WHITE PAPER

Guidance for Ensuring your EnVision Multimode Plate Reader Complies with 21 CFR Part 11

EnVision® Multimode Reader

Introduction

Ensuring that laboratory processes are compliant with the regulations of the U.S. Food and Drug Administration (FDA), such as CFR Part 11, and other references, e.g. Annex 11 published by the European Commission, can be time-consuming and laborious, requiring meticulous documentation of procedures and record-keeping.

Within a laboratory environment, software, such as that used for controlling instrumentation, on its own cannot be "compliant" with such regulations. However, a combination of software tools and administrative procedures, when well-aligned, can pave the way towards compliance.

To help ensure that procedures which involve the EnVision multimode plate reader are compliant, an add-on to the instrument's software is available. Named the Enhanced Security option, this software provides a variety of tools to enable easier and faster compliance with 21 CFR part 11.

With specific reference to the relevant paragraphs of 21 CFR Part 11, this document describes how the tools within the EnVision Enhanced Security software facilitate compliance with this regulation.

PerkinElmer® For the Better

21 CFR PART 11 AND ENVISION ENHANCED SECURITY

Controls for Closed Systems

21 CFR Part 11 reference[1]	Responsibility (control)	Explanation
11.10 Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed 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.	*User with help from PerkinElmer*	With the Enhanced Security software, the EnVision is a closed system. PerkinElmer delivers support with user training. In the system, features that ensure authenticity, integrity, and confidentiality of electronic records are activated. Automated verification routines are implemented within the software to ensure the functionality of the instrument within defined parameters.
11.10 (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	*User with help from PerkinElmer*	The user must have procedures, such as Standard Operating Procedures (SOPs) and Work Instructions (WIs), in place for appropriate validation and operation of the system. PerkinElmer can deliver substantial support with user training, IQ and OQ services. The audit trail is provided to track alteration of records.
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.	PerkinElmer *(Technical)*	Result reports and audit trails can be displayed on screen and printed from the EnVision Enhanced Security software.
11.10 (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	PerkinElmer *(Technical)* User *(Procedural)*	All data generated with the EnVision system is stored and protected within a relational database. Stored results can be reloaded for review. The user must establish guidelines and procedures for the operators of the instrument to back up the database regularly.
11.10 (d) Limiting system access to authorized individuals.	PerkinElmer *(Technical)* User *(Procedural)*	A password and unique user login name is necessary for the use of the instrument controlled by the Enhanced Security option. Also the software for service of the instrument is login-controlled and intended for PerkinElmer personnel only. All logins, login attempts and logoffs are tracked by the software. A user is notified if an unsuccessful login attempt has occurred for his account. After a definable number (defined by the security administrator of the instrument) of failed login attempts the affected account will be locked and can only be released again by the security administrator. The security administrator of the instrument can allocate a new password to a user. The user is required to change this password at his first login. The user is also able to change his password at any time. The user has to ensure regular review of the user audit trail which must be part of the system's procedural compliance. It is recommended to set up further security administrator accounts in the event that the original security administrator is absent or has forgotten his password.

21 CFR Part 11 reference	Responsibility (control)	Explanation
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.	PerkinElmer *(Technical)*	All data generated with the EnVision under control of the Enhanced Security option is stored and maintained within the relational database. All settings, processes (such as protocol runs) and results are stored together with the data and tracked within an audit trail. Original data cannot be overwritten. Changes to records will not obscure previous database entries. Changes will generate a new data set. Full user name, time and type of action will be tracked within the audit trail. If settings of the instrument or within a protocol change, new and old values are documented. The audit trail can be exported and printed for inspection purposes. With the EnVision 1.14 Enhanced Security software, an optional audit trail viewer (ATV) can be installed. This web-based application allows easy access to the user and instrument audit trails with several filter options to find the required information faster. With the installation of the ATV the 'reason for change' option will be enabled. With this functionality the user is prompted to enter the reason for the change of certain values.
11.10 (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	PerkinElmer *(Technical)* User *(Procedural)*	Protocols with automated data collection, data processing (calculations), and data export (e.g. to Excel) can be set up within the EnVision software. The setup of the protocols is the responsibility of the user. The user group to which a user is assigned defines which parts of the software he is permitted to use. The system checks whether accessories (e.g. mirrors) were changed and are appropriate for the selected method in a protocol to ensure the validity of the data. Scheduling of instrument performance checks must be defined by the user and must be part of the system's procedural compliance.
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.	PerkinElmer *(Technical)*	The EnVision Enhanced Security software offers default user groups with different access rights for the software. The 'Security Administrator' can edit these groups or create new groups to adapt the access levels of the individual users to the needs within the organization. Individual roles with specific permission rights can be assigned to each authorized user of the system. Predefined groups are 'Security Administrator', 'Administrator', 'Editor', and 'Operator'. With the installation of the audit trail viewer (ATV) the 'reason for change' entry field is enabled within the software. The EnVision software also allows custom access levels to be created by the Security Administrator. As the permission matrix is complex, we recommend using the default levels for enhanced security environments.
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.	PerkinElmer *(Technical)*	The EnVision software is the only device that is able to write into the relational database. The user control functionality inhibits access to the database by unauthorized persons. Only one user can be logged into the system and input can only come from logged in users.
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.	PerkinElmer *(Technical)* User *(Procedural)*	PerkinElmer service engineers are trained and certified to provide install service (including IQ/OQ) and maintenance for Multimode Detection (MMD) instruments. The training of the end users of the EnVision instrument is the responsibility of the user and should be part of the system's procedural compliance. PerkinElmer can provide in-house or off-site user training on the instrument and the software to provide support for this requirement.

