CTech™ ViPER® ANLYTX Software: 21 CFR Part 11 & Annex 11 Compliance Position for VPT Systems

White Paper

DOC0198 eRev. 02 02/06/2023

analytics-applications@repligen.com | +1 908-707-1009 | ctech.repligen.com

REPLIGEN
INSPIRING ADVANCES IN BIOPROCESSING

Repligen Corporation

685 Route 202/206 Bridgewater, NJ 08807 USA

International telephone:	+1 908-707-1009
International fax:	+1 908-707-1030
Applications email:	analytics-applications@repligen.com

Disclaimer: This document serves as a template for Standard Operating Procedure (SOP) development through use of the CTech™ variable pathlength technology (VPT) systems. Repligen Corporation and/or its affiliates, to the extent allowed by law, disclaims, and in no event shall be liable for, any incidental or consequential damages in connection with user, instrument, or system performance in relation to all content contained in this document, including but not limited to fitness for location of use, specific purpose for use, or application.

Information, descriptions, and specifications in this publication are subject to change without notice.

Abstract

The CTech™ Variable Pathlength Technology (VPT) System comprising the ViPER® ANLYTX Software has tools that enable compliance with the ruling on electronic records and electronic signatures by the Food and Drug Administration (FDA) and the European Union. The FDA is responsible for outlining the rules and regulations for 21 CFR Part 11 while the European Union is responsible for outlining the rules and regulations for Annex 11. As the capabilities and functions available in the software alone cannot guarantee a compliant implementation, the procedural controls set by the organization are responsible for proof of compliance.

In order to comply with 21 CFR Part 11 and Annex 11, procedural and administrative controls must be included in an organization's software package(s). These include validating the electronic records system and drafting and maintaining standard operating procedures for the use of the electronic records system. Also required is adequate training of the system's users so they fully comprehend its role in compliance, understand administrative privileges or restrictions, and adhere to their assigned tasks.

Repligen understands that its VPT System users have complex records systems and privacy policies for data storage. Online support and training for the VPT System are readily available in order to close potential 21 CFR Part 11 and Annex 11 compliance gaps.

Introduction

Title 21 CFR Part 11 of the Code of Federal Regulations, by the United States Food and Drug Administration (FDA), sets the criteria for which electronic signatures, electronic records, and handwritten signatures executed to electronic records are considered trustworthy and reliable.[1] It provides the guidelines and rules related to copying, permissions, audit-log tracking, version control, and the application of electronic signatures to electronic documents.

EudraLex is the collection of rules and regulations set by the European Union governing medicinal products. Annex 11 is part of these GMP guidelines that defines the terms of reference for computerized systems in the pharmaceutical industry.[2] The three main areas of focus include the system features, standard operating procedures and system validation. The guidelines set forth by the European Commission are similar to their U.S. counterpart created by the FDA.

This paper is intended to provide information about the tools, capabilities, and functionality available in the ViPER software for organizations considering the implementation of a 21 CFR Part 11 and Annex 11 compliant system. Ultimate responsibility for achieving full compliance with these requirements lies with the VPT System user's criteria, implementation, and validation processes and efforts. Nevertheless, Repligen works with VPT System users to assist them in understanding any software limitations and, at its discretion, incorporates possible enhancements.

The full text of 21 CFR Part 11 can be found on the Electronic Code of Federal Regulations website: https://www.ecfr.gov

The full text of Annex 11 can be found on the EudraLex website: https://ec.europa.eu/health/documents/eudralex/vol-4_en

[1] See U.S. Department of Health and Human Services, Food and Drug Administration, Center for Drug Evaluation and Research, Center for Biologics Evaluation and Research, Center for Devices and Radiological Health. Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers: Guidance for Industry (June 2017).

[2] See European Commission, "Guidelines on Good Manufacturing Practice Specific to Advanced Therapy Medicinal Products" (2017).

1. Background

CTech ViPER ANLYTX software utilizes an industry standard authentication model known as Lightweight Directory Access Protocol (LDAP), which is an open- and cross-platform protocol used for directory services authentication. It enables anyone to locate data in a network, whether on the public Internet or on a corporate Intranet. This allows the ViPER software to create a complete interface for command and control of the VPT System hardware for any application.

ViPER software is bundled with applications developed for all of CTech Variable Pathlength instrument systems. The software's application-based structure allows users to run a variety of tests and collect data under one environment. Each application has built-in assistance with configurations that are simple, accessible, and granular.

