Luminex®
complexity simplified.

xMAP INTELLIFLEX® Compliance Matrix – 21 CFR Part 11

Technical Support
Telephone: 512-381-4397
North America Toll Free: 1-877-785-2323
International Toll Free: + 800-2939-4959
Email: *support@luminexcorp.com*
www.luminexcorp.com

RUO For Research Use Only.
Not for use in diagnostic procedures
89-30000-01-000
04/2023

Luminex Corporation
12212 Technology Blvd.
Austin, Texas 78727
U.S.A

Table of Contents

Introduction

The Regulatory Compliance Matrix is intended to describe how the xMAP INTELLIFLEX® system software enables the regulated company to comply with the Food and Drug Administration (FDA) Code of Federal Regulations (CFR) Title 21 Part 11, Electronic Records and Electronic Signatures.

The xMAP INTELLIFLEX® system equipment is designed to facilitate end user compliance with 21 CFR Part 11. Under the FDA Code of Federal Regulations (CFR), xMAP INTELLIFLEX equipment is designed to be used as a closed system. A closed system is controlled by a user responsible for the content of the electronic records generated on the system. In addition to the system technical controls, 21 CFR Part 11 requires that user facilities have established procedural and administrative controls. These include defined and documented policies and procedures, personnel training, and other controls.

Definitions

Understanding the following terms is essential for the successful implementation of the regulations. These definitions will be the starting point for xMAP INTELLIFLEX® software compliance with the regulation.

- **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.
- **Open system**—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.
- **Digital signature (DS)**—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.
- **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.
- **Application:** Software installed on a defined platform/hardware providing specific functionality.
- **IT Infrastructure:** The hardware and software such as networking software and operation systems, which makes it possible for the application to function.
- **Life cycle:** All phases in the life of the system from initial requirements until retirement including design, specification, programming, testing, installation, operation, and maintenance.
- **Regulated company:** A company that must demonstrate that its drug or biological product is safe and effective for the intended use, and that it can manufacture the product to federal quality standards.

Software Features

xMAP INTELLIFLEX® software adheres to FDA quality guidelines covering all aspects of system development. The following features are included in the xMAP INTELLIFLEX software to facilitate adherence to 21 CFR Part 11 regulations.

- **Audit Trail**

  The system automatically generates audit trail information, located in the system log and the XLS report. Changes to the configuration are logged. Once the audit log record is written, it cannot be modified by normal means. The audit log will include user comments for actions. Software provides human-readable and digitally signed reports of the results log. The system provides access to this audit trail information in the System Logs area, this information can also be exported to an Excel file for a specific individual date or a date range. The audit trail provides the read-only log of data file creation and modification activities.

- **Curated Workflow**

  When successive operations, events, and/or data entry are required, the system may be configured to ensure the steps are followed in the correct sequence and logs each step in the Audit Trail. The software can be configured to require electronic signatures to perform specific actions. Input data is validated when appropriate.

- **Detailed Reports**

  Reports and output files are available in human-readable CSV, and XLS format. Raw, per-well fluorescence data is not exported and is not available in human-readable format as this data is not considered a required portion of the result output. Acquisition data may be manually or automatically exported from the instrument as human-readable CSV files. XLS files contains both acquisition data and configuration/logging data associated with the acquisition. The xMAP INTELLIFLEX system allows the creation of a report of the system's calibration, verification, and fluidics history, system log report, and plate configuration. Each report is a multi-page XLS file with summary and detail pages, and includes lot numbers, timestamps, and run information. In addition to providing summary and detail result information Luminex® technical support uses this information to aid in troubleshooting failures; this information can also be helpful for your internal Quality Control (QC) purposes.

- **Digital Signatures**

  Files exported in Excel format are digitally signed using the Excel digital signature process that can be used to verify the content of the file has not changed since export. Files exported in the xMAP INTELLIFLEX CSV format can be configured to include a proprietary digital signature that can be used to verify the content of the file has not changed since export.

- **Electronic Signature**

  The system logs separate computer system sign in events and application events which require an electronic signature . Electronic signatures are attached to the relevant records. The electronic signature includes:

  - Username of the signer
  - Computer generated date and time
  - User comment (default comments are provided)

  Electronic signatures are user configurable and can be applied for the following actions:

Maintenance:

- Running a Calibration, Verification or Fluidics Verification
- Importing/Saving a Calibration or Verification Kit

Results:

- Exporting Result Data
- Changing the Column Formatting of the xMAP INTELLIFLEX format
- Archiving Result Data
- Running a Plate
- Ignoring Laser Warm-up when Running a Plate
- Running Without Valid Calibration/Verification
- Running a Plate with Reacquired Wells
- Editing a Plate

Saving/Deleting Configuration Items:

- Saving/Deleting a Protocol
- Saving/Deleting a Panel
- Saving/Deleting Acquisition Settings
- Saving/Deleting a Plate Layout
- Saving/Deleting a Plate

Admin Settings

- Changing Administrator Settings

- **Secure Record Retention**

  The user may encrypt the hard drive using BitLocker. Data acquired on the instrument is retained in various formats:

  - Secured SQL Server Database
  - Raw fluorescence data is stored on the file system as FCS compatible files.
  - Acquisition data may be manually or automatically exported from the instrument as human-readable CSV files and XLS files. XLS files contain both acquisition data and configuration/logging data associated with the acquisition.

  Records are retained until an authorized user explicitly removes them through a process that exports them to an external device.

