White Paper

INTEGRA

21 CFR Part 11 – Electronic Records; Electronic Signatures compliance of the VIALAB, ASSIST PLUS and electronic pipettes

1 Introduction

21 CFR Part 11 – Electronic Records; Electronic Signatures defines the criteria under which the FDA accepts electronic records and electronic signatures as equivalent to paper-based records and handwritten signatures. These requirements apply to pharmaceutical and medical device manufacturers, biotech companies, CROs and other FDA-regulated industries worldwide.

This document describes how the ASSIST PLUS pipetting robot, VIALAB software (version 3.7.0 or higher) and electronic pipettes align with the requirements of 21 CFR Part 11, and supports its use in regulated laboratory environments.

2 Scope of this document

This document is intended to support laboratory, quality and validation teams in assessing the suitability of the ASSIST PLUS for implementation in GxP-regulated environments, and preparing for audits and inspections.
The ASSIST PLUS is not a fully compliant, turnkey 21 CFR Part 11 solution. Instead, it is designed to enable and support compliant workflows when integrated into a properly controlled laboratory and IT environment.

As with any system used in GMP environments, overall compliance depends on the customer's implementation, including:

- execution of validation activities
- integration into the existing IT infrastructure (e.g. Active Directory, secure data storage)
- establishment of appropriate SOPs and change control procedures
- configuration and management of user access and roles
-

With the introduction of VIALAB 3.7.0, significant enhancements have been implemented to further support regulated use, including:

- role-based user management via Active Directory, enabling controlled system access
- enhanced run reports supporting traceability
- unique hash-based program identification, ensuring the integrity and traceability of validated methods

3 Definitions and interactions of INTEGRA software and pipettes

This section defines the operating modes and interactions between the VIALAB software, electronic pipettes and the ASSIST PLUS, hereinafter referred to as the ASSIST PLUS pipetting system.

The ASSIST PLUS pipetting system can be operated in 2 distinct configurations (PC control and standalone), which can be enabled or restricted through password-protected system settings. This allows customers to implement controlled workflows in accordance with their internal requirements and SOPs.

A pipetting program represents a complete set of liquid handling instructions, including parameters such as volumes, speeds and pipetting positions. These programs define the execution of a laboratory method and therefore constitute electronic records within the scope of 21 CFR Part 11.

In **PC control mode**, VIALAB serves as the central control interface, where methods are created, transferred and executed within the ASSIST PLUS pipetting system. The ASSIST PLUS instrument and electronic pipettes complete these instructions without modification, ensuring consistent and reproducible process execution.

In **standalone mode**, pipetting programs are transferred from VIALAB to the electronic pipette prior to execution. The program is then carried out directly by the pipette, without any active connection or interaction with the VIALAB software during method execution.

3.1 Visualization of PC control mode

VIALAB PC software

- User management via Active Directory
- Create, store and execute pipetting programs
- PDF/HTML run reports of executed pipetting steps