ViPER software uses Microsoft SQL Server as its database, which allows data to be stored and retrieved within the software itself. Users and groups are no longer dependent on the Windows New Technology File System (NTFS) structure; they now depend on the computer systems' Active Directory and user permissions governed by ViPER software. This allows for data to be saved to a network or local database. If the data is being stored on a network database, ViPER software can be accessed from multiple computer systems, making it easy to manage each system.

ViPER software uses the VPTCore service to handle the communication between the user interfaces and the hardware logic. The VPTCore service acts as an Open Platform Communications Unified Architecture (OPC UA) server which allows it to control the instrument functionality through a generic OPC client. This provides the VPT System user with another communications platform to configure and run their methods. To ensure compliant OPC implementation, the OPC client must be configured by the systems administrator. A full exploration of OPC UA integration is beyond the scope of this document; however, Repligen can provide proper documentation if requested.

This document includes more detailed information regarding the specific functionalities within the software, and some examples and options of how ViPER software can be used to achieve a compliant implementation.

2. 21 CFR Part 11: Specific Applications

This section provides more detailed information as to how the tools available in the VPT System can be applied by companies to the relevant 21 CFR Part 11 regulations as part of an overall compliance plan.

2.1 §11.10 Controls for closed systems.

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. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Repligen provides qualification services in the form of Installation Qualification Operational Qualification (IQOQ) of the VPT System by trained VPT Support Specialists. This service is included when systems are purchased to ensure that the hardware and software are properly installed at the VPT System user's location. Following the IQOQ, the VPT System user can begin to develop the required policies and procedures and utilize the tools available with the system in accordance with the compliance plan.

Preventative Maintenances (PMs), which include an IQOQ, can be purchased to ensure optimal and consistent performance of the system. Repligen recommends periodic requalification of the system and offers periodic PM services to VPT System owners.

Repligen offers computer system validation services. The service is performed by executing a protocol that addresses the creation of user accounts, the management of software, the execution of test cases, and the verification of a fully validated system.

Audit trails in the system provide detailed information regarding system access, performance, use, and manipulation to help users comply with regulation. Invalid or altered records are captured and stored within the audit trails. Electronic signatures utilize unique user ID and password authentication to ensure that signed records are genuine and linked to the appropriate individual. Audit trail information is stored within the ViPER software and can be filtered by the user, device, application, event type, and date/time.

(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.

The ViPER software environment is designed to allow users to run, collect, analyze, and report samples from a variable pathlength instrument. Data is represented in a table that can be exported to an Excel or CSV format. Word-based reports can be exported as a PDF, as it is a more secure and compliant format.

To ensure data security and integrity and to safeguard against possible malicious intent or accidental compromise, electronic records reside within the ViPER software environment and are incapable of being deleted or overwritten once created. ViPER software permanently autosaves data to the software's database. The SecureVPT™ and Admin Settings allow the user to configure and access specific applications. These settings allow for electronic signatures to be authored, reviewed, approved, or overridden where the original file cannot be duplicated. The administrator is responsible for establishing proper user and group permissions and incorporating their use into the workflow and standard operating procedures.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

The ability to access and configure electronic records can be controlled through the user's appropriate and supportive use of permissions within the ViPER software. Records exist in the ViPER database and backups are highly encouraged. The administrator is responsible for establishing proper user and group permissions and incorporating their use into the workflow and standard operating procedures. Users must define roles within their organization and grant the necessary permissions that are appropriate for their compliance plan.

(d) Limiting system access to authorized individuals.

Access controls to the VPT System can be set at two levels of the ViPER software, where permissions can be granted or revoked for the user and/or group. Each layer provides unique options and functionality that the VPT System user should consider when developing a compliance plan.

The following chart provides a basic overview to give guidance on how to incorporate these features into a compliance plan.

Layer	Access Control Overview
Admin Settings	• The Admin Settings is a feature within the ViPER software that contains information about the System and the specific applications. This feature gives the user the ability to configure details specific to the organization as well as the device. • A complete exploration of the parameter settings available in the Admin Settings is beyond the scope of this document. However, it is crucial to understand that the controls provided at this layer of the security structure relate exclusively to the ViPER software and need to be configured appropriately to meet the goals of the organization.
SecureVPT Settings	• The SecureVPT Settings is a built-in security module that allows users to define roles within ViPER software and the specific application. • ViPER software allows the SecureVPT Settings to be linked to the Active Directory for user and group data at the domain level. Local users and groups can be created within the ViPER software without the need for LDAP authentication. • The ViPER Role feature grants users administrative or standard privileges while the User Type feature defines the level of control within a specific application. Feature Access grants or revokes user authorization to a specific function within each application.

(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.

Extensive audit trails are recorded within the ViPER software environment through the Audit Log. This feature contains a granular, efficient, and robust log that captures all events within the software.

The application provides read-only viewing of the audit trail information. It provides a single source for reviewing specific audit trails and ensures accessibility, even without administrative privileges. The Audit Log can be filtered based on the username, device, application, event type, and date/time. The date/time format can be configured to meet the guidelines of the organization. The Columns feature allows the user to configure the amount of audit trail information they want to view.

The extent to which a VPT System user makes use of these capabilities must be decided by the organization and be implemented with their own internal network experts. These decisions need to include their plan for maintaining, backing up, and archiving data.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Repligen recommends the organization develop policies and procedures that utilize the capabilities and functions within the ViPER software to enforce the permitted sequencing of steps and events using operational system checks. The security features of the ViPER software, particularly the SecureVPT settings, allow administrators to set up users and groups with specific permissions to create, modify, and run methods. When permissions are properly configured, users are constrained by the method parameters and their authorization to specific applications. Proper configuring of permissions combined with the electronic signature capability allows the VPT System user to ensure the integrity and authenticity of the electronic record.

(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.

The VPT System can be configured to authorize access to and control of the system, configuration or record changes, and electronic signatures. The organization is responsible for designing the policies and procedures around the System's capabilities in order to meet their compliance goals. Because there are multiple layers of security features, it is important to consider the specific features available within each layer when designing the security plan. Each layer can be configured to secure specific types of access, control, and data.

Repligen provides specific information regarding the security requirements of its software packages; however, it cannot provide guidance on the overall network security due to the complexity and variability existing in the industry. At the most basic level, however, Microsoft Windows allows VPT System users to configure unique user accounts that are password-protected. The network administrator can control user access to the computer/network through the Active Directory. When implemented in this fashion, the Windows login creates a first line of defense for securing the computer system.

The Admin Settings is the second level of security for the VPT System. This feature allows the user to control the parameters within the device and the application. In order to have access to the Admin Settings, the permissions must be granted within the SecureVPT Settings. Modification of any of these settings requires the user to authenticate themselves with their username and password.

The SecureVPT Settings is the final and more detailed level of security threshold for the System. This software feature enables the organization to configure a permissions matrix for each user that is System-specific. The permissions can be set to specific features and functions within the ViPER software environment, providing administrators the flexibility to control what actions users perform when they access the System. Similar to the Admin Settings, any modification requires the user to authenticate themselves with their username and password.

The ViPER software is independent of the Agilent Cary WinUV software and is no longer bound to NTFS permissions. Additionally, the eSignature capability within the ViPER software is configured within the SecureVPT Settings thus prompting the user to provide authenticated credentials to authorize critical steps in the process.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

The SecureVPT Settings can be configured to prompt the logged-in user to record an eSignature through an authentication prompt. This requires the user to provide their password before and after critical operations to ensure the validity of the input and output.

(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.

Repligen has been supporting fiber-optic-based spectroscopy equipment in the biopharmaceutical industry for more than a decade. As part of its implementation of the System, an organization can contact Repligen to request and review aspects of its development policies, processes, and procedures. Repligen provides employee training and education in a variety of ways. Some of the services include on-site training, validation support, support webinars, user documents, and phone support.

(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.

Repligen recommends that the organization develop policies and procedures that describe and govern the actions that administrators and end users must perform using the System. For administrators, policies and procedures should be developed for system-related actions such as user and group management, password management, and SecureVPT user permissions. For end users, policies and procedures should be developed for actions such as method creation, data-naming conventions, and eSignature applications.

(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.

Repligen provides documentation with each System. The documentation is updated and distributed with each version of the software. It is up to the organization to implement security controls over the access, retention, and use of the documentation.

2.2 §11.30 Controls for open systems.

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.

