Sparta Systems TrackWise Solution

21 CFR Part 11 and Annex 11 Assessment

June 2019

Introduction

The purpose of this document is to outline the roles and responsibilities for compliance with the FDA's 21 CFR Part 11 and alignment with the European Union's Annex 11 as they apply to Sparta System's TrackWise product. The regulations require organizations to have administrative, procedural, and technical controls in place. While it is not possible for Sparta to offer a turnkey 21 CFR Part 11 or EU Annex 11 compliant system, the information provided in this document will assist customers in achieving compliance.

Both regulations cover the same topic, the use of computerized systems in regulatory environments. However, the approach of 21 CFR Part 11 is to clarify the requirements to be met with an emphasis on activities and reporting. EU Annex 11 points to risk assessment as the start of compliance activities. In addition, Part 11 differentiates security for open and closed systems, with security for open systems but without reference to risk and criticalities. The aggregate of these differences is represented with the comparison matrix shown below.

Contents

High-level Comparison of EU Annex 11 and FDA 21 CFR Part 11

	Part 11	Annex 11
Scope/Principle	Electronic records and electronic signatures as used for all FDA regulated activities.	Computerized systems as part of GMP regulated activities. Application should be validated. IT infrastructure should be qualified.
Focus	Using electronic records and signatures in open and closed computer systems.	Risk- based quality management of computerized systems.
Objective	Electronic records and signatures should be as trustworthy and reliable as paper records and handwritten signatures.	Using a computerized system should ensure the same product quality and quality assurance as manual systems with no increase in the overall risk.

Controls for Closed Systems

21 CFR Part 11	Annex 11	Responsible Party	TrackWise
11.10(a) Is the system validated to ensure accuracy, reliability, and consistent intended performance? Is it possible to discern invalid or altered records?	4.1 Do validation documents and reports cover the relevant steps of the life cycle?	User & Sparta	Customers are responsible for validation of any changes that impact their TrackWise implementation, performing risk-based testing and validation before each release in accordance with their internal documented SOPs or processes. TrackWise offers a full audit trail where changes to quality records are logged. The audit trail includes user ID, old and new value, and time stamp. Unauthorized changes are prevented by the access security controls. Multiple checks, such as unique identifiers of files, are used to help detect and prevent unauthorized data manipulation.
11.10(b) Is the system capable of producing accurate and complete copies of records in electronic form for inspection, review, and copying by the FDA?	8.1 Is the system capable of producing clear printed copies of electronically stored data?	Sparta	Records can be exported for viewing and printing in common electronic formats.
11.10(c)	17	User & Sparta	It is the customer's responsibility to define retention periods.

21 CFR Part 11	Annex 11	Responsible Party	TrackWise
Are the records protected to ensure their accurate and ready retrieval throughout the records' retention period?	Is data archived? If data is archived is it checked for accessibility, readability and integrity? When changes are made to the system, is the ability to retrieve archived data ensured and tested?		TrackWise has an infinite retention period and data is retrievable at any time. If data is archived, the customer is responsible for managing that archive in compliance with retention periods defined in applicable predicate rules.
11.10(d) Is system access limited to authorized individuals?	10 Are system changes made in a controlled manner in accordance with a defined procedure? 12.2 Do the security controls extend depending on the criticality of the system?	User & Sparta	Customers are responsible for defining a procedure for system changes for their system configuration. The customer is responsible for defining authorized access to the system. Data is secured by both the TrackWise functionality and the customer configuration. A unique user ID and password is required for each user session. Any session left idle based on customer configuration is automatically terminated.

21 CFR Part 11	Annex 11	Responsible Party	TrackWise
11.10(e) Is there a secure, computer-generated, time-stamped audit trail that independently records the date and time of operator entries and actions that create, modify, or delete electronic records? Upon making a change to an electronic record, is the previously recorded information still available (e.g. not obscured by the change)? Is an electronic record's audit trail retrievable throughout the record's retention period? Is the audit trail available for review and copying by the FDA?	14.c Do electronic signatures include the time and date that they were applied? 12.4 Is the system designed to record the identity of operators entering, changing, confirming or deleting data including date and time? 9 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.	Sparta	TrackWise provides full audit trail for create and modify operations. The TrackWise audit trail records previous values. Audit trail entries and record data cannot be deleted. the identity of operators entering, changing, confirming, or deleting data, including date and time. The audit trail can be made available during the entire retention period. TrackWise activity history details are available for review and printing.

21 CFR Part 11	Annex 11	Responsible Party	TrackWise
11.10(f) Are the operational system checks used to enforce permitted sequencing of steps and events?	5 Computerised systems 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. 6 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.	User & Sparta	TrackWise allows for fully configurable workflow management, thus the customer can define the required sequence of steps and events and ensure the proper process which must be followed.
11.10(g) Does the system, through the use of authority checks, 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 other operations?	7.1 How is data secured by both physical and electronic means against damage? How is data accessible throughout the retention period? 12.1 Are physical and/or logical controls in place to restrict access to the system?	User & Sparta	TrackWise allows for fully configurable security modeling, user groups, roles, and permissions. Access and role application are under customer's control and should follow customer defined processes.