Live program transfer of pipetting instructions

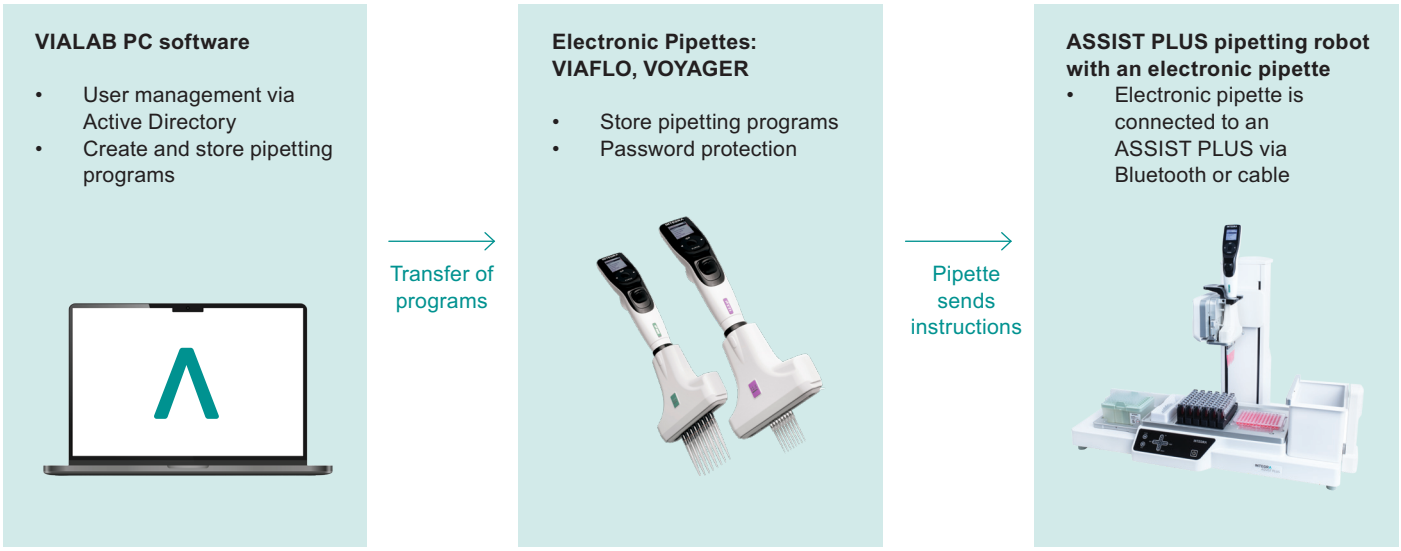
Live log of executed pipetting steps

USB cable connection

ASSIST PLUS pipetting robot with an electronic pipette

- Electronic pipette is connected to an ASSIST PLUS via Bluetooth or cable

3.1 Visualization of standalone mode



4 Comparison of the ASSIST PLUS pipetting system versus US 21 CFR Part 11 – Electronic Records; Electronic Signatures

The ASSIST PLUS pipetting system comprises VIALAB software, the ASSIST PLUS pipetting robot and electronic pipettes.

Compliance-relevant technical controls are primarily implemented within the VIALAB software, while hardware components execute validated instructions without modification. Additional safeguards, such as password protection of the electronic pipettes to prevent unauthorized program changes, support the controlled execution of validated methods.

Compliant in the context of this document means that the system provides the necessary capabilities for customers to achieve regulatory compliance when implemented and operated within a properly controlled laboratory and IT environment.

4.1 Comparison table for PC control mode

Requirement	Compliant	INTEGRA statement
§ 11.10 (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	N/A	**No requirement for the ASSIST PLUS pipetting system.** The validation must be carried out by the end customer in accordance with the generally applicable guidelines. INTEGRA supports validation through design, specifications and training materials.
§ 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.	Yes	**This requirement is fulfilled through VIAL**AB. Quality-relevant process data can be exported as a PDF in an unalterable manner. The process raw data is saved in HTML format in the VIALAB installation directory on the computer. Pipetting programs (configurations) are saved in a common XML (.iaa) file format and can be exported to PDF. The access security of the storage location must be defined and configured by the end customer.
§ 11.10 (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Yes	**This requirement is fulfilled through VIALAB.** VIALAB stores quality-relevant data reliably and securely. An external path for storing the logs can be set in the standard operating procedure. The configuration of long-term storage is the responsibility of the end customer.
§ 11.10 (d) Limiting system access to authorized individuals.	Yes	**This requirement is fulfilled through VIALAB.** User management and all associated regulatory requirements are fulfilled by connecting user management to the Windows Active Directory. During installation, the corresponding Active Directory group name must be entered for each role.
§ 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.	Yes	**This requirement is fulfilled through VIALAB.** End users do not have the ability to modify configuration data. Each configuration is assigned to a unique identifier (hash code). Any modification to a configuration that has already been validated must be performed through the customer‘s formal change control process. Therefore, a dedicated audit trail for configuration changes within VIALAB is not required.
§ 11.10 (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Yes	**This requirement is fulfilled through VIALAB.** The menu navigation by the end user is clearly structured. System checks ensure that process steps are executed in the permitted sequence, preventing out-of-order actions.
§ 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.	Yes	**This requirement is fulfilled through VIALAB.** User management and security policies are controlled by Active Directory. The authorizations are predefined in the system and cannot be adjusted.
§ 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.	N/A	No quality-relevant data is entered manually.

