

# Clarity Detailed GLP Compliance Overview

## Introduction

US *Part 11* in *Title 21* of the *Code of Federal Regulations (CFR)*, *EudraLex Chapter 4, Annex 11*, and other national legislations or guidelines (such as those in China or Brazil) define requirements for **electronic records and electronic signatures** in regulated pharmaceutical organizations. The objective of all of these regulations is to ensure that all created and used electronic records are **Attributable, Legible, Contemporaneous, Original, and Accurate** (known as the ALCOA principle) and that they are maintained with integrity throughout their lifetime. These regulations have been in place and applicable for quite a long time (*Part 11* was released in 1997 and enforced in 1999), and they follow the same principles as those governing paper-based records.

This datasheet provides a set of answers for Clarity users (version 10 and higher) whose organizations have to comply with these regulations. Regulatory agencies, such as the US FDA or UK MHRA, have a legal relationship only with pharmaceutical companies, not with the Chromatography Data Station (CDS) manufacturer (DataApex). It is the **CDS end-user organization's responsibility** to ensure that all functionalities of Clarity used for both data acquisition and data processing are properly configured and utilized to maintain laboratory compliance.

Operational compliance status can be fulfilled not only by using technical controls Clarity provides but also through **procedural controls established** by the user organization (such as **SOPs** – Standard Operating Procedures) that cover non-technical requirements defined by the regulations. Examples of such procedural controls include internal audit programs, staff training, and emergency procedures.

The end-user organization is also responsible for ensuring that relevant staff (laboratory operators, laboratory management, and others) have good knowledge of the SOPs and that all the staff correctly follow them. During a regulatory agency audit, staff members may be required **to demonstrate adequate knowledge of and adherence to the applicable SOPs**.

This datasheet provides a detailed description of how Clarity (version 10 and higher) supports its users and organizations in meeting the requirements stated in the related regulations. All these detailed descriptions are based on the assumption that access to the system (including instrument hardware and software) is controlled by the staff that is responsible for the electronic records contained in the system and Clarity is set according to M132 manual. Thus, the Clarity environment is designed as a "closed system" as defined in *21 CFR Part 11.3 (b)(4)*. Clarity is not designed to be deployed in a regulated environment as an "open system" according to the definition given in *21 CFR Part 11.3 (b)*. If the Clarity user organization decides to deploy Clarity in an "open system" environment, it is solely the Clarity user organization's responsibility to fulfill all related requirements in order to operate Clarity in a compliant manner. DataApex does not provide support for Clarity in an "open system" configuration in the regulated environment at all.

## Area of interest of 21 CFR Part 11 and other regulations

### 21 CFR Part 11

21 CFR Part 11 deals with selected areas of laboratory practice in regulated organizations that mainly originate from the implementation of the ALCOA principle. These areas are:

- Security/Protection of all relevant electronic records
- Work attribution
- Electronic signatures (usage of electronic signatures is optional, but once used, it must comply).

### Security/Protection of all relevant electronic records

This area can be explained as a requirement to have "the right data to be accessible only by the right people". Organizations operating in regulated environments must be able to identify each user and ensure that system access is granted only to appropriately trained and authorized personnel, as defined in parts 11.10 (d), (g), (i) and 11.100 (b). Furthermore, organizations must clearly define the level of access granted to each authorized individual, since laboratory personnel typically have different responsibilities depending on their job roles. Selected users should have only the access privileges necessary for their assigned tasks and should be able to access only the data relevant to those tasks.

### Attribution of work

Attribution of work simply documents the performed work in terms of "who," "what," "when," "where," or "why." Built-in audit trails record such actions of users, thus linking individuals of laboratory staff and their work performed in Clarity. Therefore, it is possible to reconstruct a complete list of actions done with the selected electronic record using audit trails.

### Explanations of individual terms:

- Who: clear identification of the user who performed a particular action resulting in a modification or creation of an electronic record
- When: clear declaration of the time and date when the action occurred
- What: definition of the performed action and, if applicable, indication of both the old and new (changed) value
- Where: clear identification of the affected electronic record
- Why: the user performing modification is asked to fill in the reasoning behind the record modification

### Electronic signatures

Electronic signatures are not required by 21 CFR Part 11. However, if they are used, they have to be used in a compliant manner according to given regulations. When an organization decides to use electronic signatures, the following conditions have to be assured:

- Showing of Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: the printed name of the signer; the date and time when the signature was executed; and the meaning (such as review, approval, responsibility, or authorship) associated with the signature
- Electronic signatures are present whenever the signed record is displayed or printed
- Electronic records are permanently bonded with their respective records and cannot be removed from their respective electronic records

## DataApex's comments on requirements stated by 21 CFR Part 11 and other worldwide related regulations and their linkage to Clarity 10 and higher

The following text is organized into sections related to different areas of laboratory practice in regulated organizations. Every requirement is followed by DataApex's comment addressing the respective requirement, and if applicable, the respective Clarity tools are mentioned.