- **Secure Login**

  Windows users accounts are used to control access and prohibit access by unauthorized users. The administrator via User Management can set the attempt threshold, define a lockout period, and manually unlock the account. Unsuccessful sign in attempts are recorded in the system log. There are two (2) components required for access and are always required for user account access:

  - User account
  - Password

The xMAP INTELLIFLEX system supports the requirement to input user account and password required on startup. The system defines user access by assigning roles. The administrator does not have the ability to customize what each role has access to. The different roles are:

- Administrator
- Lab Lead
- Operator
- Field Technician

For unattended devices, the administrator can set the inactivity log-out/time-out. The user will have to sign in to re-access the application.

- **User Management**

Secure Login and User Management for the xMAP INTELLIFLEX System support multiple user accounts that can be set up locally on the system or a network. The xMAP INTELLIFLEX user permissions are managed in four pre-defined Windows groups:

- Administrators: grants Administrator-level access to both Windows and the xMAP INTELLIFLEX Software interface.
- Luminex Lab Leads: grants Lab Lead-level access to the xMAP INTELLIFLEX Software interface.
- Users: grants Operator-level access to the xMAP INTELLIFLEX Software interface.
- Luminex Field Technicians: grants User-level access to Windows and access to the Service sections of the xMAP INTELLIFLEX interface software.
- The administrator has the ability to disable and add accounts.

21 CFR Part 11 Compliance Statements

The software application uses the following to facilitate 21 CFR Part 11 Compliance.

§11.10 Controls for closed systems

a) *Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.*

The system inhibits unauthorized personnel from altering records held in the instrument by including the verification status of the system at the time of the sample reading. All updates to records are maintained in the system's **Audit Trail**. Data exports can be secured with a **Digital Signatures** that can be used to verify data has not been altered after it has left the instrument.

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 records are maintained in a Secure Record Retention repository in the system. Users are able to export these records in a variety of Detailed Reports. These reports export records including Electronic Signature information suitable for review and inspection. The reports are protected by Digital Signatures verifying the integrity of the data.

c) *Protection of records to enable their accurate and ready retrieval throughout the records retention period.*

Records are maintained as part of a Secure Record Retention repository on the system. These records may be exported from the system in a variety of Detailed Reports that can be verified with Digital Signatures. The user may use these records to meet their own retention procedure and is responsible for configuring record retention procedure.

d) *Limiting system access to authorized individuals.*

The system is protected with a **Secure Login**. The system's **User Management** enables administrators to give users varying access to features based on their authorization level.

e) *Use of secure, computer-generated, time-stamped audit trails to independently record the date and time or 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*

The system maintains a comprehensive **Audit Trail**. The Audit Trail can be exported as part of **Detailed Reports**. Even after export, the integrity is protected with **Digital Signatures**.

f) *Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.*

The system maintains **Curated Workflow** and validates all configuration entries.

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.*

The system is protected with individual Secure Login. Administrators configure authorization and Electronic Signature access via a User Management console.

h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

A Curated Workflow validates input data. User Management enables administrators to authorize appropriate personnel for plate configuration. Digital Signatures validate the source instrument of all exported reports.

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.

User Management and Secure Login enables administrators to limit who may access the instrument and apply electronic signatures. This enables administrators to only give this authorization to only those who have been properly trained by the end user.

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.

NOTE: The regulated company is responsible for establishing a policy/process to ensure accountability, responsibility, and to deter individuals from falsifying records and signatures.

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.

NOTE: Luminex provides version-controlled user documentation for operation and maintenance of the INTELLIFLEX system. The regulated company is responsible for establishing appropriate controls within their document control system.

§11.30 Controls for open systems

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

The system is a closed system.

§11.50 Signature Manifestations

a) *Signed electronic records shall contain information associated with the signing that clearly indicates all the following:*

   1) *The printed name of the signer.*

   2) *The date and time when the signature was executed.*

   3) *The meaning (such as review, approval, responsibility, or authorship) associated with the signature.*

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)*

The xMAP INTELLIFLEX system's **Electronic Signature** includes all regulation required information.

§11.70 Signature/record linking

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.

Electronic Signatures are maintained in the Secure Record Retention repository where access is not allowed. The Detailed Reports within which the Electronic Signatures are exported are protected with a Digital Signatures that will verify the report data has not been modified.

Subpart C - Electronic Signatures

§11.100 General requirements.

a) *Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.*

The combination of **Secure Login & User Management** enables administrators to facilitate individual, unshared and genuine **Electronic Signatures**.

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.*

NOTE: The organization is responsible to verify the identity of the individual.

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 submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.*

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.*

NOTE: The regulated company is responsible for certifying 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.

§11.200 Electronic signature components and controls.

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.*

Electronic Signatures requires both a user account and password to be verified. Subsequent **Electronic Signatures** in a single session still requires both user account and password, but the user account is prepopulated in the dialog.

2) *Be used only by their genuine owners; and*

The combination of **Secure Logins** & **User Management** enables administrators to facilitate individual, unshared and genuine **Electronic Signature**s.

NOTE: It is the responsibility of the regulated company to establish a policy to prevent sharing of user accounts.

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.*

NOTE: It is the responsibility for the regulated company to establish a policy to address collaboration of two or more individuals when there is an attempted use of an individual's electronic signature by anyone but the owner.

b) *Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.*

NOTE: xMAP INTELLIFEX does not support biometrics.

§11.300 Controls for identification codes/passwords

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.*

The combination of **Secure Logins** & **User Management** enables administrators to require individual, unshared and genuine **Electronic Signatures**.

b) *Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).*

Secure Logins & **User Management** enables administrators to define a lockout period, set password complexity and require password changes.

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.*

Secure Logins & **User Management** enables administrators to disable existing user accounts.

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.*

System and technical logs record all failed login and **Electronic Signatures** attempts.

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.*

NOTE: INTELLIFLEX does not incorporate any such devices defined by 21 CFR Part 11 11.300 (e).