Rheolution
TEST SMARTER

21 CFR Part 11 Compliance Add-On for Soft Matter Analytics™

Specs and Features

The following table describes how the features and functionality of Soft Matter Analytics™ software with the CFR21 add-on enable laboratories to meet the regulatory requirements of 21 CFR Part 11.

	21 CFR PART 11	Soft Matter Analytics™ software application(s)
SUBPART B : ELECTRONIC RECORD		
11.10 Controls for closed systems		
11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	The operating company must validate the Soft Matter Analytics™ software as part of their electronic record system.
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.	All relevant measurement parameters and results can be exported as Microsoft® Excel® file format. The complete audit trail database can also be exported to a USB drive as an encrypted, password-protected archive that can be opened on another workstation for inspection. Before each export, the software verifies the integrity of the complete audit trail.
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Soft Matter Analytics™ protects electronic records maintained within the software and enables their accurate and ready retrieval by users with appropriate access privileges.

© Rheolution Inc. All rights reserved.

		User profiles may be deactivated without being deleted, preserving the attribution of existing records to their respective users. For retention beyond the period during which records are maintained within the software, records may be transferred to an external electronic archive. The operating company is responsible for ensuring the continued protection, availability, and retrievability of externally archived records throughout the applicable retention period.
11.10 (d)	Limiting system access to authorized individuals.	Prior to utilizing the system, each user must log in to gain access. Every user is assigned a specific role, which determines their access privileges.
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.	When the CFR21 add-on is licensed, the audit trail is automatically active and records applicable activities associated with electronic records, including changes to data, tests, and settings. Audit trail entries include the date and time of the action and are securely associated with the corresponding electronic record. For modifications, previously recorded information is preserved and both the previous and new values are available in the audit trail. Where applicable, users are required to provide a reason for change. Audit trail information is protected against unauthorized alteration and remains available throughout the applicable retention period. It can be reviewed within Soft Matter Analytics™ and exported for inspection. If a required audit trail entry cannot be recorded, the corresponding operation is cancelled and the user is informed, preventing applicable record changes from occurring without the associated audit trail entry.
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Not applicable.

© Rheolution Inc. All rights reserved.

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.	Each user is assigned a role that defines, screen by screen, which functions the user can access and at which permission level. The right to electronically sign records, and the signature meanings a user may apply, are also granted by role.
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.	Soft Matter Analytics™ software offers the flexibility to display input values in both text and graphical formats on the screen. Numerical data entry is validated upon input to ensure proper formatting. Additionally, Soft Matter Analytics™ features customizable choice inputs, allowing users to select values from predefined dropdown lists, thereby minimizing input errors. Access to the instrument is restricted to the configured devices exclusively. The system can identify instrument models and serial numbers, and communicates with paired instruments over a dedicated local wireless link established by the tablet.
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.	Rheolution service team undergoes training to install, service, and maintain Rheolution systems equipped with Soft Matter Analytics™ software. End-user training is the operating company's responsibility and should be integrated into the system's procedural compliance.
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.	Responsibility of the operating company.
11.10 (k)	1) Use of appropriate controls over systems documentation including:Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. 2) Use of appropriate controls over systems documentation including:Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	A release-specific software manual is distributed alongside the Rheolution's line of products and Soft Matter Analytics™. The development of Soft Matter Analytics™ software adheres to a design and change control process, ensuring the creation and tracking of relevant documents. Written procedures control the development, testing, and maintenance of Rheolution systems and software.

© Rheolution Inc. All rights reserved.

11.50 Signature manifestations

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.	Soft Matter Analytics™ offers electronic signatures on test results and reports. Each signature contains the full printed name of the signer, the date and time of signing (UTC with local offset) and the meaning selected by the signer from a predefined list, such as authorship, review or approval.
11.50 (b)	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	Signature information is securely maintained with the associated electronic record and is covered by the audit trail. It is displayed with the signed record and included in associated PDF and Excel® exports.

11.70 Signature/record linking

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.	Users authenticate using their unique username and password. Electronic signatures require both components for the first signing during a session. Subsequent signings within the same continuous, controlled session require at least the password. Following logout, session timeout, or application restart, both components must be provided again. Each electronic signature and failed signing attempt is recorded in the audit trail, ensuring traceability and accountability. The operating company is responsible for maintaining the confidentiality of user credentials and ensuring they are used exclusively by their assigned owners.

© Rheolution Inc. All rights reserved.

SUBPART C : ELECTRONIC SIGNATURES

11.100 General requirements

11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	The user management system ensures that all user IDs are unique, guaranteeing that all electronic signatures are also unique. It is the responsibility of the operating company to configure unique users.
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.	It is the responsibility of the operating company to configure and assign users.
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. 1) The certification shall be signed with a traditional handwritten signature and submitted in electronic or paper form. Information on where to submit the certification can be found on FDA's web page on Letters of Non-Repudiation Agreement. 2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	Responsibility of the operating company.

© Rheolution Inc. All rights reserved.

11.200 Electronic signature components and controls		
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.	Users authenticate using their unique username and password. The operating company is accountable for safeguarding that usernames and passwords remain confidential and exclusive to their rightful owners. Electronic signatures require both the user ID and the password for the first signing of a session; subsequent signings during the same continuous session require at least the password. After a logout, an inactivity lock or an application restart, both components are required again. Every signature and every failed signature attempt is recorded in the audit trail.
11.200 (b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Not applicable.

© Rheolution Inc. All rights reserved.

11.300 Controls for identification codes/passwords		
11.300 (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.	The system administrator ensures the assignment of unique user IDs. The software rejects any new account whose user ID matches an existing or deactivated account, so that no two individuals can ever share the same identification code.
11.300 (b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	The user management system supports password expiration, with criteria that can be individually configured by the system administrator. Users cannot reuse any of their most recent passwords when a password expires or is changed.
11.300 (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.	Soft Matter Analytics™ allows authorized administrators to issue a temporary password when a user's password is lost or otherwise compromised. Temporary passwords have a limited validity period and must be changed by the user upon first login. The operating company is responsible for establishing and maintaining appropriate procedures for managing lost or compromised credentials.
11.300 (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.	When the CFR21 feature is active, Soft Matter Analytics™ provides safeguards to detect and prevent unauthorized access attempts. User accounts are automatically locked after a configurable number of consecutive failed login or screen-unlock attempts. Failed access attempts, account lockouts, and subsequent administrative unlocks are recorded in the audit trail. Locked accounts can only be restored by an authorized system administrator. The operating company is responsible for configuring appropriate access controls and for establishing procedures to identify and respond to unauthorized access attempts.

© Rheolution Inc. All rights reserved.

11.300 (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.	Responsibility of the operating company.

Rheolution
TEST SMARTER

Contact us today to join the Data-Driven Science Community

Rheolution Inc.
7182 Saint-Urbain St
Montreal, QC, H2S 3H5
Canada

Rheolution Europe
36bis Montcalm St
Office A202
17 000 La Rochelle
France

US & Canada: +1 (800) 507-2811
Europe: +33 9 81 31 77 78
World: +1 (514) 270-2090
info@rheolution.com
www.rheolution.com