FDA 21 CFR Part 11 Compliance by Metrohm Raman

Norms and Standards

21 CFR Part 11 is the FDA rule relating to the use of electronic records and electronic signatures. Recognizing the increasing impact of electronic media on critical data in regulated environments, the FDA met with members of the pharmaceutical industry in the early 1990s. The pharmaceutical industry and the FDA were interested in how they could accommodate paperless record systems and ensure the reliability, trustworthiness, and integrity of electronic records.

Metrohm International Headquarters; Herisau, Switzerland

Metrohm Raman

The result was 21 CFR Part 11, which became effective on August 20, 1997. The criteria described herein apply to pharmaceutical companies conducting business in the U.S., suppliers to pharmaceutical companies, laboratories, and manufacturers of analytical instruments used by pharmaceutical companies.

As the producer of Mira P, a Raman analyzer specifically designed for ID and verification in pharmaceutical and other regulated industries, Metrohm Raman is acutely aware of standards set forth by 21 CFR Part 11. This document describes the requirements of 21 CFR Part 11 in terms of MiraCal P software compliance.

Overview, Definitions, and Clarifications

Government Norms & Standards can be confusing, to say the least. For that reason, this section will attempt to simplify certain points for the reader, in advance of a return to government jargon. Metrohm Raman's compliance with 21 CFR Part 11, broadly, involves data transmission and archiving by MiraCal P software. Specifically, we ensure the user's information fidelity when it comes to:

- Access control
- Data integrity and security
- Audit trails
- Electronic signatures
- Validation

The following definitions from 21 CFR Part 11 will be useful for the reader:

Electronic record – «any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.»

Electronic signature – «a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.»

Closed system – «an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.»

Digital signature – «an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.»

Metrohm has made every effort to interpret the meaning and intent of 21 CFR Part 11 regulations, drawing on the expertise of multiple sources. However, it must be understood that implementation of certain activities is the responsibility of the user; such as IQ/OQ, guiding policies on the part of a user's agency, and management of User ID's. We believe that, with diligence on the part of Mira P and MiraCal P users, the customer will be in full compliance.

First, a summary of items:
The software is compliant to the following 21 CFR Part 11 requirements:

- 11.10 (b), (d), (e), (f), (g), (h)
- 11.50,11.70
- 11.300 (a)

The software is compliant to the following 21 CFR Part 11 requirements with support of the operator:

- 11.10 (a), (c), (I), (j), (k)
- 11.100 (a), (b), 11.200 (a), 11.300 (b), (c), (d)

The guiding document is found at: **https://www.gpo.gov/fdsys/pkg/FR-1997-03-20/pdf/97-6833.pdf**

Requirement	Outline	MiraCal P Capability
§11.10(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records	• Standard methods for system validation (i.e. system suitability tests) are stored in the system. • The audit trail is stored internally and can be examined within the software. For library, training set, and operating procedure modifications, all former versions are saved in the database and are subject to version control.
§11.10(b)	The ability to generate accurate and complete copies of records in both paper and electronic form suitable for inspection, review, and copying.	• Reports can be printed out for results, operating procedures, samples, and the audit trail. All reports can be provided in PDF format. • All data can be stored as an encrypted file and can be reviewed and evaluated with Mira Cal software.
§11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	• The system stores data permanently in the encrypted Mira Cal software database. Copies can be made via the system backup function or on paper via regular print-out. • Data on the storage device is encrypted and provided with a checksum. Modifications are recognized by the system.
§11.10(d)	Limiting system access to authorized individuals.	• The system provides a login system with three internal access levels (System Administrator, Lab Manager and Instrument User). The administrator ensures that access rights are granted to authorized persons only.
§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. Audit trail documentation shall be retained and available for agency review.	• The audit trail documents all user entries and actions. Additionally, all modifications of security settings, user administration, or data configuration are recorded in the audit trail. • A new version is automatically created and saved upon record changes.