### Validation of the (Computerized) System

- **21CFR §11.10 (a)** - *"Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records."*

**DataApex:** This requirement is included in all common regulations (*Annex 11, Part 4, Brazil GMP 572*) in this field. The final responsibility for validating (computerized analytical) system is in the hands of the Clarity user organization. Clarity provides integrated tools to help to validate a complete (computerized analytical) system. Clarity offers Installation Qualification (IQ) and Operational Qualification (OQ) procedures for validation of the Clarity software. It is not possible to rely solely on the inbuilt Clarity IQ and OQ procedures for the validation of a complete (computerized analytical) system. During the development, DataApex extensively tests and verifies if Clarity provides accurate, reliable, and consistent performance, but in the end, it is the Clarity user organization that has to demonstrate that a sufficient validation of a complete (computerized analytical) system has been performed.

- **EudraLex 4, Annex 11, Principle B** - *"The application should be validated; IT infrastructure should be qualified."*  
**Brazil GMP 577** - *"The system should include, where applicable, verification of data entry and processing."*

**DataApex:** The Clarity user organization must be able to demonstrate, through its validation, that Clarity and the associated analytical instruments are suitable for their intended use. If Clarity is used in a network environment, the validation of the used infrastructure is the responsibility of the Clarity user organization. Clarity itself does not provide any direct tools to assist the user organization in this process.

### Security, Protection, and Retrieval of Records

- **21CFR §11.10 (b)** - *"The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records."*  
**EudraLex 4, Annex 11, point 8.1** - *"It should be possible to obtain clear printed copies of electronically stored data."*  
**Brazil GMP 583** - *"In the case of quality audits should be possible to obtain printed copies of electronically stored data."*

**DataApex:** Clarity allows all generated records to be printed directly to paper or exported to commonly readable formats (such as PDF, XPS, or CSV), which can be accessed outside the Clarity environment.

- **Brazil GMP 585** - "Data should be protected by performing backups (backup) at regular intervals. § 1 The backup data must be stored for a set time and place separate and safe. § 2 There must be procedures to ensure the process of restoration and maintenance of data backup."
- EudraLex 4, Annex 11, point 7.2** - "Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically."
- China GMP 163** - "Batch records stored electronically should be protected by back-up transfer on magnetic tape, microfilm, paper or other means."

**DataApex:** The Clarity user organization is responsible for backing up all necessary data. There is an Archive tool in Clarity that simplifies backing up data, but any appropriate backing-up solution can be employed for this purpose if suitable for the environment of the Clarity user organization. The Archive tool can also be executed automatically using the standard Windows Task Scheduler, which enables a certain level of backup automation within Clarity. In all cases, the selected solution should be validated for its intended purpose.

- **21CFR §11.10 (c)** - "Protection of records to enable their accurate and ready retrieval throughout the records retention period."
- EudraLex 4, Annex 11, point 7.1** - "Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period."
- EudraLex 4, Annex 11, point 17** - "Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested."
- China GMP 163** - "It is particularly important that the data are safe, and readily available throughout the period of retention."
- Brazil GMP 584** - "The data must be stored securely by physical or electronic means against accidental or intentional damage. § 1 The stored data should be checked for accessibility, durability and accuracy. § 2 If proposed change in equipment or software mentioned checks should be performed at a frequency appropriate to the storage medium in use."

**DataApex:** In terms of "electronic" security, all Clarity electronic records (such as result data, metadata, and raw data) are stored securely if the computer environment is set according to Chapter 3.1 in the M132 manual. In terms of "physical" security, the Clarity user organization is responsible for implementing appropriate security measures. When the data is backed up, the Clarity user organization is responsible for verifying that the data remains accessible, readable, and intact. This ensures that complete data sets are stored at an accessible location in a readable format. Clarity is capable of reading data generated in its previous versions.

## Authorized Access to System

- **21CFR §11.10 (d)** - "Limiting system access to authorized individuals."
- China GMP 163** - "Access should be restricted by passwords or other means."
- Brazil GMP 579 § 1** - "The inputs and data modifications can be made only by authorized persons. § 1 must be taken not to allow unauthorized persons to include, exclude or modify data in the system and can be used safety measures such as use of passwords, personal code, access profiles, keys, or restricted access to the system terminals."
- ICH Q7, point 5.43** - "Computerized systems should have sufficient controls to prevent unauthorized access or changes to data."