§ 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.	Yes	**This requirement is fulfilled through the ASSIST PLUS pipetting system.** Manuals, user manuals, videos and training documentation are always tailored to the version used.
§ 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.	N/A	All requirements for electronic signatures are omitted. VIALAB electronic signatures are not implemented.
§ 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	N/A	No requirement for the software. Documentation is the responsibility of the user.
§ 11.10 (k) (2) System Documentation Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Yes	**This requirement is fulfilled through VIALAB.** End users do not have the ability to modify configuration data. Each configuration is assigned to a unique identifier (hash code). Any modification to a configuration that has already been validated must be performed through the customer‘s formal change control process. Therefore, a dedicated audit trail for configuration changes within VIALAB is not required.
§11.30 Controls for open systems	N/A	The ASSIST PLUS pipetting system is a closed system.
§11.50 Signature manifestation §11.70 Signature/record linking	N/A	All requirements for electronic signatures are omitted. VIALAB electronic signatures are not implemented.
§ Subpart C – Electronic Signatures §11.100 General requirements §11.200 Electronic signature components and controls § 11.300 Checks for identification codes and passwords	N/A	All requirements for electronic signatures are omitted. VIALAB electronic signatures are not implemented.

4.2 Comparison table for standalone mode

Requirement	Compliant	INTEGRA statement
§ 11.10 (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	N/A	**No requirement for the ASSIST PLUS pipetting system.** The validation must be carried out by the end customer in accordance with the generally applicable guidelines. INTEGRA supports validation through design, specifications and training materials.
§ 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.	Yes	**This requirement is fulfilled through VIALAB.** VIALAB offers the option to export and print PDF files. The PDF reports include all critical details of the pipetting program. Pipetting programs can be saved as XML and PDF files on the PC or network drive, and can be archived.
§ 11.10 (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Yes	**This requirement is fulfilled through VIALAB.** Pipetting programs are saved in a common XML file format and can be exported to PDF.
§ 11.10 (d) Limiting system access to authorized individuals.	Yes	**This requirement is fulfilled through VIALAB.** User management and security policies are controlled by Active Directory. The authorizations are predefined in the system and cannot be adjusted.
§ 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.	No	The pipettes themselves can be protected against program changes and overwriting. The end user has no option to change the configuration data. A change to a configuration that has already been validated must be made as part of a change process. An audit trail functionality that monitors changes is not implemented.
§ 11.10 (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Yes	**This requirement is fulfilled through VIALAB and the pipette.** The menu navigation by the end user is clearly structured. System checks ensure that process steps are executed in the permitted sequence, preventing out-of-order actions.
§ 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.	Yes	**This requirement is fulfilled through VIALAB and the pipette.** VIALAB user management and security policies are controlled by Active Directory. The authorizations are predefined in the system and cannot be adjusted. Pipetting programs on the pipette can be password protected to prevent unauthorized modification.
§ 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.	N/A	Not a requirement. All inputs to VIALAB come from the user. There is no interface to other systems. VIALAB programs transferred to the pipette are in a proprietary file format. The pipette itself cannot receive data from any device other than a computer running VIALAB.

§ 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.	N/A	All requirements for electronic signatures are omitted. VIALAB electronic signatures are not implemented.
§ 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.	N/A	All requirements for electronic signatures are omitted. VIALAB electronic signatures are not implemented.
§ 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	N/A	No requirement for the software. Documentation is the responsibility of the user.
§ 11.10 (k) (2) System Documentation Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	N/A	Documentation is the responsibility of the user.
§ 11.30 Controls for open systems	N/A	The ASSIST PLUS pipetting system is a closed system.
§11.50 Signature manifestation §11.70 Signature/record linking	N/A	All requirements for electronic signatures are omitted. VIALAB electronic signatures are not implemented.
§ Subpart C – Electronic Signatures §11.100 General requirements §11.200 Electronic signature components and controls § 11.300 Checks for identification codes and passwords	N/A	All requirements for electronic signatures are omitted. VIALAB electronic signatures are not implemented.

Contact us: