Vi-CELL BLU Regulatory Compliance – 21 CFR Part 11

The following document describes the relevant portions of the 21 CFR Part 11 regulations and their implementation using the Vi-CELL BLU control software. The implementation and compliance of 21 CFR Part 11 remains the responsibility of the organization or entity creating and signing the electronic records in question. Proper procedures and practices, such as GLP and GMP, are as much part of the overall compliance with these regulations as are the features of the Vi-CELL BLU control software.

21 CFR PART 11

The Electronic Records and Electronic Signatures Rule (21 CFR Part 11) was established by the FDA to define the requirements for records in electronic form and the criteria for approved electronic signatures.

ELECTRONIC RECORDS

Per Section 11.3 subpart A of 21 CFR Part 11, an electronic record is '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'. This refers to any digital computer file submitted to the FDA, or any information not submitted but that needs to be archived. Public docket No. 92S-0251 of the Federal Register (Vol. 62, No. 54) identifies the types of documents acceptable for submission in electronic form and where such submissions may be made.

FDA REQUIREMENTS

The general comments section of the ruling states that 'The agency emphasizes that these regulations do not require, but rather permit, the use of electronic records and signatures'. The introduction to the final ruling states that 'The use of electronic records as well as their submissions to FDA is voluntary'.

If electronic submissions are made, Section 11.2 explains that 'persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures provided that: (1) The requirements of this part are met; and (2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251'.

The Vi-CELL BLU control software has been designed to enable users to comply with the electronic records and signatures rule.

BECKMAN COULTER
Life Sciences

IMPLEMENTING ELECTRONIC RECORDS AND SIGNATURES

Section 11.3 Subpart A describes two classes of systems:

1. **Closed Systems**

   A closed system is one 'in which system access is controlled by persons who are responsible for the content of electronic records'. In other words, the people and organization responsible for creating and maintaining the information on the system are also responsible for operating and administering the system.

2. **Open Systems**

   An open system is one 'in which system access is not controlled by persons who are responsible for the content of electronic records'. Under this definition Vi-CELL BLU is consided to be an Open system.

The Vi-CELL BLU control software is designed to ensure the proper operation, maintenance and administration for system security and data integrity. Anyone who interacts the Vi-CELL BLU, from administrators to users, must abide by these procedures. Therefore the ultimate responsibility is with the organization generating electronic records and signatures. The Vi-CELL BLU software is a component, albeit a vital one, of the overall process.

CONTROLS FOR ELECTRONIC RECORDS

Subpart B, Section 11.10 describes the controls to be applied to a "closed system". Section 11.30 describes the controls for an "open system", which include "those identified in Section 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards".

The primary thrust of these controls is "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". In other words, to protect the data and to make it difficult for someone to say that this is not their "signature". Many of the controls described in Section 11.10 refer to written procedures (SOPs) required of an organization by the agency, for the purpose of data storage and retrieval, access control, training, accountability, documentation, record keeping, and change control. The other controls are addressed either by the Vi-CELL BLU software itself, or in combination with end-user procedures.

ESTABLISHING AN ELECTRONIC RECORD

The Vi-CELL BLU software employs a system of usernames and passwords, consistent with the specifications of Subpart C, Section 11.300, "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".

21 CFR PART 11 SECURITY

To turn on the security option, select

NOTE Inactivity timeout is set to prevent unofficial access to the system, as when the system is left unattended directly after starting the queue.

The system will prompt you to log in. On the Log In dialog, enter your user name and password.

New users can only be created and passwords reset by users with Administrator rights. This file is protected with a checksum and for each user name, contains information on when the user was created, by whom, at what level, the user's password in encrypted form and the user's file paths. If this file does not exist or if the checksum is missing, or invalid, then access to the system will only be possible to a limited number of special users.

FILE HISTORY

The Vi-CELL BLU software also performs data input and "operational checks", as specified in Subpart B, Section 11.10, "to determine, as appropriate, the validity of the source of data input or operational instruction", and "to enforce permitted sequencing of steps and events". These two features ensure that valid data are being entered into the system, and all required steps have been completed to perform the task at hand.

