

SOFTWARE

CHROMATEC ANALYTIC

BUILD 4.0

COMPLIANCE WITH

21 CFR PART 11

Edition 10.01.2025

TABLE OF CONTENTS

Introduction 4
1 Key elements of 21 CFR part 11 5
1.1 Security 5
1.2 Work Attribution 5
1.3 Electronic Signatures 6
1.4 Specifics of Chromatec Analytic Functionality 6
2 21 CFR part 11 requirements 7
2.1 Requirements for Closed Systems 7
2.2 Requirements for Open Systems 10
2.3 Requirements for Digital Signatures 10

INTRODUCTION

Part 11 in Title 21 of the Code of Federal Regulations (CFR) of US Food and Drug Administration (FDA), as well as its European counterpart, Chapter 4, Appendix 11, of the European Union Law on Drug Regulatory Affairs, include the guidelines for electronic records application by pharmaceutical organizations under their jurisdiction.

Part 11 in Title 21 of the CFR was issued in 1997 and was put into effect in 1999. The intent of these guidelines is to ensure that applicable electronic records are specified, legitimate, advanced, authentic, precise, and maintained with high integrity.

This document is intended for the users of Chromatec Analytic Software, version 3.1, whose organizations are obliged to guarantee the compliance with requirements of the regulatory acts mentioned.

The Chromatec Analytic executes management of data collection and processing for GC (Gas Chromatography), GC-MS (Mass Spectrometry) and HELC (High-Efficiency Liquid Chromatography). It is user company's responsibility to guarantee accurate use of the functionality of Chromatec Analytic while performing data collection and laboratory processing.

1 KEY ELEMENTS OF 21 CFR PART 11

21 CFR Part 11 describes:

- Secure data handling requirements;
- System work attribution;
- Application of electronic signatures (if applicable).

The analytic system applied for data collection and processing is meant by the "system".

1.1 Security

Security means the following: "Suitable persons have suitable access to suitable information".

Every user having access to the data collection and processing system must be identified by the system. The access must be available only to authorized employees who have got the required training. The different privileges for working with the system can be assigned to the employees (differentiation of access levels).

1.2 Work Attribution

Work Attribution describes "**what/by whom/when/where/why**" will be performed.

Laboratory personnel are connected to their work by recording all user actions into automatized protocol (audit trail). The audit trail protocol recordings enable the personnel and audit inspectors to reproduce the complete history of electronic records.

The audit trail protocol records enable the following:

- Precise identification of an individual accountable for taking particular action while working with the system.
- Ascertaining the precise time when the action was taken.
- Description of the action including the old value of the system parameters and the new value after the alterations if possible.
- Defining the object exposed to the operation.
- Description of the action reason can be specified in some cases, as well.

1.3 Electronic Signatures

21 CFR Part 11 **does not require** any use of electronic signatures.

Despite this, the document adduces the standards for application of electronic signatures in the case when they are applied nonetheless.

1.4 Specifics of Chromatec Analytic Functionality

The functionality of Chromatec Analytic Software provides adherence to 21 CFR Part 11 requirements.

Chromatec Analytic enables the following:

- User authentication by username and password.
- Differentiation of users data access privileges.
- Independent maintenance of user actions" audit trail (user cannot delete or alter the records).
- Maintenance of audit trail for operations performed by the system automatically without user's participation.
- Data protection from any alterations made by any third-party software.
- Creating a data audit to ensure that all alterations are traceable.
- Signing all records in the audit trail automatically by using a time-stamp indicating the time of record entry.

This functionality is off by default in Chromatec Analytic. It can be turned on in any moment by any user, who has computer administrator privileges.

After this functionality is turned on, it can be turned off by any individual, who has the privileges mentioned above. However, the **main audit trail containing audit activation/deactivation records cannot be deleted or modified**.

SDO Chromatec ensures that Chromatec Analytic Software does not have any functionality enabling the audit trail records to be deleted, altered or concealed somehow.

The audit trail resides in a protected storage, which is inaccessible for third-party software in particular.

2 21 CFR PART 11 REQUIREMENTS

The columns **Section** and **Requirement** seen in the charts listed below specify the requirements of 21 CFR Part 11 in the order in which they are represented in the reference document of the US Food and Drug Administration.

The majority of the requirements are implemented either by technical control elements (i.e. the software functionality), or by procedure control elements (i.e. standard testing guidelines).

