BD FACSuite™ and BD FACSuite™ Clinical Application

U.S. FDA 21 CFR Part 11 (Electronic Records; Electronic Signatures) Support

BD FACSuite™ and BD FACSuite™ Clinical Application have many functions and options relevant to 21 CFR Part 11. The following table refers to both BD FACSuite™ and BD FACSuite™ Clinical Application.

11.10 Controls for Closed Systems

Section		Rule Summary	BD FACSuite™ and BD FACSuite™ Clinical Application
11.10(a)	Validation to ensure accurate, reliable and intended performance, and the ability to discern altered/invalid records	System validation	BD FACSuite™ Application goes through validation and verification testing by BD. The validity of the exported date is ensured by checksum and the database and audit log cannot be tampered with. IQ and OQ procedures are available for the BD FACSLyric™ System and an OQ is available specifically for software features related to 21 CFR Part 11.
11.10(b)	Generate valid copies in human-readable and electronic records suitable for inspection	Record generation for inspection	The software provides both electronic and human-readable formats (for example, reports, audit trails, user logs). A sample report is available as a PDF with a configurable header and footer in the BD FACSuite™ Application. A predefined report in the BD FACSuite™ Clinical Application tracks all necessary characteristics of the sample. Up to three electronic signatures, with comments, can be included in the report. A usage tracking log and audit log is also available as a PDF.
11.10(c)	Protect records, enabling their accurate retrieval	Record protection	The software stores operational files, data files and result information in an encrypted format within a hidden folder structure controlled by an indexing database. All records are retained until the user decides to delete records. Database backup and restore capabilities are available for the system. The validity of any exported data is ensured by checksum. Recorded FCS file names are disguised in the Windows™ operating system. All metadata is maintained in the database and is not available through the Windows file system.
11.10(d)	Limit system access to authorized individuals	System access limitation	The software requires all users to log in. Each user will have a defined role, including access privileges. Users are authorized within the User Management function. Roles and Permissions are assigned within User Management. Only active users may access the software via a valid User ID and Password. Access to User Management is restricted to the Administrator role. The system allows the Administrator to restrict access to certain features.
11.10(e)	Use audit trails to record date, time, operator, actions (for example, create, modify); changes shall not obscure previous information	Audit trails	Audit trails are automatically enabled for all entries in all worklists. For each worklist entry, the software will automatically track the lifecycle through audit trails including reason for change. The usage tracking log tracks the timestamp of each login and logout. The software records actions related to password management, worklist acquisition and other functions.
11.10(f)	Use of operational checks to enforce permitted steps and events	Operational checks	The software restricts what users can do based on their role and access privileges (Administrator and Operator). Each user can only perform operations as permitted by their role assigned by the Administrator. An Administrator can restrict Operators from performing operations. A hierarchy of up to three signatures can be defined by the Administrator for each test.
11.10(g)	Use of authority checks to ensure system use, record signature, operation of computer system or alter record	Authority checks	The software provides the users with the authority to carry out particular functions based on their roles and access privileges. For example, an Administrator (highest access privilege) is able to restrict an Operator (lower access privilege) from deleting data. For each test, a hierarchy of up to three signatures can also be defined by the Administrator. The software also has a tracking log to enable users to monitor system use. The validity of the exported data is ensured by checksum.
11.10(h)	Check to determine validity of data input or operation	Data/operation validity checks	The software informs a user who attempts to put invalid information into a software field based on the design specifications and limitation of each input field. The software also prevents accidental or malicious alteration of the data in an exported file by attaching a checksum value to the file when it is exported. Before it can be imported, the software checks the value and prevents the import if the value has changed.
11.10(i)	Persons using electronic records/ electronic signatures has proper training	User training	BD provides software and BD FACSLyric™ System user training with certification. The user's organization is responsible for training on the Electronic Record/Electronic Signature SOP. An electronic reference system is available for detailed instructions on how to use the software.