The purpose of all such data checking and validation is described in Section 11.10, Paragraph (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". Vi-CELL BLU software data files are all automatically saved upon creation and protected with a checksum. Vi-CELL BLU software also allows for the capability for backing up data to mirror directories.

Section 11.10, paragraph (e) requires "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. Such audit trail documentation must be retained for a period at least as long that required to for the subject electronic records and must be available for agency review and copying." The Vi-CELL BLU software complies with this rule by generating an audit trail which records the time a user was logged on. The audit trail is encrypted and check summed for added security. The audit trail also will record and time-stamp: failed login attempts, switching users, turning security on or off, adding new user, enable/disable user, change password, reset password, lock instrument and failed checksums. Refer to Table 6.4 in the Vi-CELL BLU Instructions for Use (document C13232) for a list of audit trail events and the related descriptions.

When a data file is created, the Vi-CELL BLU system software provides a computer-generated time-stamped record that documents actions taken to create a record. This information is stored with in the actual data file itself, not in the Audit Trail file. Each data file contains a computer-generated time-stamped record, the date and time of operator entries, and the actions taken to create the datafile.

The system software does not allow a data record to be modified or deleted within the normal operation of the system software.

If the integrity of a data file is compromised in some way, the file is rendered unusable by the system and it can no longer be used by the Vi-CELL BLU software. Each data file contains an embedded checksum that is used to check the integrity of the file each time the file is loaded. If the data file is compromised, an error message is displayed and the file does not load.

ELECTRONIC SIGNATURE

In Subpart A, Section 11.3, an electronic signature is defined as "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". Subpart C, Section 11.100 of the regulation defines the general requirements of such a manifestation. Paragraph (a) states that "each electronic signature must be unique to one individual and must not be reused by, or reassigned to, anyone else". These two paragraphs, taken together, mean that an electronic signature is some computer representation of a user's identity, developed to ensure the distinct and unique identity of that user. The procedural aspect of Section 11.100 requires that before any such electronic representation is applied, the organization first must "verify" the identity of that individual.

Subpart C, Section 11.200, refers to biometric and non-biometric forms of electronic signature. Non-biometric signatures are those that are computer generated and, as per Section 11.200,"Employ at least two distinct identification components such as an identification code and password". It is this form of electronic signature that is supported by the Vi-CELL BLU software.

GENERATING ELECTRONIC SIGNATURES

The Vi-CELL BLU software employs User IDs and passwords to verify the identification of each user logging into the system. When using this technique, Subpart C, Section 11.300 of the regulation requires “maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password”. This section also requires that the “identification code and password issuances are periodically checked, recalled, or revised”. Vi-CELL BLU software supports both of these provisions.

NOTE To support 21 CFR Part 11 compliance the user name entered should be the full user display name.

The administration of the system requires that individuals are added to the list of valid Vi-CELL BLU users via the Add a New User dialog box. The “identification code” or username of each Vi-CELL BLU user must be unique. No two users on the same Vi-CELL BLU system can have the same user name. It is also required that these users supply a password to access the Vi-CELL BLU software, thus satisfying the requirement to “employ at least two distinct identification components such as an identification code and password”. Passwords can be controlled to prohibit the use of duplicates and to force the selection of new passwords after a prescribed period of time.

By the implementation of these features, the Vi-CELL BLU software can satisfy the requirement that “identification code and password issuances are periodically checked, recalled, or revised”.

APPLYING ELECTRONIC SIGNATURES

Subpart C, Section 11.200 stipulates several requirements for the control of electronic signatures. Procedurally, the regulations require that electronic signatures “be used only by their genuine owners” and that they “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”. Through the application of Vi-CELL BLU user and password configuration procedures, the system can be configured to “ensure” that inappropriate use of these identifiers can be performed only by the intentional divulgence of security information.

Section 11.200 further specifies the use of electronic signature components during a period “when an individual executes a series of signings during a single, continuous period of controlled system access”, and “when an individual executes one or more signings not performed during a single, continuous period of controlled system access”. To comply with these provisions, the Vi-CELL BLU software uses the application of the username and password to authenticate the user making and saving the changes, in conjunction with file history.

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

PART-5229FLY04.19