21 CFR Part 11	Annex 11	Responsible Party	TrackWise
11.10(h) If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g. terminals) and does the system check the validity of the source of any data or instructions received	4.8 When data is transferred to another data format or system, does the system check the validity to confirm data was not altered in value and/or meaning during migration.	User	Customers control security related to the application by controlling network access, system access, and security around other system interfaces including web services.
11.10(i) Is there documentation that persons who develop, maintain, or use TrackWise have the education, training, and experience to perform their assigned tasks?	2 Is there close cooperation between all relevant personnel such as process owner, system owner, qualified persons and IT? Do all personnel have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties?	User & Sparta	Within Sparta, employees are formally trained on policies, SOPs, and work instructions. These SOPs outline how relevant personnel work together to complete their tasks. Employees also receive on the job training appropriate to their responsibilities. It is the customer's responsibility to demonstrate that their administrators and users have the education, training, and experience to perform their assigned tasks.
11.10(j) Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures?		User	This is the responsibility of the using organization.
11.10(k) (1) Is the distribution of, access to, and use of systems operation and maintenance documentation controlled? (2) Is there a formal change procedure for system documentation that maintains a time sequenced audit trail of changes?	4.2 Do validation documents include change control records (if applicable) and reports on deviations observed during the validation process?	User & Sparta	Sparta restricts distribution of system operation and maintenance documentation to contracted customers. It is the responsibility of the customer to establish procedures covering the distribution of, access to, and use of documentation once the system is in use. It is the responsibility of the customer to ensure adequate change control procedures for documentation related to their implemented solution.

Controls for Open Systems

21 CFR Part 11	Annex 11	Responsible Party	TrackWise
11.30			Not applicable as TrackWise is a closed system.

Signature Manifestation

21 CFR Part 11	Annex 11	Responsible Party	TrackWise
11.50 (a) Do signed electronic records contain the following related information? • The printed name of the signer • The date and time of signing • The meaning of the signing (such as approval, review, responsibility)		Sparta	Yes, this information is included in TrackWise.
11.50 (b) Is the above information shown on displayed and printed copies of the electronic record?		Sparta	Electronic signature information can be viewed on the record and record history in TrackWise.

Signature/Record Linking

21 CFR Part 11	Annex 11	Responsible Party	TrackWise
11.70 Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred by ordinary means for the purpose of falsification?	14(b) Are electronic signatures permanently linked to their respective record	Sparta	Signatures cannot be cut, copied, or otherwise transferred by ordinary means.

Electronic Signatures – General

21 CFR Part 11	Annex 11	Responsible Party	TrackWise
11.100(a) Are electronic signatures unique to one individual and can not be reused by, or reassigned to, anyone else?		User & Sparta	Every user has a unique id and the id is associated to their e-Signature. Only one user with the same name and PID (Personal ID) can be active at any time. It is the customer's responsibility to ensure PIDs accounts are never re-assigned to different users.
11.100(b) Is the identity of an individual verified before an electronic signature is allocated?		User	It is the customer's responsibility to verify the identity of individuals assigned to an electronic record. Login to the system must occur by a named user before e-signature can be executed.
11.100(c) Can the user certify that the electronic signatures in their system are the legally binding equivalent to traditional handwritten signatures?	14 (a) Do electronic signatures have the same impact as hand-written signatures within the boundaries of the company?	User	It is the responsibility of the customer to manage this certification to the agency. In TrackWise, users are unable to complete registration without first confirming that they agree to an electronic signature certification.

Electronic Signatures – Non-Biometric

21 CFR Part 11	Annex 11	Responsible Party	TrackWise
11.200(a)(1) Is the signature made up of at least two components, such as an identification code and password?		Sparta	Signatures in TrackWise consist of a User ID and Password.

21 CFR Part 11	Annex 11	Responsible Party	TrackWise
11.200(a)(1)(i) When several signings are made during a continuous session, is the password executed at each signing? Note: Both components must be executed at the first signing of the session. 11.200(a)(1)(ii) If signings are not done in a continuous session, are both components of the electronic signature executed with each signing?		Sparta	The password is required at each signing. When a user initially signs into TrackWise, the first signing, both a user name and password are required. For non-continuous sessions, the user will be logged out of the application and be required to enter both the user name and password to log back into the system prior to performing additional electronic signatures.
11.200(a)(2) Are non-biometric signatures only used by their genuine owners?		User	It is the responsibility of the customer to ensure employees only use their own electronic signature.
11.200 (3) Would an attempt to falsify an electronic signature require the collaboration of at least two individuals? 11.200(b) Has it been shown that biometric electronic signatures can be used only by their genuine owner?		User	Customers need procedures that users do not divulge their electronic signature (e.g. password). Not Applicable.

