BD FACSuite™ and BD FACSuite™ Clinical Software

US FDA 21 CFR Part 11 (Electronic Records; Electronic Signatures) Support

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

11.10 Controls for closed systems

Section		Rule Summary	BD FACSuite and BD FACSuite Clinical Software
11.10(a)	Validation to ensure accurate, reliable, and intended performance, and the ability to discern altered/invalid records	System validation	The BD FACSuite software goes through an extensive validation process by BD. IQ and OQ procedures are available for the BD FACSLyric™ system.
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).
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.
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.
11.10(e)	Use audit trails to record date, time, operator, actions (for example, create, modify); changes shall not obscure previous information	Audit trails	The software provides the option to turn on audit trails for Worklist entries. Once turned on, audit trails cannot be turned off. For each worklist entry, the software will automatically track the lifecycle through audit trails including reason for change.
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).
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. The software also has a tracking log to enable users to monitor system use.
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.
11.10(j)	Written policies holding individuals accountable for actions	User accountability	Responsibility of the user's organization.
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.

Visit **bdbiosciences.com** for more information.

BD

11.50 Signature Manifestations

Section		Rule Summary	BD FACSuite and BD FACSuite Clinical Software
11.50(a)	Signed records to contain printed name of signer, date and time of signature, and meaning of signature (eg, 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 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. Any modification of the record will automatically remove the e-signature.

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	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.
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.
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.
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 FACSuite 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.

BD FACSuite software is For Research Use Only.
BD FACSuite Clinical software is for In Vitro Diagnostic Use.
23-19923-01

BD Life Sciences, San Jose, CA, 95131, USA

bdbiosciences.com