WHITE PAPER

VISION SP: Security Pack for 21 CFR Part 11 compliance

Introduction

Wyatt Technology's VISION® Security Pack (SP) product provides multiple features to address those aspects of regulatory compliance that are relevant to the VISION software in a regulated environment per Title 21/Part 11 of the U.S. Code of Federal Regulations (21 CFR Part 11). This white paper contains (1) a brief discussion of 21 CFR Part 11, (2) a description of software development at Wyatt Technology, (3) detailed descriptions of how VISION satisfies each of the relevant provisions of the federal ruling, and (4) a discussion regarding validation of the VISION product.

21 CFR Part 11 Overview

The United States Food and Drug Administration (FDA) adopted regulations in 1997 covering the use of electronic records and electronic signatures in a regulated environment. These rules are contained in the Code of Federal Regulations (CFR), Title 21, Part 11, and contain subparts regarding electronic records and electronic signatures. The rules define how computer-generated data are to be stored and used, and aim to make electronic records comparable to a lab notebook in terms of providing an immutable, traceable record.

The 21 CFR Part 11 ruling leaves significant room for interpretation, and the FDA has no process whereby a software product can receive an official "21 CFR Part 11 Approved" stamp. Each customer is encouraged to perform their own audit to verify that the implementation of 21 CFR Part 11 in VISION SP meets the needs of the company.

Software Development at Wyatt Technology

All software development at Wyatt Technology is carried out under a formal quality system (ISO 9001:2015). We follow a standard software lifecycle including requirements analysis, functional analysis, design, implementation, and testing. We employ fully automated software configuration management tools that make it possible to trace requirements through the development process to final testing. The result is a development process that creates quality, compliant software that can be validated.

21 CFR Part 11 Requirements and VISION

The ruling defines two broad types of software systems, open and closed, and the requirements for each. VISION is a closed system, as defined by "...system access is controlled by persons who are responsible for the content of electronic records that are on the system."

Therefore, the following will contain only requirements pertaining to closed systems. These requirements begin in Section 11.10:

Subpart B—Electronic Records

§ 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.

There are two parts to this requirement. The first concerns the validation of the VISION software for maintaining accurate, reliable and consistent performance. For this purpose, Wyatt Technology provides a validation procedure designated 'IQ/OQ', or Installation Qualification / Operation Qualification which the user may employ to check that the software interacts reliably with the instruments and the analyses performed with the software are consistent with the results obtained at the factory.

The second part of this requirement concerns the ability to discern invalid or altered records. Under SP, all VISION data are stored in a secure database which takes advantage of the security regime provided by Microsoft® SQL Server® and Microsoft Windows®, and each database entry contains an encrypted checksum. VISION uses this checksum to verify that the data being read from the database has not changed since it was last written and to discern invalid or altered records. VISION notifies the user of any data corruption or attempt to alter the data.

(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.

With regards to original records in electronic form, all VISION data are stored in a secure database. It is necessary to use the VISION application to view the records in the database.

VISION can export a copy of a single record to a file that can be opened by another VISION installation for review. All records stored in the database contain encrypted checksums to verify that the data is accurate.

VISION can generate human readable copies of these records. All records can be exported to text, shown in tables, or graphed, where applicable. VISION also generates human readable reports of records in VISION RUN that can be saved for printing or review.

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

All data and audit trails generated under VISION SP are stored together in a secure database requiring administrative privileges on the computer to access directly. All other access is controlled by VISION. The database is accessed via the Open Database Connectivity (ODBC) industry standard. Use of the ODBC standard enables the database to be installed either locally or on a networked server for automatic backup by the IT department. A networked architecture also allows multiple computers to access the data and facilitates disaster recovery. The database structure for VISION SP ensures that records and the associated audit trails will not be lost.

Records in the database are protected from accidental deletion or modification by the use of privilege levels in VISION SP. Since database access is controlled by VISION, it is possible to control the actions of users in the database based on privilege levels. Only administrators have the ability to delete records. In addition, the metadata associated with each record is never modified. It is therefore not possible to overwrite or inadvertently modify the metadata.

(d) Limiting system access to authorized individuals.