Repligen recommends that the organization implement appropriate policies and procedures, given the capabilities and constraints of the VPT System, to achieve compliance with this requirement. The VPT System and security capabilities provide specific functionality intended to support compliance as it relates to user authentication, data integrity, and confidentiality as follows:

Authentication: System access can be controlled through both the Windows Active Directory as well as the SecureVPT Settings.

Integrity: Administrators can configure various security levels to constrain the generation, modification, and storage of data by specific user accounts and electronic signatures. They can utilize the Audit Log to view specific events that occurred within the software.

Confidentiality: To ensure confidentiality, Repligen recommends that VPT System users appropriate workstation and network security profiles that can control user-specific visibility and accessibility of information. Documented policies and procedures also need to be part of the implementation plan for the organization.

Digital Signatures: The SecureVPT Settings allows the implementation of account-driven electronic signatures. Additionally, the system can be configured to allow users to initiate electronic signature events for reviews and approvals.

2.3 §11.50 Signature manifestations.

(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.

Electronic signatures are executed by the user through the ViPER software application interface, whereupon the user is required to enter their username and password. The electronic signature is stored with the data along with the signer's full name, date, time the signature was executed, purpose of the signature (e.g., author, review, approval, or override) and reason for 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).

The ViPER software appends a human readable text block with the details of each electronic signature. This information saves to the ViPER SQL Server database. Since it co-exists with the data, the security and control structure are identical.

2.4 §11.70 Signature/record linking.

Electronic signature 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.

The electronic signature, if applied, is added to the report. Appending additional electronic signatures to a previous report will force the user to save the data as a separate file. The collected data saves to the SQL Server database, which will contain the established electronic signature. Repligen recommends that the organization create the necessary policies and procedures, given the capabilities and constraints of the VPT System, to achieve compliance with this requirement.

2.5 §11.100 General requirements.

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

Repligen recommends that the organization implement policies and procedures to ensure that usernames are assigned to only individuals and that each individual agrees not to divulge their password under any circumstances. These policies and procedures must be applied to the Windows Active Directory usernames, and the user must be given authorization to eSignatures within SecureVPT settings.

(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.

Repligen recommends that the organization incorporate policies and procedures to ensure that usernames are assigned to individuals with proper authorization and approval given their role and responsibilities. The VPT System user's IT team or equivalent must be responsible for creating user profiles that align with the identity of the individual.

(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.

Repligen recommends that the organization implement policies and procedures, given the capabilities and constraints of the ViPER software, to comply with the certification requirements of this regulation. Repligen affirms that the electronic signatures within the ViPER software are the legally binding equivalent of the signer's handwritten signature. It is up to the organization to certify that the electronic signatures create legally binding equivalents to traditional handwritten signatures.

2.6 §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 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.

The electronic signature requires the user’s username and password for every execution. Repligen recommends that the organization implement policies and procedures, given the capabilities and constraints of the ViPER software, to comply with the certification requirements of this regulation. It is up to the organization to certify that the electronic signatures require corroboration of two of more individuals when attempting to sign for the owner of that signature. Repligen does not recommend password sharing of any sort.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

The VPT System does not use biometric authentication techniques. Instead, a user of the System enters their username and password to authorize a signature.

2.7 §11.300 Controls for identification codes/passwords.

Persons who use electronic signatures based upon use of identification codes (usernames) 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.

Repligen recommends that the organization create policies and procedures to ensure the uniqueness of the identification code and password combinations. The Windows Active Directory capabilities provide for extensive types of password policies including complexity, aging, change requirements, lock out, reuse prevention, and expiration. It is the responsibility of the VPT System user‘s IT team or equivalent to authorize unique identification codes and passwords for individuals. Organizations should involve their network administrator to define policies that support their overall implementation plan.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

Repligen recommends that the organization create policies and procedures to ensure that identification codes and passwords are periodically reviewed and managed as required. The Command Prompt can be utilized to view the details of a user’s password. The Windows Active Directory capabilities provide for extensive types of password policies including complexity, aging, change requirements, lock out, re-use prevention, and expiration.

(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.

Repligen recommends that the organization create policies and procedures to ensure that identification codes and passwords are deauthorized, if required. The VPT System user's IT team or equivalent is responsible for performing the deauthorization. Windows Active Directory allows for deactivation of user profiles within the domain and the local computer. The Windows Active Directory capabilities provide for extensive types of password policies including complexity, aging, change requirements, lock out, re-use prevention, and expiration.

(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.

