAMP and ISO 9001 guidelines. The certificate for the current software version can be downloaded from www.dataapex.com. The D021 Datasheet for older software versions is available upon request and can be found in *...\DOC PDF\DATASHEETS* section of the installation media (not in the Clarity installation itself).

2. **Installation Qualification** (IQ) is an integral component of the station. This test verifies that Clarity and its components have been properly installed and records the results in a printable protocol.

3. **Operational Qualification** (OQ) validation is an optional package requiring SST extension (p/n A22) available for testing and validating the station. Depending on the HW setup, it can be performed using either a virtual or a physical (Validator) signal generator.

4. **GLP Options** are station-level settings that enforce behavior to protect data integrity. They can, for example, prevent user account deletion (ensuring complete list of users), require users to enter a reason for change, or hide the user list in the login dialog to ensure two-factor identification. Other options can restrict the use of the spike filter, or limit saving data to the current project only. (Not all available options are listed here.)

5. **User Accounts** provide unique, password-protected user profiles that define individual rights within the station and restrict access to authorized instruments only. Password expiration and minimum length alongside other password restrictions can be enforced according to company policy.

6. **Electronic signatures** enable users to sign chromatograms electronically, either using their Clarity user credentials or personal digital certificates. Each signature record contains the signer's name, date and time, and the meaning of the signature (for example, *Measured by* or *Approved by*).

7. **Audit Trail** records all system actions, data modifications, and configuration changes in secure audit trails that are stored as one general file (Station Audit Trail) as well as parts of the corresponding files — chromatograms, methods, calibrations, and sequences. Each file therefore contains its own complete audit trail. Every modification entry includes the username, date and time, and can also contain the reason for change if this option is enabled in GLP Options. In addition to their own audit trail, methods and chromatograms contain a complete version history.

8. **System Suitability Test (SST)** – extension suitable for method performance and system consistency monitoring. (Required for OQ.)

9. **Printed reports** include page numbering and their contents are customizable. Among other options, it is possible to include the date and time of analysis and printout, and information about applied electronic signatures. Reports can be printed physically or as PDF files.

ALCOA+ principles

Data integrity is ensured by following **ALCOA+** principles, meaning data should be attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring and available. While some of these principles are achievable on the SW level alone, some overlap with broader end-user SOPs and data handling, and these must be set accordingly by the end-user organization to fulfill all principles.

1. **Attributable** – All records are attributable to the persons who generated them including who performed which action and when. This is ensured by each user having their own user account. Each action performed in Clarity is logged under the user account which executed it.

2. **Legible** – All data must be legible and permanent throughout their lifecycle. Legibility is ensured by possibility of opening data from older Clarity version on newer ones. Permanent part must be ensured by Windows setting according to M132 manual for the software part and by end-user organization on the HW side of computerized system (access to the hard drives etc.).

3. **Contemporaneous** – Data is created when the activity is performed and automatic timestamps follow the order of execution of given actions. For this purpose, Clarity provides overall Station Audit Trail as well as audit trails for individual files as described in the first part of this document.

4. **Original** – Data must be stored in their original format. For Clarity data integrity and persistence must be ensured by setting up Windows according to M132 manual. HW side of the system is again responsibility of end-user organization as mentioned in second point.

5. **Accurate** – Data should be complete, free from errors and truthful. It could be also said that the records include the "whole truth" without uncontrolled manipulation. This can be achieved by proper Windows and Clarity settings according to the M132 manual as well as strict adherence to end-user SOPs to minimize risk of any errors occurring during the entire process.

6. **Complete** – Data should not only include the original records but also any record of repeat measurement etc. It should be clearly identified which person is responsible for each record. In Clarity this is again achieved by combination of audit trail and proper GLP settings to ensure that every single measurement results in separate chromatogram file.

7. **Consistent** – Data must be recorded in an expected sequence of events. Similarly to the **Contemporaneous** any action in Clarity is logged into audit trail(s) with an automatic timestamp.

8. **Enduring** – Data must remain accessible throughout its lifecycle. It is end-user organization's responsibility to ensure that data is securely backed up, and it can be restored in case of storage HW failure. Clarity either provides a simple archiving tool described more in M132 manual or it is possible to use third party utility to back up relevant files.

9. **Available –** Data must be readily available for review, audits etc. during their lifetime. Similarly to the previous point if the data is archived it is end-user organization's responsibility that it can be restored when required.