21 CFR Part 11 reference	Responsibility (control)	Explanation
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.	User *(Procedural)*	The user has to ensure that individuals are accountable for actions undertaken under their electronic signature and must be part of the system's procedural compliance.
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.	PerkinElmer *(Technical)* User *(Procedural)*	System and software related documentation is provided on a portable electronic data storage device (e.g. USB flash drive) delivered together with the instrument and cannot be changed. It is the responsibility of the user to maintain and provide controls and documentation of the installed system. This must be part of the system's procedural compliance. The software, print-outs, and data exports contain the version information. It can also be included in the user's documentation.

Controls for Open Systems

21 CFR Part 11 reference	Responsibility (control)	Explanation
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 ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.		The EnVision software itself is a closed system. PerkinElmer offers in collaboration with MyAssays Ltd an option to transfer measurement data to MyAssays Desktop for further data analysis. With the implementation of an electronic certificate, record integrity is implemented for this data transfer.

Signature Manifestations

21 CFR Part 11 reference	Responsibility (control)	Explanation
11.50 (a) **(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 (a1), (a2), and (a3) 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).	PerkinElmer *(Technical)*	(1), (2) Only one user can be logged into the system. Any actions undertaken by the logged-in user will be documented in the audit trail with full name of the user and the date and time of the action. (3) With the installation of the audit trail viewer (ATV) the 'reason for change' entry field is enabled within the software.

21 CFR Part 11 reference	Responsibility (control)	Explanation
11.50 (b) The items identified in paragraphs (a1), (a2), and (a3) 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).	PerkinElmer *(Technical)*	Login and log off events are tracked within the audit trail.

Signature / Record Linking

21 CFR Part 11 reference	Responsibility (control)	Explanation
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.	PerkinElmer *(Technical)* User *(Procedural)*	The data and settings generated with the EnVision Enhanced Security software are linked with the user information of the logged-in user within the database. This information is also tracked within the audit trail. It is the responsibility of the user to take action to prevent the misuse of user account names and passwords. The control of hardcopy printouts of data (graphs, results, reports, audit trails) is the responsibility of the user.

General Requirements

21 CFR Part 11 reference	Responsibility (control)	Explanation
11.100 (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	PerkinElmer *(Technical)*	Each user name is unique and cannot be assigned to another user. Deactivated user accounts cannot be re-used.
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.	User *(Procedural)*	User is responsible for compliance with parts (b) to (d)
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), 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.		

Electronic Signature Components and Controls

21 CFR Part 11 reference	Responsibility (control)	Explanation
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.	PerkinElmer *(Technical)* User *(Procedural)*	To log into the system the user must enter both a user name and an associated password. A single user name must be restricted to a single person's use. Only this person must know the password for his user name.
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.		Not applicable

Controls for Identification Codes / Passwords

21 CFR Part 11 reference	Responsibility (control)	Explanation
11.300 (a) Controls for identification codes/passwords. 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: Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	PerkinElmer *(Technical)*	Each user has a unique user name which cannot be assigned to another user.

21 CFR Part 11 reference	Responsibility (control)	Explanation
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 EnVision Enhanced Security software provides controls for password length and complexity, expiry date, number of failed log ins, and time until automatic log out when system is idle. With the EnVision Enhanced Security option the settings can be adapted to the individual password policies of the organization.
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.		Not applicable
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.	PerkinElmer *(Technical)* User *(Procedural)*	Failed login attempts are recorded and documented in the audit trail. User is notified if there were such attempts with his account. The number of failed logins can be defined within the password management settings of the EnVision Enhanced Security software. It is the responsibility of the user to check the audit trail on a regular basis to discover attempts to circumvent the security procedures.
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.		Not applicable

References

1. Code of Federal Regulations, Title 21 Food and Drugs, Chapter I Food and Drug Administration, Department of Health and Human Services, Subchapter A General, Part 11 Electronic Records; Electronic Signatures. www.ecfr.gov. Accessed November 2017.

PerkinElmer, Inc.
940 Winter Street
Waltham, MA 02451 USA
P: (800) 762-4000 or
(+1) 203-925-4602
www.perkinelmer.com

PerkinElmer®

For a complete listing of our global offices, visit www.perkinelmer.com/ContactUs

010931A_01 PKI