VISION SP leverages the Microsoft Windows security system to limit system access to authorized individuals. This includes:

Secure login: In order to run VISION under SP, users must enter a unique user ID and password. Logins, login attempts, and logouts are all recorded in a system audit trail. VISION SP and ASTRA SP are synchronized, i.e., running VISION SP automatically requires ASTRA SP being launched and synchronized. VISION SP and ASTRA SP also use the same joint SQL database for VISION and ASTRA data.

Setting up user accounts: VISION SP uses Microsoft Windows user accounts and groups for security. System administrators create four security groups specific to VISION SP, then associate existing Microsoft Windows users with these groups. The Microsoft Windows user accounts are then used to log in to VISION SP. VISION SP and ASTRA SP user accounts and groups are synchronized, i.e., they use a single login to VISION under the same privileges. For details on ASTRA SP compliance, please refer to *M1008, ASTRA SP: Security Pack for 21 CFR Part 11 compliance.*

Networked security: It is possible to set up the VISION SP security groups in the Active Directory, such that

network-authenticated accounts can be given VISION SP privileges. One domain-level user account can then be used to log in to any instance of VISION SP on the network.

(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.

VISION SP provides two levels of audit trail to independently record all operator actions that create, modify, or delete electronic records. Each entry in the audit trail is time-stamped, and records the operator performing the actions, as well as the computer where the actions are performed.

Audit trail information is added sequentially, and previous audit trail entries are not modified or overwritten. The audit trail is always associated with the records in the database. As long as the database records are maintained, the audit trail will be maintained and available. The audit trail information can be accessed through the VISION application in human readable format for review and copying.

The top-level audit trail is the system log, which is associated with the database. The system log records actions such as:

- Logins, login attempts, and logouts
- Data creation, modification, and deletion
- Database connections and disconnections
- Import and export of data from the database

A second audit trail is also associated with each type of record (methods, sequences, configurations, or experiments). Each record has a separate log that records all actions within the experiment that affect the data. The record log is always with the record and cannot be reset. The log records actions such as:

- Changes to instrument configuration settings
- Changes to sequences
- Changes to methods
- Collection of data

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

VISION structures data collection and analysis in terms of a sequence of procedures that can be saved as a method or template. VISION SP supports different privilege levels for its users. A “Researcher” privilege level enables a user to develop new methods that can be saved. A “Technician” privilege level enables a user to run existing methods without modifying them. In this way, VISION SP can enforce upon Technicians the use of validated methods developed by Researchers.

(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.

VISION SP uses the Windows security features described above to create VISION SP-specific groups. The system administrator can assign a user different privilege levels in VISION SP by associating their user account with one of the following groups:

Administrator: Administrators have rights to perform all actions, including changing database connections and deleting records. However, administrators cannot delete audit trail information.

Researcher: Researchers can create and run new FFF methods and sequence templates, change instrument configuration settings, and export and import data from the database.

Technician: Technicians can only run sequence templates and FFF methods set up by a Researcher. Technicians can collect data and perform simple processing, but cannot change any configuration settings.

Guest: Guests have read-only privileges to view audit trails and data.

If a user attempts to run VISION under the SP without a valid user account, or does not belong to one of the above VISION SP security groups, the user will not be allowed to run the program or access data. VISION SP makes direct calls to the Windows operating system to verify users and privilege levels. VISION SP also makes use of the same security mechanisms to ensure that only authorized individuals can electronically sign a record.

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

Only one computer should be allowed access to the Wyatt Technology instrument by setting up a local sub-network that includes only the computer and the set of intended instruments.

Data input to VISION can only come via a direct connection of a Wyatt Technology instrument to the VISION Instrument Server Interface (ISI). The ISI uses device driver checks to verify the type of instrument connected to the computer. All recorded data is marked as coming from a particular instrument and recorded in the audit trail associated with the record. However, if multiple Wyatt instruments are on the local network, VISION cannot ascertain if the specific instrument(s) selected is/are the one(s) intended by the user. This must either be left to the user to determine, or hardwired during installation by creating a local sub-network that includes only the intended instruments.

(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.

Not applicable. This is the responsibility of the user.

(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.

Not applicable. This is the customer's responsibility.

(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.