Repligen recommends that the organization create policies and procedures to ensure that identification codes and passwords are safeguarded as required. The VPT System user's IT team or equivalent is responsible for creating appropriate safeguards. The Windows Active Directory capabilities provide for extensive types of password policies including complexity, aging, change requirements, lock out, re-use prevention, and expiration.

(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.

Repligen recommends that the organization create policies and procedures to ensure that devices containing identification codes and passwords are periodically tested as required. The ViPER software does not require devices that contain identification code or password information to access the system. If necessary, it is the responsibility of the VPT System user's IT team or equivalent to create and implement such devices. The Windows Active Directory capabilities provide for extensive types of password policies including complexity, aging, change requirements, lock out, re-use prevention, and expiration.

3. Annex 11: Specific Applications

This section of the document provides more detailed information as to how the tools available in the VPT System can be applied to the relevant section of the Annex 11 regulations by companies as part of an overall compliance plan.

3.1 Risk Management

3.1.1 Risk management should be applied throughout the lifecycle of the computerized system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerized system.

Repligen recommends that the organization create policies and procedures to assess the risk of the system. Repligen works with their VPT System users through available training and online support, to ensure that the capabilities and functionality of its System are fully understood and that any potential risks are addressed. It is recommended that the VPT System user discusses their risk assessment protocol(s) with Repligen's analytical applications team.

3.2 Personnel

3.2.1 There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.

Administrators must define roles within their organization and grant the necessary permissions that are appropriate for their compliance plan. Repligen can provide documentation that recommends specific access levels for various roles. Ultimately it is up to the administrator to define these roles and the level of access within the system.

3.3 Suppliers and Service Providers

3.3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerized system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.

Repligen works with several authorized partners that provide, install, configure, integrate, validate, maintain, modify, or retain our VPT Systems. For the most up to date list of partners, please refer to our website. Ultimately it is up to the VPT System user to decide if they want third parties to be involved with the implementation of the system; however, Repligen will work with customer-provided third parties to ensure a successful and compliant implementation.

3.3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.

Repligen is a competent, reliable, and ISO 9001 certified organization that supplies variable pathlength systems. ISO 9001 is recertified every three years and the organization is audited yearly. Repligen will allow its customers to audit their Quality Management System as applicable.

3.3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.

This requirement is not within the scope of this document; however, user manuals and specification documents can be provided.

3.3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.

Repligen is ISO 9001 certified and will always allow its customers to audit their Quality Management System as applicable.

3.4 Validation

3.4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.

Repligen will be able to justify their standards, protocols, acceptance criteria, procedures, and records based on VPT System users' risk assessment. Repligen will assist with their VPT System users' validation documentation; however, it is ultimately up to the administrator to define and evaluate all the necessary requirements.

3.4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.

Repligen recommends that the organization include change control records and reports on any deviations within their validation documentation. It is highly recommended that the VPT System users utilize the software's Audit Trail feature to watch for any deviations. Repligen will assist with their VPT System users' validation documentation; however, it is ultimately up to the administrator to define and evaluate all the necessary requirements.

3.4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.

Repligen can provide documentation relevant to the GMP functionality of the VPT System. Documentation detailing the system specifications, software release notes and user manuals will cover the requirements within this section. It is up to the VPT System user to keep an updated log of this information.

3.4.4 User Requirements Specifications should describe the required functions of the computerized system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.

Repligen recommends that the organization create a user requirements specification that describes the required functions of the system based on the VPT System user' risk assessment and GMP impact. Repligen can provide VPT System users with a suggested user permission guideline associated with each user type. Repligen does not provide documentation on user requirements specifications; however, we will work with our VPT System users on developing such documentation tailored to the risk assessment guidelines of the organization. Ultimately it is up to the administrator to define and evaluate these requirements.

3.4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.

Repligen recommends that their VPT System users take actions to ensure that the system has been developed in accordance with their quality standards. Repligen will work with its VPT System users to ensure that the system has been developed, validated, and implemented in accordance with the specifications and guidelines of the VPT System user. It is up to the administrator to define these steps within their validation plan and verify that all requirements have been met accordingly.

3.4.6 For the validation of bespoke or customized computerized systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.

Repligen recommends that its VPT System users create a process to ensure that the quality and performance of the system has been formally assessed and reported. Repligen will work with its VPT System users to develop such process; however, it is up to the VPT System user to have these procedures defined in their validation plan.