The technical control elements represent the control elements provided by the software, i.e. by software supplier. The user company bears responsibility for the procedure control elements.

The column **Resp.** ("Responsibility") specify responsibilities for every requirement. **S** ("System") refers to the analytic system supplier (SDO Chromatec). **U** ("User") refers to user company.

2.1 Requirements for Closed Systems

If system access is controlled by individuals who bear responsibility for contents of electronic documents, the system is determined as a "closed system" and the following 21 CFR Part 11 requirements can be applied:

Section	Question / Requirement	Resp.	Implementation in Chromatec Analytic
11.10(a)	Has the system been validated in order to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records?	**SU**	**Yes**. SDO Chromatec conducts equipment and software testing to ensure accuracy, reliability and consistent performance. However, the user is obliged to accomplish validation of its analytic system in accordance with standards regulating its activity. Detection of invalid and altered records is performed by means of the audit trail. The audit trail enables tracing any data alterations. Chromatec Analytic has carried into effect the audit options for the following objects: • Instrumentation audit. • Analyses sequence audit. • Method audit. • Chromatogram audit.
Appendix 11	Has the infrastructure been certified?	**U**	User company bears responsibility for certification of such infrastructures as servers and networks.
11.10(b)	Is the system capable of generating accurate and complete copies of all required records in both human readable and electronic form suitable for inspection, review and copying by	**S**	**Yes**. The audit trail records are accessible in printed and digital versions (PDF or XPS formats).

	the FDA?		
11.10(c)	Are the records protected for accurate and convenient retrieval throughout the record retention period?	**SU**	**Yes**. Raw data and result data generated by Chromatec Analytic are stored in a protected storage location. User company bears responsibility for physical security (management of physical access to workstations and servers).
11.10(d)	Is system access limited to authorized individuals?	**SU**	**Yes**. Each user is identified by a unique user ID and password combination. Access to the system requires the entry of both identification components.
11.10(e) #1	When records are altered, is previously recorded information left unmodified?	**S**	**Yes**. Chromatec Analytic enables creating data audits while the data altering. The audit protocols reside in a protected storage and cannot be deleted or modified by means of Chromatec Analytic software as well as third-party means.
11.10(e) #2	Is audit protocol information saved as long as its subject electronic record?	**S**	**Yes**. Audit protocol information is stored in electronic record and cannot be separated from it.
11.10(e) #3	Are audit protocols available for review and copying by the FDA?	**S**	**Yes**. Audit protocols are available for review and copying.
11.10(f)	Are operational system checks used to enforce permitted sequencing of steps and events when necessary?	**S**	The system maintains standard chromatographic process with established steps sequences as follows: • Data collection. • Peaks identification. • Peak area calculation. • Quantitative determination of analyzed object composition. • Creating reports.
11.10(g) #1	Are authority checks in place 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 current operation?	**S**	**Yes**. The system maintains adjustable user privileges, which determine system access. User cannot gain access to data without a valid user ID and password.
11.10(g) #2	Does the system maintain records of IDs of operators who enter, alter, confirm, or delete data, including date and time?	**S**	**Yes**. ID of every operator who performs any actions in the system is being recorded in the audit trail.
11.10(h)	Are device checks used to determine, as appropriate, the validity of the	**S**	**Partly**. The system is developed for continuous providing computer work station with

	source of data or operational instruction?[1]		connection to instruments. Identification of some equipment components is not indicated as data source in electronic records.
11.10(i)	Is there a documented proof that the persons who develop, maintain, or use electronic records and signature systems have the education, training, and experience to perform their assigned tasks?	**U**	**Yes**. SDO Chromatec conducts training workshops on Chromatec Analytic data audit systems and issues confirmation certificates. User company initiates training for their employees.
11.10(j)	Have written policies that hold individuals accountable and responsible for actions initiated under their e-signatures in order to deter record and signature falsification been established and followed?	**U**	**No**. SDO Chromatec does not establish user responsibility for record and signature falsification.
11.10(k)	Are there adequate controls over system documentation, including the following: 1. Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. 2. Revision and alteration of control procedures to maintain an audit trail that documents time-sequenced development and modification of system's documentation.	**U**	**No**. User company bears responsibility for documentation maintenance.

[1] There are two equivalent interpretations of this requirement. The systems have to be developed to accomplish the following:

a) The right communication to be established between computer and entry data source (i.e. an instrument) before instructions transmission to the source or data transmission from the source.

b) Controlled data created by the system have to point unambiguously at data source (i.e. an instrument or component which created the data).