Section		Rule Summary	BD FACSuite™ and BD FACSuite™ Clinical Application
11.10(j)	Written policies holding individuals accountable for actions	User accountability	Written policies holding individuals accountable for actions is the responsibility of the user's organization. However, password expiration time and number of unsuccessful login attempts can be configured by an Administrator according to lab standard operating procedures. In addition, password length, complexity and restrictions on reuse of passwords is implemented by the system.
11.10(k)	Controls over distribution and use of documentation of system and its maintenance. Also revision and change controls to maintain an audit trail that documents time-sequenced development and modification of systems documentation	System documentation control	BD adheres to a change control process for documentation creation and revisions as dictated by the BD internal quality system.

11.50 Signature Manifestations

11.50(a)	Signed records to contain printed name of signer, date and time of signature, and meaning of signature (e.g., review, approval)	Signature manifestations	The software enables printing of e-signatures and comments on all reports as specified by the user/administrator. Reports include whether results pass/fail, have been reviewed or have been approved. All electronic records within the software are time, date and author stamped. Stamps cannot be changed on the final report.
11.50(b)	Same controls as for electronic records		

11.70 Signature/Record Linking

	Signature to be linked to record to ensure signature cannot be excised, copied or altered	Signature/record linking	The software provides e-signatures to link records with user signatures and a hierarchy of up to three signatures can be defined by the Administrator. Any modification of the record will automatically remove the e-signature and the user will be required to re-sign the report. Password expiration time and number of unsuccessful login attempts can be configured by an Administrator according to lab standard operating procedures. In addition, password length, complexity and restrictions on reuse of passwords is implemented by the system.

11.100 Electronic Signatures

11.100(a)	Each signature is unique to one person and shall not be reused or reassigned.	General e-signature requirements	The software provides a unique name and password.
11.100(b)	Before organization establishes an electronic signature, it shall verify the identity of the individual.	General e-signature requirements	Verifying the identity of an individual is the responsibility of the user's organization. The Administrator controls user ID's roles and permissions. Responsibility of the user's organization.
11.100(c)	Certify electronic signatures are equivalent to handwritten signatures and submit to FDA.	General e-signature requirements	Responsibility of the user's organization.

11.200 Electronic Signature Components and Controls

11.200(a)	Electronic signatures shall employ two distinct IDs (ID and Password), after first signing; subsequent signings only require a single ID during a continuous session.	Controls for e-signature	A software e-signature consists of a unique username and password. The software requires both components at each signing.
11.200(b)	Electronic signatures using biometrics ensure they cannot be used by anyone else.	Controls for e-signature	Not applicable.

11.300 Controls for Identification Codes/Passwords

11.300(a)	Maintain uniqueness of combined ID and Password for each individual	Uniqueness of ID/password	The software provides a unique name and password and duplicated user ID's are not supported.
11.300(b)	Ensure ID and Password are periodically checked, recalled or revised	Password aging	The software enables the administrator to set a password expiration date and duplicated user ID's are not supported.
11.300(c)	Deauthorize lost or missing ID and Password and issue new temporary/permanent replacement following all previous controls	Lost ID/password management	The software enables the administrator to manage user profiles, including user IDs and passwords. Password expiration time and number of unsuccessful login attempts can be configured by an Administrator according to lab standard operating procedures. Password length, complexity and restrictions on reuse of passwords is implemented by the system.
11.300(d)	Safeguards to prevent unauthorized use and report any attempts of unauthorized attempted use	Prevention of unauthorized use of system	The administrator can configure the software to lock an account after a number of failed login attempts. The operating system of BD FACSuite™ Application will lock the screen after a period of inactivity.
11.300(e)	Periodic testing of the generation of ID and Password procedure/device to ensure proper operation	Periodic testing of ID/password generation	Responsibility of the user's organization.

The BD FACSLyric™ Flow Cytometer is a Class 1 Laser Product.

BD - Europe, Terre Bonne Park – A4, Route de Crassier 17, 1262 Eysins, Switzerland

CE

bdbiosciences.com