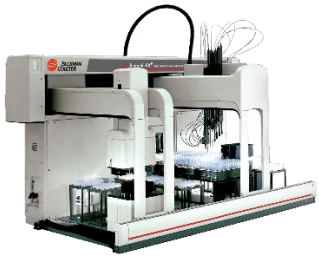
Beckman Coulter's Biomek Liquid Handlers Provide Support for 21 CFR 11 Compliant Laboratories

Introduction

This document summarizes how Beckman Coulter software running on Biomek liquid handlers supports compliance with 21 CFR Part 11. Beckman Coulter software includes:

- Beckman Coulter Accounts & Permissions (BCAP) software is an integrated set of features used by compatible software applications, including Biomek Software and SAMI, to assist users in complying with electronic signature requirements, such as 21 CFR Part 11, for closed systems.
- Biomek Software controls the liquid handler and works in conjunction with BCAP.
- SAMI software is used in larger, integrated systems to control multiple Biomek instruments and devices. SAMI also works in conjunction with BCAP to control access to the instrument.

All Beckman Coulter software is developed under ISO 9001 certified processes that include verification of the intended use. Additionally, BCAP, Biomek Software, and SAMI have features that enable labs to implement 21 CFR Part 11 compliance.

Note: Achieving full compliance with 21 CFR Part 11 requires enabling accounts and permissions features in software and implementing site and user processes beyond the control of Beckman Coulter software.

21 CFR 11 Subpart A — General Provisions

The following definitions from 21 CFR 11 are related to the discussion of Beckman Coulter software. Please note that Biomek instruments are closed systems.

Sec. 11.3 Definitions

(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(6) Electronic record means 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.

(7) Electronic signature means 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.

(9) Open system means 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.

Subpart B—Electronic Records		
Part	**Description**	**Comments**
11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Beckman Coulter software is developed following an ISO 9001 certified development process that involves defining product requirements and testing to validate that those requirements are met. Beckman Coulter software records cannot be modified or deleted by the Administrator or Users. The software generates an operation log that cannot be modified by Administrators or Users.
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. 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.	Beckman Coulter software generates and stores records in both human readable and electronic form suitable for inspection and review. Electronic records can be printed or exported as text files.
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Records are stored in a protected area of the system. Records may not be altered or deleted by Administrators or Users.
11.10 (d)	Limiting system access to authorized individuals.	Beckman Coulter software limits system access to authorized individuals. Administrators create accounts for individual Users and define a set of permissions for each user. Users cannot change their own permissions; only Administrators can perform this function.

Part	Description	Comments
		If a Biomek instrument is inactive for a length of time, the User is automatically logged out. This time interval is defined by the Administrator. The Administrator can force Users to change their password after a defined number of days. The Administrator can also prevent Users from re-using old passwords.
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.	Beckman Coulter software generates a time-stamped audit trail that lists the date, time, and name of the user or Administrator that performs a task. Beckman Coulter software does not enable the modification or permanent deletion of electronic records, including the audit trail. The audit trail can be exported as a text file for review.
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Beckman Coulter software is designed to require Users to login before executing a permitted sequence of steps.
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.	Each User is required to login to the system using the account created for that user by the Administrator. Users must supply the correct username and password to gain access to the system. Users may not change their own permissions; only an Administrator may perform this function. Beckman Coulter software does not enable records to be altered.
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.	Administrators define which User accounts have permission to validate operational instructions (for instance a method), and which User accounts have permission to run validated methods. Users with permission to validate methods may also electronically sign those methods, for instance to indicate approval of the method. Electronic signatures appear in the audit trail when the method is run.

Part	Description	Comments
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.	Beckman Coulter ensures and documents the qualification of the staff who create and maintain Beckman Coulter products. Regulation refers additionally to the responsibility of the User and should be maintained using proper protocols and documentation.
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.	Regulation refers to the responsibility of the User and should be maintained using proper protocols and documentation.
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.	Documentation is installed on the Biomek instrument by authorized Beckman Coulter Field Service Engineers and Field Applications Specialists. Updated versions of documentation are available at www.beckmancoulter.com Beckman Coulter software has built-in Help that is validated as part of ISO 9001 certified development process and cannot be altered by users. Beckman Coulter uses an ISO 9001 certified change management process to update and release system documentation. Instructions for use of the account management system (BCAP) are contained in the online help for that system and can only be accessed by users with access to BCAP.
11.30	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	Beckman Coulter software and Biomek instruments are closed systems. If the User operates Beckman Coulter software and the Biomek instrument as an open system, the User is responsible for using proper protocols and documentation.

Part	Description	Comments
	ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	
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. (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).	Beckman Coulter software enables the electronic signature of electronic records, e.g., methods. The electronic signature process captures the User's name, the record they are signing, the reason it is being signed, e.g., approval, and a date/time stamp. The signature is only executed after a User with signing permission provides their account password. Electronic records can be displayed, printed, and exported in text format.
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.	Electronic signatures are linked to their respective electronic records. Signatures cannot be excised, copied, or transferred. Biomek methods may be printed as text; printed methods include the date and time stamp of the printing, which allows traceability to the version of the method in the software. Control of handwritten signatures is the responsibility of the user.

Subpart C—Electronic Signatures

11.100 General requirements.

Part	Description	Comments
(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	The Administrator may make a unique account for each individual user. A unique electronic signature is associated with each unique account. Signatures cannot be reused across accounts. Usernames may not be reused in the system. Control of the transfer of accounts is the responsibility of the user.

Part	Description	Comments
(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.	Regulation refers to the responsibility of the User and should be maintained using proper protocols and documentation.
(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.	Regulation refers to the responsibility of the User and should be maintained using proper protocols and documentation.
Sec. 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	To submit an electronic signature, users must first login to Beckman Coulter software by employing two distinct identification components: a username and a password. Once the User is logged into the software, the user must again supply their password to successfully execute an electronic signature. The Administrator can configure the Biomek software to automatically log the User out after a period of inactivity. Users can log themselves out at any time.

Part	Description	Comments
	signature components.	
	(2) Be used only by their genuine owners; and	Regulation refers to the responsibility of the User and should be maintained using proper protocols and documentation.
	(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.	No one (including the Administrator) can use another individual User's account.
(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Beckman Coulter software does not currently support biometrics.
Sec. 11.300 Controls for identification codes/passwords.		
Part	**Description**	**Comments**
	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.	Beckman Coulter software requires that every individual User has a unique identification code (username).
(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	The Administrator can configure Beckman Coulter software to require users to a) change their passwords after a set number of days and 2) never re-use a password.
(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.	Administrators can deactivate compromised accounts. Administrators can set up a new account; the intended User of that account must create the password, ensuring that the Administrator does not know the User's password and thus cannot electronically sign a document as that User.
(d)	Use of transaction safeguards to prevent unauthorized use of passwords and/or	Administrators can deactivate compromised accounts. Accounts can be

Part	Description	Comments
	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.	automatically disabled after a number of failed attempts to login (can be set to any number from 1 – 999).
(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.	Beckman Coulter software does not currently support devices such as security tokens and cards.

Biomek Automated Workstations are not intended or validated for use in the diagnosis of disease or other conditions.