2.2 Requirements for Open Systems

If system access is **not controlled** by persons who bear responsibility for contents of electronic documents, the system is determined as "open system" and the following 21 CFR Part 11 requirements can be applied:

Section	Question / Requirement	Resp.	Implementation in Chromatec Analytic
11.30 #1	Are the procedures and controls used to protect the authenticity, integrity and confidentiality of the electronic records from their creation point to the point of their receipt?	**S**	**No**. These procedures are not applicable when Chromatec Analytic works in an open system.
11.30 #2	Are additional measures such as document coding and application of appropriate e-signature standards used to ensure the record authenticity, integrity and confidentiality?	**S**	**No**. These procedures are not applicable when Chromatec Analytic works in an open system.

2.3 Requirements for Digital Signatures

Section	Question / Requirement	Resp.	Implementation in Chromatec Analytic
11.50(a)	Do the signed electronic records contain information associated with the signing that clearly indicates the following noted below? (1) Full name of signer. (2) Data and time the signature was executed. (3) Meaning associated with the signature (e.g. verification, approval, responsibility, or authorship).	**SU**	**Partly**. The signed electronic records include the full name of the signer (as it was indicated when the record was being created), the date and time of signing. The signature meaning is not indicated.
11.50 (b)	Do the elements mentioned in the points (a)(1), (a) (2) and (a)(3) of this section belong to the same control elements as electronic records, and are they part of any human readable form of the electronic record (e.g. electronic variant of printed version)?	**S**	**Yes**. All supported signature elements are viewable.
11.70	Are all electronic and hand-written signatures linked to their respected electronic records to ensure that the signature cannot be excised, copied or otherwise transferred to falsify an electronic record by ordinary means?	**S**	**Yes**. Electronic signatures can be inserted into PDF reports.
11.100(a)	Is each electronic signature unique to one individual and not reused by, or reassigned to, anyone else?	**SU**	**Yes**. Each user has unique registration data, including a unique signature which cannot be reused by anyone else.
11.100(b)	Are the identities of the individuals verified prior to the establishment, assignment,	**U**	**No**. It is the user company's responsibility to verify and certify the

	certification, or any other authorization of an individual's electronic signature or any element of an electronic signature?		individual's identity.
11.200(a) #1	Do electronic signatures not based on biometrics employ at least two distinct identification components such as user ID and password?	**SU**	**Yes**. User account (user identifier) and password are required to create an electronic signature.
11.200(a) #1 (I)	When an individual executes a series of signings during a single, continuous period of controlled system access, is the first signing executed using all the electronic signature components?	**S**	**Yes**. User account (user identifier) and password are required to create an electronic signature.
11.200(a) #1 (I)	When an individual executes a series of signings during a single, continuous period of controlled system access, is each subsequent signing executed using at least one electronic signature component that is only executable by, and designed to be used by, the individual?	**S**	**Yes**. User account (user identifier) and password are required to create an electronic signature.
11.200(a) #1 (II)	When an individual executes a series of signings during a single, continuous period of controlled system access, is each signing executed using all the electronic signature components?	**S**	**Yes**. User account (user identifier) and password are required to create an electronic signature.
11.200(a) #2	Are controls in place to ensure that only their genuine owners can use the electronic signature not based on biometrics?	**S**	**Yes**. User account (user identifier) and password are required to create an electronic signature.
11.200(a) #3	Are the electronic signatures to be administered and executed to ensure that the attempted use of an individual"s electronic signature by anyone other than its genuine owner requires the collaboration of two or more individuals?	**SU**	**Yes**. Illegitimate use of electronic signatures by anyone other than their genuine owners requires purposeful collaboration between user and system administrator.
11.200(b)	Are electronic signatures based on biometrics designed to ensure that only their genuine owners can use them?	**S**	**No**. Chromatec Analytic does not maintain biometric verification of authenticity.
11.300(a)	Are controls in place to ensure the uniqueness of each combined identification code and password maintained, such that no two individuals have the same combination of identification code and password?	**SU**	**Yes**. Chromatec Analytic does not enable creating user accounts with the same identification data.
11.300(b)	Are controls in place to ensure that the identification code and password issuance is periodically checked, recalled, and revised (e.g. to compensate such events as password obsolescence)?	**SU**	**No**. Chromatec Analytic does not provide password expiration.