**DataApex:** Clarity supports unique user accounts protected by passwords. A separate Clarity user account must be configured for each individual who accesses Clarity and its data, as described in Chapter 3.3 of the M132 manual. Each Clarity user is also expected to have their own operating system account, as described in Chapter 3.1 in the M132 manual.

Be aware that the FDA issues warning letters because of failure to fulfill this requirement. Refer to the [FDA guidance document](#), page 7 (Q5).

## Audit trails

- **21CFR §11.10 (e)** - "Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying."
- **21CFR §58.130 (e)** - "All data entries shall be dated on the date of entry. Any change in entries shall be identified at the time of the change."
- **EudraLex, Annex 11, point 8.1** - "It should be possible to obtain clear printed copies of electronically stored data."
- **EudraLex, Annex 11, point 9** - "Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed."
- **China GMP 163** - "Entering or modifying data in the system should be recorded. Records stored electronically should be readily available throughout the period of retention."

**DataApex:** There are several audit trails in Clarity. Each audit trail records a timestamp for every action performed, along with the identity of the user who performed it, based on both the Clarity user account and the operating system account. User actions in chromatograms, calibrations, sequences, and method files are recorded in the respective audit trails of these files. Such audit trails are inextricable parts of the respective files, are stored within these files, and can be reviewed from the corresponding parts of Clarity. There is also a "general" station audit trail accessible from the Clarity Main Window. All audit trails can be directly reviewed from the Clarity environment.

If audit trails need to be reviewed later, they can be printed directly on paper or saved as a PDF. It is also possible to export audit trails to other formats (Text, DBF, and Excel) and review them outside of Clarity. In general, it is not possible to switch off the audit trails in Clarity, but it is possible to configure the extent of information logged into the audit trail through the Audit trail settings. Access to the Audit trail settings should be limited to selected personnel only and is set in the User Account dialog under the Open Audit trail option.

- **EudraLex 4, Annex 11, point 8.2** - "For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry."

**DataApex:** There is no kind of feature like this in Clarity. However, it is possible to review audit trails of relevant files in order to find out if any of them have been modified since their creation.

## System and its Checks

- **21CFR §11.10 (e)** - "Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate."

**DataApex:** Clarity is designed to follow common laboratory workflow for chromatographic analyses: entering sample identification information, defining the measurement method, triggering the measurement, acquiring and processing data (integrating chromatograms), linking integrated peaks and their areas to the corresponding compounds and their concentrations in the sample (applying calibration), displaying the calculated results based on the applied calibration, and generating reports.

- **21CFR §11.10 (g)** - "Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand."  
**EudraLex 4, Annex 11, point 12.4** - "Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time."

**DataApex:** Clarity allows the configuration of different privilege levels for individual users. It is the responsibility of the Clarity user organization to define appropriate user roles using the User Accounts tool. This tool should be used to restrict the actions that unauthorized users can perform within Clarity. The audit trail clearly records both the Clarity user account and the corresponding operating system account associated with each action performed. The prohibition of record deletion is ensured once Clarity and the folders containing electronic records are configured as described in Chapter 3.1 of M132.

- **21CFR §11.10 (h)** - "Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction."

**DataApex:** Clarity, when running, continuously checks if configured instruments (data input source) communicate with the software. If a communication issue occurs during data acquisition or if you attempt to send a method (operational instruction) to an instrument and the communication fails, Clarity immediately displays an error message. This event is recorded in the Audit trail. Each instrument used to create a regulated record (such as a chromatogram) is uniquely identifiable. In addition, the chromatograms generated by Clarity include read-only fingerprints of the methods (operational instructions) for all components of the chromatography system involved in the analysis.

- **21CFR §11.10 (i)** - "Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks."  
**EudraLex 4, Annex 11, point 2** - "There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties."  
**Brazil GMP 571** - "There must be cooperation between key staff and the people responsible for computer system. § 1 The people in positions of responsibility must have training for the management and use of systems that are under their responsibility. § 2 It must be ensured that people with necessary knowledge are available to advise on aspects of design, development, validation and operation of the computer system."  
**China GMP 18** - "The manufacturer should have an adequate number of managerial and operating personnel with appropriate qualifications (with respect to, including education, training, and practical experience)."

**DataApex:** The Clarity user organization must maintain documented evidence demonstrating that all personnel who develop, maintain, or use electronic records (or electronic signatures) have the appropriate education, training, and experience to perform their assigned tasks. DataApex can support regulated users by providing training for personnel who work with Clarity as part of their job responsibilities.