3.4.7 Evidence of the appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tolls and test environments should have documented assessments for their adequacy.

Parameter and data limits can be configured in the Admin Settings of the ViPER software. Additionally, Repligen offers computer system validation services. The service is performed by executing a protocol that addresses the creation of user accounts, the management of software, the execution of test cases, and the verification of a fully validated system. However, if the VPT System user decides to utilize our services, Repligen is not responsible for the implementation and compliance of the System. Repligen will assist with developing the appropriate test methods and test scenarios; however, it is up to the administrator to define, document, and assess their criteria.

3.4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.

Repligen recommends that VPT System users check the integrity of their values when transferring data from one data format or system to another. The ViPER software can append data to common file formats, such as .PDF and .CSV, and the SQL Server database can be read on a variety of software management systems. Repligen will work with its VPT System users to assess this criterion; however, it is up to the administrator to implement this into their validation plan.

3.5 Data

3.5.1 Computerized system exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.

The ViPER software has the capability to exchange data to other computerized systems. A full list of those systems is beyond the scope of this document; however, Repligen will work with its VPT System users to develop accurate and secure processing of data from one computerized system to another. Ultimately it is up to the administrator to define the necessary built-in checks and minimize the potential risks.

3.6 Accuracy Checks

3.6.1 For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.

Repligen recommends that the criteria for manually entered data be defined by the VPT System user. The ViPER software does not allow its users to manually input data that was measured by the VPT System. The software sends instructions directly to the VPT System which does not allow the user to manipulate any corresponding data.

3.7 Data Storage

3.7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.

Repligen recommends that the organization create policies and procedures to ensure that identification codes and passwords are safeguarded as required. The ability to access and configure electronic records can be controlled through the VPT System users' appropriate and supportive use of permissions within the ViPER software. The administrator is responsible for establishing proper user and group permissions and incorporating their use into the workflow and standard operating procedures. Administrators must define roles, grant the necessary permissions that are appropriate for their compliance plan, and ensure that data is secure by both physical and electronic means.

3.7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of back-up data and the ability to restore the data should be checked during validation and monitored periodically.

The ViPER software allows users to transfer, back up and store data to other computerized systems. Since data is stored within the ViPER software, it is the VPT System user's IT Team responsibility for periodically backing up the ViPER SQL Server database. Repligen recommends that VPT System users incorporate regular back-ups of their data that is periodically monitored, especially throughout the validation of the system.

3.8 Printouts

3.8.1 It should be possible to obtain clear printed copies of electronically stored data.

The ViPER software environment is designed to allow users to run, collect, analyze, and report samples from a variable pathlength instrument. Data is represented in a table that can be exported to Excel, CSV or PDF. Hard copy output is possible when a physical printer is connected to the System.

3.8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.

Repligen recommends that VPT System users review printouts of data to ensure that the integrity and accuracy has not been changed since the original entry. It is up to the administrator to integrate this process into their implementation plan.

3.9 Audit Trails

3.9.1 Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.

The ViPER software contains an Audit Log. This feature contains a granular, efficient, and robust log that captures all events within the software.

The application provides read-only viewing of the audit trail information. It provides a single source for reviewing specific audit trails and ensures accessibility, even without administrative privileges. The Audit Log can be filtered based on the user, device, application, event type, and date/time. The Columns feature allows the user to configure the amount of audit trail information they want to view.

3.10 Change and Configuration Management

3.10.1 Any changes to a computerized system including system configurations should only be made in a controlled manner in accordance with a defined procedure.

Repligen recommends that users define a process for changing system configurations. It is highly recommended that only system administrators have the ability to make these changes. Administrators must define roles that are in accordance with their implementation plan.

3.11 Periodic Evaluation

3.11.1 Computerized systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.

Repligen recommends that VPT System users periodically evaluate the System to confirm that their requirements are still within the specifications of their compliance plan. Repligen will assist in developing a periodic evaluation plan; however, it is up to the administrator to ensure that the evaluation includes the above requirements.

3.12 Security

3.12.1 Physical and/or logical controls should be in place to restrict access to computerized system to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.

Repligen recommends that the organization create policies and procedures to ensure that access to computerized devices is restricted only to authorized personnel. The Windows Active Directory capabilities provide for extensive types of password policies including complexity, aging, change requirements, lock out, re-use prevention, and expiration. ViPER software has the same capabilities for accounts that are built into the software.

