WHITEPAPER

BECKMAN COULTER
Life Sciences

CytoFLEX Flow Cytometers with CytExpert 2.3 Software

Support for Compliance with 21 CFR Part 11

Introduction

21 CFR Part 11 refers to the section in the Code of Federal Regulations (CFR) that sets forth the United States Food and Drug Administration's (FDA) guidelines on using electronic records and electronic signatures. Chapter 21 covers all regulations pertaining to GCP (Good Clinical Practice), GLP (Good Laboratory Practice) and GMP (Good Manufacturing Practice), relating to the pharmaceutical and healthcare industries. Part 11 covers all FDA regulated issues pertaining to electronic records and electronic signatures.

All computer systems that store data used to make Quality decisions or data that will be reported to the FDA must be compliant with 21 CFR Part 11. The purpose of the law is to define the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records.

The regulation requires organizations to have in place three levels of control: administrative controls such as policies for electronic records, procedural controls such as SOPs for using the system, and technical controls for the functions built into software that ensure the reliability and integrity of electronic records and signatures. Software can be designed to facilitate compliance with 21 CFR Part 11 technical controls, but it is the user who is responsible for providing policies and procedures to ensure their policies and procedures are fully compliant with the regulations.

CytExpert 2.3 has features that were designed to facilitate user compliance with 21 CFR Part 11, when installed using the Electronic Record Management option. The table below references specific sections of the regulation and indicates how CytExpert 2.3 facilitates compliance with that section.

Compliance Support Notes

Section	Requirement	CytoFLEX with CytExpert 2.3 software with Electronic Records Management mode installed
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.	An instrument IQ/OQ procedure is available to validate the instrument performs to specifications upon installation. Instrument QC confirms the instrument is working properly within the specified parameters. Quality control determines whether the instrument can provide signal strength and precision to meet performance specifications. A software IQ/OQ procedure is available for the Electronic Records Management installation mode which may be used to validate the software performs to specifications. The system can discern tampering of records that are entered in the audit log and indexed database.
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.	Data from multiple samples may be displayed in a report. Report may be printed to PDF or paper. Header displays experiment name and path within the closed system. Footer displays username, full name, unambiguous date and time including UTC offset and comment associated with the signature. Experiment Operation Log includes Print in the audit trail.

Section	Requirement	CytoFLEX with CytExpert 2.3 software with Electronic Records Management mode installed
11.10	**Controls for closed systems (continued)**	
11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Retention period may be configured for each experiment or a batch of experiments. Retention period may be from 0 to 99,999 days. Experiment name is disguised in the Windows directory. Folder containing FCS files is disguised in the Windows directory. FCS file name is disguised in the Windows directory. Checksum is generated for experiment files. Checksum is generated for FCS files. Data integrity is verified for FCS files.
11.10(d)	Limiting system access to authorized individuals.	Users are authorized within the User Manager. Each User is assigned to a Role. Roles and Permissions are assigned within the Role Manager. Only active users may access the software via a valid User ID and Password.
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.	There are three logs which facilitate audit trails for a wide range of operations. The Experiment Operation Log tracks all operations applied to an Experiment (.xit file). The System Operation Log tracks all operations applied to the system. The User Management Operation Log tracks all operations within the User and Role Managers. Information displayed in each log inlcudes the Operation, Username, User Full Name,Timestamp and Record of the operation being recorded.
11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Operational system checks are built into the Role Manager via Permissions and Signature Settings. A retention period is assigned to an experiment or batch of experiments. Specific operations related to instrument control and data processing are controlled by assignment to a Role. Each User has a Role assigned that is appropriate for the requirements of the system as defined by the Administrator. A signature hierarchy is defined by the Administrator which enforces the sequence of approval or rejection of an experiment. A completed sequence of signatures validates an experiment. Validated experiments can not be modified or deleted within the Retention Period.
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.	Authority checks are built into the Role Manager via Permissions and Signature Settings. A signature hierarchy is defined by the Administrator which enforces the sequence of approval or rejection of an experiment. A completed sequence of signatures validates an experiment. Validated experiments can not be modified or deleted within the Retention Period.
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.	A checksum is generated for FCS files to facilitate detection of data tampering. The Administrator controls Permissions related to Signatures, File Management and Instrument Operation.
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.	User training is offered by Beckman Coulter. Users who take the training and pass the exam receive verified completion certificates. Laboratory policies and procedures should also be generated to assure users are trained properly.

Section	Requirement	CytoFLEX with CytExpert 2.3 software with Electronic Records Management mode installed
11.10	**Controls for closed systems (continued)**	
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 Administrator configures the Account Policies within the system. These Account Policies address Passwords, Application Inactivity and Account Lockout. Laboratory procedures should be in place to enforce the integrity of system.
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.	System documentation is controlled via ISO compliant ECO (Engineering Change Order) process.
11.3	**Controls for Open Systems**	
11.30	Controls for Open Systems	N/A The system, CytoFLEX with CytExpert 2.0 software with Electronic Record Management mode, applies to closed systems.
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.	Signatures are composed of all required components, including the username and the full name of the signer, unambiguous timestamp, and a comments included with the signature explaing the purpose of the signature.
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 appears in the footer of each page produced as a report for the experiment. All components of the signature and all signatures are included in the signature.
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.	Signatures including approvals and rejection are captured in the Experiment Operation Log. Once all Signatures in the hierarchy are executed within an Experiment, the Experiment may no longer be modified. Deletion of an Experiment or FCS file is controlled using permissions and a Retention period.
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 ID is unique to each User of the system.
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 Administrator controls access to the system via the User Manager and the Role Manager.

Section	Requirement	CytoFLEX with CytExpert 2.3 software with Electronic Records Management mode installed
11.100	**General Requirements (continued)**	
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 submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 12420 Parklawn Drive, RM 3007 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.	Lab procedures enforce responsibility and accountability for the use of the electronic signatures in the system.
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.	Signatures are composed of the User ID and password. The first instance of the signature within a session requires the User ID and password. Subsequent signatures within the session require entry of the password.
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.	N/A

Section	Requirement	CytoFLEX with CytExpert 2.3 software with Electronic Records Management mode installed
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 User ID is unique to each User of the system. Duplication of User ID is not supported.
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 Password Policy includes configuration of the expiration, complexity and minimum length, and password history to suppress repeating a password within a comfigurable number of previous passwords.
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.	Users may be inactivated or locked out of the system by the Administrator.
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.	The Account Lock Policy controls the number of allowable invalid login attempts before lockout. The lockout duration is also configurable.
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.	Qualification of the performance of the system may be tested periodically by the laboratory personnel or by Beckman Coulter using the CytoFLEX IQ/OQ Service.

BECKMAN COULTER
Life Sciences

For research use only. Not for use in diagnostic procedures.

For Beckman Coulter's worldwide office locations and phone numbers, please visit "Contact Us" at beckman.com