§11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	• Sequences are defined by design of the software, which guides the user through the steps.
§11.10(g)	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 other operations.	• Access to the computer and instrument for valid user accounts only – the administrator ensures that access rights are granted to authorized persons only. • Objects and determinations can be signed electronically, and the system demands that the reviewing and releasing person are different. • 3 user levels: routine, lab manager, administrator
§11.10(h)	The system controls validity of connected devices.	• Metrohm Mira instruments are recognized automatically (e.g. firmware version and serial number are confirmed). • Qualification of connected instruments is carried out as part of system validation.
§11.10(i)	Persons who develop, maintain, or use electronic record and signature systems have the education and experience to perform their assigned tasks.	• The operator is responsible for user training. • Metrohm offers standard training courses for all application fields. Our product developers and service personnel receive further training on regular intervals.
§11.10(j)	Written policies exist to hold individuals accountable for actions initiated under their electronic signatures, in order to deter record and signature falsification.	• The operator must have a policy in place, in which the equality of handwritten and electronic signatures is made clear.
§11.10(k)	Distribution of, access to, and use of systems operation and maintenance documentation is controlled. Formal change control procedures for system documentation maintain a time-sequenced audit trail for creation and modification.	• System documentation is unambiguously assigned to a particular system and software version. • Release notes exist for each software version, from which changes can be derived.
§11.30	Controls for open systems.	• Mira instruments and MiraCal software are closed systems

§11.50(a)	Signed electronic records must contain the following information: • Printed name of signer • Date and time of signing • Meaning of the signing (such as approval, review, responsibility or authorship.)	• All signatures contain the full name of the signer, date and time of the signature, and the meaning for signing.
§11.50(b)	Information specified in §11.50 (a) is shown on displayed and printed copies of the electronic record.	• User ID, date and time, and meaning of the signature is displayed on screen and on reports. The full name is also displayed in the audit trail and user management of Mira Cal software.
§11.70	Electronic and handwritten signatures shall be linked to respective electronic records to ensure that signatures cannot be excised, copied, or transferred to falsify an electronic record by ordinary means.	• Signatures are securely linked to the respective configuration or sample and cannot be cut, copied or transferred by ordinary means.
§11.100	Each electronic signature shall be unique to one individual and shall not be reused by or reassigned to anyone else. Before an individual's electronic signature is established, the organization shall verify the identity of the individual.	• Each user gets a unique user ID, and the system monitors the unambiguousness of the user ID. The identity of the respective person must be verified upon initial assignment of signing rights. • User accounts can be disabled, but not deleted- it must be operationally ensured that this user ID is not reassigned to another person.
§11.200(a)(1)	Electronic signatures that are not based upon biometrics shall employ at least two distinct ID component.	• The signing function is carried out with user ID and password.
§11.200(a)(1)(i)	During a single continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings require at least one electronic signature components.	• A password must be entered with each signature.
§11.200(a)(1)(ii)	If signings are not done in a continuous session, both components of the electronic signature are executed with each signing.	• The user ID and password must be entered with each signature.
§11.200(a)(2)	Electronic signatures not based upon biometrics shall be used only by their genuine owners.	• The operator ensures that a user uses his/her credentials only.

§11.200(a)(3)	Any attempt to falsify an electronic signature must require the collaboration of at least two individuals.	• Nobody has access to the electronic signature data by ordinary means.
§11.200(b)	Electronic signatures based on biometrics must be unusable by anyone other than their genuine owners.	• Metrohm Raman's electronic signatures are not based on biometric means.
§11.300	Persons who use electronic signatures based on ID codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: • maintaining the uniqueness of each combined ID code and password – ensuring that ID and password issuances are periodically checked, recalled, or revised. • procedures to electronically deauthorize potentially compromised ID codes or password information • transaction safeguards to prevent unauthorized use of passwords and/or ID codes and to detect and report any attempts at their unauthorized use	• The system ensures that each user ID is used only once. • It is recommended that ID codes and guidelines exist in which the creation of user accounts and the use of passwords (length, period of validity...) are specified by the operator for all systems across the whole organization. • The system supports the operator with a password expiration function – after the validity period, the user is forced to change his/her password. The system saves the password history and prevents the user from re-using the last 5 passwords. • In the event of potentially compromised ID codes or passwords, the corresponding user account can be disabled in the system by the administrator, but remains saved in the system without any access rights. • After incorrect attempts (defined by the administrator) the system indicates that the maximum number of unsuccessful login attempts has been reached and the user account is disabled. Any failed login attempt is recorded in the audit trail.

WP-038EN, published August, 2018