Dotmatics
FCS Express

Compliance Summary 21 CFR Part 11

FCS Express offers you the most complete set of 21 CFR Part 11 compliance tools to meet the needs of your regulated life-science flow cytometry laboratory including security, access limitations, authority checks, record protection, audit trails, electronic signatures, and much more. The table below outlines requirements for Part 11 and FCS Express compliance strategies.

Code of Federal Regulations Title 21 - Subpart B – Electronic Records

Section 11.10 – Controls for Closed Systems

FCS Express is designed to be run as a closed system. Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

Requirement and sub-sections	Strategy	Compliance
11.10(a) - Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	De Novo Software has validated FCS Express. Additional validation plans for your laboratory may be developed by your institution.	✓
1.10(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.	FCS Express stores its layout files and results in a format that is both human readable and machine readable.	✓
11.10(c) - Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Records are saved in an encrypted and locked format, with checksum measures in place to detect tampering. De Novo Software advises that you save your FCS Express files in a secure folder.	✓
11.10(d) - Limiting system access to authorized individuals.	FCS Express contains security features that limit access to authorized individuals.	✓
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.	Audit trails are secure and time stamped. They record the date and time of actions that modify any aspect of your analysis, along with the name of the person who made the change.	✓
11.10(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	This does not apply to FCS Express.	N/A
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.	User credentials are required to access FCS Express. FCS Express also features a comprehensive set of permissions that can limit access on a individual user basis.	✓

Section 11.10 – Controls for Closed Systems (continued)

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.	FCS Express applies checks to determine if it has received a valid flow cytometry file.	✓
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.	De Novo Software can assist your laboratory with preparation of a training plan so that your scientists understand how to use FCS Express as well as the implications of Part 11 on their work.	Through laboratory procedures
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.	The institution must create their own policy.	Through laboratory procedures
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.	De Novo Software follows change control and life cycle management procedures for document control.	✓

Section 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 a signature was executed, (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	FCS Express offers a comprehensive set of electronic signature features that will include, but not limited to: 1. The name of the Signer/Unsigner, 2. The date, time and the time zone in which the document was Signed or Unsigned, 3. The signature meaning or status.	✓
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).	FCS Express offers a convenient table display of the electronic signatures being used in a document that can be included in readable form in any printout or electronic display.	✓

Section 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.	Electronics signatures in FCS Express are unique to users. Any change in the history of an electronic signature is captured within the audit trail.	✓

Code of Federal Regulations Title 21 - Subpart C – Electronic Signatures

Section 11.100 – General Requirements

Requirement	Strategy	Compliance
11.100(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	FCS Express ensures that all user IDs are unique; therefore, all electronic signatures are unique	✓
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.	The institution must verify the identity of their FCS Express users.	Through laboratory procedures
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.	You must certify with the FDA that you intend to use electronic signatures.	Through laboratory procedures

Section 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.	FCS Express ensures that all user IDs are unique; therefore, all electronic signatures are unique. FCS Express requires entry of username and password to sign layout files and results. To gain access to FCS Express and to sign a layout file or result, users must have a valid username and password.	✓
11.200(a) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	FCS Express does not use biometrics. When LDAP integration is enabled for FCS Express, Active Directory may be used to support controls.	N/A

An FCS Express icon in the compliance column indicates compliance achievable within FCS Express via security and logging add-ons.

Section 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:

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.	In order to maintain the uniqueness of each individual, FCS Express does not allow duplicate login names. Also, LDAP integration is available for FCS Express.	✓
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).	FCS Express has a comprehensive set of password criteria.	✓
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.	Accomplished through laboratory, administrative, and information technology procedures using security tools in FCS Express. When LDAP integration is enabled for FCS Express, Active Directory may be used to support controls.	✓
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.	FCS Express disables accounts after a configurable number of failed login attempts.	✓
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.	This does not apply to FCS Express.	N/A

FCS Express with CFR Part 11 Compliance features is designed to maintain both the machine-readable metadata and human-readable reports, FCS has the following features to enhance your Part 11 compliance program:

- **Security, Access Limitations, and Authority Checks** allow you to control which functions people are allowed to perform on a user-based and layout-based level. Over 300 independent security permissions can be set for each user security group, giving you tremendous flexibility in defining your own access limitations.
- **Audit Trails**: FCS Express employs secure, computer-generated, time-stamped audit trails to track actions that create, modify, or delete FCS Express layout files and reports.
- **Electronic Signatures**: When users are satisfied with their flow cytometry report, they can electronically sign it. Signing events are maintained in the audit trail. Signed reports can be securely transferred in a variety of formats to your laboratory information management system. Signing order may be enforced with FCS Express.
- **Record Protection** prevents unauthorized manipulation of FCS Express metadata and reports. Flow cytometry raw data can also be stored with metadata and reports, facilitating protection and traceability.
- **Much, much more**: sophisticated encryption, system level audit trails, print logging, print tagging, password aging and many other features serve to help you ensure that your flow cytometry analysis can meet compliance with Part 11 regulations.

Learn more at denovosoftware.com/cfrpart11

Contact us at support@denovosoftware.com to arrange for a free trial with security and logging enabled.