- **21CFR §11.10 (j)** - "The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification."

**DataApex:** The Clarity user organization has to have valid SOPs, proving that the organization's personnel are aware of the responsibility for their actions done using their electronic signature.

- **21CFR §11.10 (k)** - "Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation."

**DataApex:** (1) – The Clarity user organization has to have a valid policy defining the system of documentation. (2) – The Clarity user organization has to maintain its documentation related to the system and its changes, and such documentation should be easily accessible to relevant personnel. DataApex maintains documentation of Clarity's development and its testing; this documentation can be reviewed based on Clarity user organization requests. The Declaration of Software Validation (DataApex's datasheet D021) for the current release version can be easily accessed on the DataApex [website](#).

- **21CFR §11.3 (b) (9)** - "Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system."

**DataApex:** If Clarity should be used in a regulated environment, it must not be configured and used as an "open system".

## Data Integrity, Accuracy of Time and Date

- **EudraLex 4, Annex 11, point 5** - "Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks."

**DataApex:** As Clarity does not provide built-in automated interfaces that directly exchange data with other systems, this regulation does not need to be addressed. If the Clarity user organization exports or imports data to/from other (computerized) systems (for example, databases such as LIMS, EMS, cloud systems, etc.), it is expected that this process is validated and governed by a written procedure. Clarity is also tested in a networked environment where multiple stations use network hard drives accessible via a local network for data storage.

- **EudraLex 4, Annex 11, point 6** - "For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management."
- **Brazil GMP 580** - "When critical data are entered manually (e.g.: weighing value, lot number of a heavy input) should be a further verification to ensure the accuracy of data entered. The verification may be held by second operator or by validated electronic means."
- **ICH Q7, point 5.45** - "Where critical data are being entered manually, there should be an additional check on the accuracy of the entry. This can be done by a second operator or by the system itself."

**DataApex:** From Clarity's perspective, it is not possible to verify whether manually entered values are correct. It is therefore strongly recommended that the Clarity user organization establishes appropriate procedural controls (e.g., SOPs) requiring that all manually entered values be independently verified by another qualified person (e.g., a second operator). Relevant personnel should be properly trained in these procedures and strictly adhere to them.



## Electronic signatures (not required, optional)

- **21CFR §11.50 (a)** - "Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature."  
**EudraLex 4, Annex 11, point 14** - "Electronic records may be signed electronically. Electronic signatures are expected to: a. have the same impact as hand-written signatures within the boundaries of the company, b. be permanently linked to their respective record, c. include the time and date that they were applied."  
**ICH Q7, point 6.18** - "If electronic signatures are used on documents, they should be authenticated and secure."

**DataApex:** The Clarity user organization should consider the local legal environment related to the usage of electronic signatures, and the personnel using electronic signatures should be trained in their usage and know all the consequences of their usage. If the electronic signatures are used and the signature is applied through a certificate, it can be permanently associated with the corresponding Windows OS and Clarity user accounts. When a record is electronically signed, it includes the signer's name, the date and time of the signature, and the stated purpose of the signature.

- **21CFR §11.70** - "Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means."

**DataApex:** If an electronic record is signed electronically, the signature becomes an integral part of the electronic record (e.g., of the chromatogram), and it is not possible to extract the electronic signature from the signed document.

- **Preamble of Part 11, point 124 (2)** - "The agency believes that ... use of automatic inactivity disconnect measures that would "de-log" the first individual if no entries or actions were taken within a fixed short timeframe."

**DataApex:** Clarity offers an Auto-lock tool with a configurable timeframe when automated log-off takes place.

- **21CFR §11.100 (a)** - "Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else."

**DataApex:** Clarity user accounts settings do not allow the creation of user accounts with the same login. Therefore, each Clarity user has a unique username, ensuring the uniqueness of every user identity. The Clarity user organization must have procedural controls (SOPs) in place that define how user accounts are managed in cases such as personnel departure or job reassignment. User accounts should not be deleted, as this could compromise data traceability and the integrity of the audit trail.

- **21CFR §11.100 (b)** - "Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual."

**DataApex:** It is the Clarity user organization's responsibility to ensure that all involved individuals' identities are verified; thus, such a requirement is fulfilled.

- **21CFR §11.100 (c)** - "Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures."

**DataApex:** It is the Clarity user organization's responsibility to ensure that the electronic signatures of all involved personnel are legally binding for them in the same manner as their handwritten signatures, and all personnel involved are aware of this fact.



- **21CFR §11.200 (a)** - "Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components. (2) Be used only by their genuine owners; and (3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals."