Revisions to VISION are reflected in updated manuals and customer-specific procedures. Installation of updates to VISION result in immediate manual updates as well, since the manuals are installed as part of VISION. Customers can also obtain updated IQ/OQ procedures. However, manuals and IQ/OQ procedures are not protected from unauthorized access except by standard Windows login protocols. It is the user's responsibility to control distribution and access to this documentation by means of such logins.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

All software development documentation and final product documentation, such as instruction manuals and customer-specific procedures such as IQ/OQ, are under strict change control with audit trails according to our document control procedure. Change documents are provided with each new version of the software. If these documents are not sufficiently detailed, Wyatt internal documents with complete change lists will be made available to the VISION SP user upon request.

§ 11.30 Controls for open systems.

Not applicable. VISION is a closed system.

§ 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 can be executed on any data collected. As such, electronic signatures will be performed in ASTRA SP which may be executed within VISION SP. Electronic signatures in ASTRA SP can be reviewed in the experiment audit trail. The signatures contain the following information: 1) user ID, 2) full printed first and last name of signer, 3) the date and time of the signature, 4) the meaning associated with the signature, and 4) any additional details relevant to the context of the signing. The time stamp for each signature is taken from the computer system time where ASTRA is installed. ASTRA stores these time stamps in a native GMT format such that it can translate them into the appropriate time based on time zone. This also makes it possible to compare signature time stamps made across time zones, or even enables users in different time zones to use the same database.

(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).

All electronic signatures are placed into the audit trail for each record such that the signature will always be associated with the appropriate record. These signatures have the same safeguards as all other records stored in the database. All signatures are available as human readable records through the ASTRA application. In addition to viewing the signatures through the audit trail for the record, the report for each record contains the electronic signatures for that record with all of the components listed above for 11.50 (a).

§ 11.70 Signature/record linking.

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

Electronic signatures are placed directly into the ASTRA SP audit trail for the record such that they cannot be excised, copied, or transferred to another electronic record. Transfer of the record includes transfer of the audit trail for the record, so the electronic signatures are always linked to the record. ASTRA Researchers and Administrators are able to lock an experiment upon signoff.

Subpart C—Electronic Signatures § 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.

The user security for VISION and ASTRA is based on the Microsoft Windows security such that unique user IDs and passwords are enforced. It is not possible to delegate or assign an electronic signature in ASTRA to someone else. However, it is the responsibility of the user to verify that login credentials are not passed from individual to individual, as ASTRA SP and VISION SP do not utilize biometric validation.

(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.

Not applicable. This is the customer's responsibility. ASTRA SP and VISION SP do not utilize biometric validation.

(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.

Not applicable. This is the customer's responsibility.

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

Electronic signatures in ASTRA SP require a combination of unique ID and password for every signing. It is the responsibility of the user to ensure that log-in credentials are not transferred from individual to individual.

§ 11.300 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: (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.

The uniqueness of the user ID password combination is enforced by the Windows operating system user security.

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

These provisions are built into the Windows operating system user security functionality. VISION derives this functionality through Windows.

(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. This is the customer's responsibility.

(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.

Any attempts at unauthorized access to VISION or to electronic signature functionality is recorded in the system audit trail and marked as an event. An administrator can review this audit trail on a periodic basis to detect unauthorized access. Immediate and urgent reporting of unauthorized use is not supported by VISION SP.

(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. This is the customer's responsibility.

VISION Validation

One of the most challenging aspects of developing 21 CFR Part 11 compliant software is validation. VISION SP is a completely validated product: All software development is done under a formal quality system (ISO 9001:2015), using a standard software lifecycle model. Documented testing and traceability is performed to demonstrate accuracy, reliability, and consistent intended performance.

Ultimately, we understand that the end user must verify that Wyatt Technology has held true to the demands of validation when creating VISION. To that end, we welcome audits of the software development process from qualified auditors.

Questions?

Please contact us if you have any questions. If you are one of our international customers, feel free to contact your local representative directly. Contact information for our global offices is listed at www.wyatt.com/Distributors.

You may reach our corporate office at support@wyatt.com or by calling us at +1 (805) 681-9009. Selecting option 4 will connect you with our Customer Support team.

WYATT TECHNOLOGY