3.12.2 The extent of security controls depends on the criticality of the computerized system.

Security controls to the VPT System can be set at two levels of the ViPER software; the SecureVPT Settings and the Admin Settings. Each layer provides unique options and functionality that the VPT System user should consider when developing a compliance plan. It is recommended that organizations create user access levels that determine the necessary security controls. It is the administrator’s responsibility to define the criticality of the System and implement the necessary security controls that are in accordance with their compliance plan.

3.12.3 Creation, change, and cancellation of access authorizations should be recorded.

Repligen recommends that the organization track the creation, change, and cancellation of access authorizations. Windows Active Directory manages user account information within the computerized system. The Audit Log tracks any user account changes associated with the ViPER software. It is up to the administrator to manage and track all modifications regarding user authorization to the System.

3.12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.

The Audit Log provides detailed information regarding system access, performance, use and manipulation to help VPT System users comply with regulation. Each record contains the identity of the operator and the date and time as to when the action was performed. Audit trail information is stored within the ViPER software and can be filtered by the username, device, application, and event type.

3.13 Incident Management

3.13.1 All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.

The Audit Log records all events within the ViPER software, including system failures and data errors, with reasons for certain events. A full list of those events is beyond the scope of this document. It is up to the administrator to record all incidents that are incapable of being tracked within the ViPER software, and to implement the necessary corrective and preventive actions.

3.14 Electronic Signature

3.14.1 Electronic records may be signed electronically. Electronic signatures are expected to:

a. **have the same impact as hand-written signatures within the boundaries of the company,**

b. **be permanently linked to their respective record,**

c. **include the time and date that they were applied.**

Electronic signature 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 executed by the user through the ViPER software application interface, whereupon the user is required to enter their username and password. The electronic signature is stored with the data along with the signer’s full name, date, time the signature was executed, purpose of the signature (e.g., author, review, approval, or override) and reason for the signature.

3.15 Batch Release

3.15.1 When a computerized system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.

The ability to access and configure electronic records can be controlled through the VPT System users’ appropriate and supportive use of permissions within the ViPER software. The administrator is responsible for establishing proper user and group permissions and incorporating their use into the workflow and standard operating procedures. The ViPER software allows the user to interact with a laboratory information management system (LIMS). This can certify that only qualified personnel have the ability to release batches. Administrators must define qualified personnel and ensure that they have permissions to electronically sign batch release records.

3.16 Business Continuity

3.16.1 For the availability of computerized systems supporting critical processes, provision should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.

In the event of a system breakdown, it is highly recommended that the VPT System user contact Repligen. An organization can contact Repligen to request and review aspects of its development policies, processes, and procedures. Repligen provides on-site support, employee training, validation support, support webinars, user documents, and phone support. Other necessary arrangements must be defined and implemented by the administrator.

3.17 Archiving

3.17.1 Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.

Repligen recommends that the organization create policies and procedures for archiving their data. The VPT System user's IT Team is responsible for periodically backing up the ViPER SQL Server database. It is up to the administrator to periodically check the data for accessibility, readability, and integrity.

Conclusion

Repligen is committed to working with its customers to successfully achieve the implementation and deployment of its technologies. The utility and broad applicability of UV-Vis measurements is reflected in the diversity of our customers and installation sites.

Many of our customers are in the bio-pharmaceutical industry and are subject to a variety of regulatory constraints. Repligen is committed to working with our customers to ensure that the capabilities and functionality of its system enable customers to design and implement a compliance installation. To help successfully craft a compliance plan, Repligen provides support services that highlight the tools, capabilities, and requirements of the VPT System. Ultimately, compliance remains the responsibility of the customer.

References

European Commission. "Guidelines on Good Manufacturing Practice Specific to Advanced Therapy Medicinal Products.” *EudraLex: The Rules Governing Medicinal Products in the European Union, Volume 4 Good Manufacturing Practice*. November, 2017. Retrieved from the European Commission: https://ec.europa.eu/health/sites/health/files/files/eudralex/vol-4/2017_11_22_guidelines_gmp_for_atmps.pdf

U.S. Department of Health and Human Services, Food and Drug Administration, Center for Drug Evaluation and Research, Center for Biologics Evaluation and Research, Center for Devices and Radiological Health. *Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers: Guidance for Industry*. June, 2017. Retrieved from https://www.fda.gov/media/105557/download.