**DataApex:** When signing electronic records using an electronic signature, it is always required to select the respective user who is going to sign the electronic record and confirm his/her password. Attempts to falsify anyone's signature would require the intentional and close cooperation of multiple people, including the Clarity station Administrator. Within a Clarity station, the Administrator role can be independent of laboratory staff (without the *Edit Chromatogram* privilege in the User Accounts settings).

- **21CFR §11.10 (b)** - "Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners."

**DataApex:** Identification of Clarity users by biometric means is not supported in Clarity.

## User identification codes and password control

- **21CFR §11.300** - "Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: (a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password. (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g. to cover such events as password aging). (c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls. (d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management. (e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner."

**DataApex:** Clarity does not allow the creation of two user accounts with the same username. It is possible to set Clarity user account expirations in accordance with the user organization's established policy. It is the responsibility of the Clarity user organization to define and maintain such a policy. The same applies to events described in parts 11.300 (c) and 11.300 (d) as well as for initial and periodic testing of devices, such as tokens or cards that carry or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

## Development of the System

- *EudraLex 4, Annex 11, point 3.4* - "Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request."
- *EudraLex 4, Annex 11, point 4.5* - "The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately."
- *Brazil GMP 576* - "The software is a critical component of the computerized system. The user of the computer system must ensure that all steps of software construction were performed according to the system of quality assurance."
- *GAMP 5, Section 7* - Whole Section 7

**DataApex:** Clarity is developed in compliance with the ISO 9001:2015 quality management standard. The related certificate can be found in D028 datasheet on the DataApex [website](#). Additional details can be provided upon request.

- *Brazil GMP 589* - "In the case of contracting for development and maintenance of computer systems should be a formal contract including the responsibilities of the contractor."

**DataApex:** It is the Clarity user organization's responsibility to have formal agreements with their suppliers.

- *21CFR §11.10 (i)* - "Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks."

**DataApex:** It is the Clarity user organization's responsibility to have properly trained staff working with Clarity. It is highly recommended to have procedural control (SOP) established and valid covering training of staff using Clarity. Clarity developers are trained according to the training policy established by DataApex, and all the DataApex personnel involved in Clarity development are required to follow this policy.

- *ICH Q10, point 2.7* - "The pharmaceutical quality system, including the management responsibilities described in this section, extends to the control and review of any outsourced activities and quality of purchased materials. The pharmaceutical company is ultimately responsible to ensure processes are in place to assure the control of outsourced activities and quality of purchased materials. These processes should incorporate quality risk management and include: (c) Monitoring and review of the performance of the contract acceptor or the quality of the material from the provider, and the identification and implementation of any needed improvements."

**DataApex:** All mentioned topics are covered by DataApex's quality manual. This quality manual can be audited upon request at the headquarters of DataApex Ltd.

## Data Integrity and Compliance With CGMP – Guidance for Industry – Draft Guidance

The following section summarizes DataApex's comment on the Data Integrity and Compliance With Drug CGMP Questions and Answers Guidance for Industry published online by the Food and Drug Administration in December 2018.

- **21CFR § 211.68 (b)** - *"Appropriate controls shall be exercised over computer or related systems to assure that changes in master production and control records or other records are instituted only by authorized personnel. Input to and output from the computer or related system of formulas or other records or data shall be checked for accuracy. The degree and frequency of input/output verification shall be based on the complexity and reliability of the computer or related system. A backup file of data entered into the computer or related system shall be maintained except where certain data, such as calculations performed in connection with laboratory analysis, are eliminated by computerization or other automated processes. In such instances a written record of the program shall be maintained along with appropriate validation data. Hard copy or alternative systems, such as duplicates, tapes, or microfilm, designed to assure that backup data are exact and complete and that it is secure from alteration, inadvertent erasures, or loss shall be maintained."*
- **21CFR §211.110 (b)** - *"All records, including those not stored at the inspected establishment, must be legible, stored to prevent deterioration or loss, and readily available for review and copying by FDA employees."*

**DataApex:** It is the Clarity user organization's responsibility to fulfill the requirement that the Clarity data be backed up on a "secure" site. There is an Archive tool in Clarity to support the fulfillment of this requirement by the Clarity user organization, but it is the Clarity user organization's responsibility if it uses this tool and whether it is used correctly.

**DataApex special note:** DataApex recommends getting familiar with the whole "*Data Integrity and Compliance With Drug CGMP Questions and Answers Guidance for Industry*" document, especially with questions no. 3, 7, 8, and 14. Regarding *FDA CFR 21*, other parts than 11, please pay attention to sections 211.160, 211.180, 211.188, 211.194, and 212.60.