Controls for Identification Codes and Passwords

21 CFR Part 11	Annex 11	Responsible Party	TrackWise
11.300(a) Are controls in place to maintain the uniqueness of each combined identification code and password, such that no two individuals can have the same combination of identification code and password?		Sparta	Yes, every user must have a unique identification code (user name).
11.300(b) Are controls in place to ensure that identification code and password issuances are periodically checked, recalled, or revised?	11 Are computerised systems periodically evaluated to confirm that they remain in a valid state? Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security, and validation status reports.	User	The customer is responsible for defining and executing a periodic review of user access.
11.300(c) Following loss management is there a procedure 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?	12.3 Is the creation, change and cancellation of access authorisations recorded?	User	It is the responsibility of the customer to establish procedures for disabling tokens, cards, or other devices.

21 CFR Part 11	Annex 11	Responsible Party	TrackWise
11.300(d) Are there safeguards in place 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?		User & Sparta	It is the responsibility of the customer to provide a procedure for reporting repeated or serious attempts at unauthorized use. TrackWise can be configured to lockout a user when a set number of login attempts in a single instance were unsuccessful. Admins can access which users have been locked out of the system due too many login attempts.
11.300(e) Is there 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?		User	It is the responsibility of the customer to establish procedures for managing tokens, cards, or other devices.

EU Annex 11 Control for which there is no Part 11 Equivalent

Annex 11	Responsible Party	TrackWise
1 Are decisions on the extent of validation and data integrity controls based on a justified and documented risk assessment?	User	Customers are responsible for decisions regarding validation and data integrity controls.
3.1 When third parties are used to provide, install, configure, integrate, validate, maintain, modify or retain the system, do formal agreements exist?	User & Sparta	Customers are responsible for developing and executing agreements with third parties. Sparta maintains formal contracts with all third parties utilized for staff augmentation purposes.
3.2 Are third parties audited?	User & Sparta	Customers are responsible for auditing any third parties they utilize. Sparta periodically audits all critical vendors.

Annex 11	Responsible Party	TrackWise
3.3 Is documentation from commercial off-the-shelf products reviewed to check that user requirements are fulfilled?	User	Customers are responsible for reviewing and accepting the Sparta Systems validation package.
3.4 Is quality system and audit information relating to third party suppliers or developers of software & implemented systems available to inspectors on request?	User	Information is available during audits of Sparta Systems.
4.3 Is an up to date listing of relevant systems and their GMP functionality 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, hardware and software pre-requisites and security measures is available.	User & Sparta	Customers are responsible for maintaining system lists and descriptions. Sparta maintains application architecture diagrams, security details, system requirements and specifications and a detailed integration architecture.
4.4 Do user requirement specifications describe the required functions of the system? Is URS based on documented risk assessment and GMP impact. Are User requirements traceable throughout the life-cycle?	User	User requirements are the responsibility of the using organization.
4.5 Was the system developed in accordance with an appropriate quality management system?	Sparta	Sparta Systems is ISO 9001:2015 certified.
4.6 For customized systems, what process is in place to ensure the formal assessment and reporting of quality and performance measures for the life-cycle stages of the system.	User & Sparta	Sparta Systems provides a TrackWise validation package. It is the responsibility of the customer to ensure a formal assessment is completed is they choose to customize TrackWise.
4.7 What evidence of test methods and scenarios are available? Were parameter limits, data limits and error handling considered? How are automated testing tools and test environments assessed for adequacy?	Sparta	A validation package is available for each release. Parameter limits, data limits, and error handling are considered during validation. Testing tools and environments use industry-leading tools whenever possible, and are otherwise reviewed for adequacy.
6 What accuracy checks are in place for critical data entered manually?	User	Critical data fields can be configured to require the use of a drop-down selection list.

Annex 11	Responsible Party	TrackWise
7.2 Are regular back-ups of relevant data done? How is the integrity and accuracy of data and the ability to restore data checked during validation and monitored periodically?	User	Data back-ups are the responsibility of the customer.
8.2 For records supporting batch release, are printouts available to indicate if any data was changed since original entry?		Not applicable.
13 Are all incidents reported and assessed? Is the root cause of critical incidents identified? Does the identified root cause form the basis of corrective and preventive actions?	User & Sparta	All product related incidents are brought to a weekly meeting where they are prioritized, severity noted, and effort is decided. All high severity incidents are investigated, root cause analysis completed, and if applicable, a corrective action is identified.
15 Does the system allow only qualified persons to certify the release of batches and clearly identify and record the person releasing or certifying the batches?		Not applicable.
16 What provisions are made to ensure continuity of support for critical processes in the event of a system breakdown? Is the time required to bring alternative arrangements into use based on risk and appropriate for the system and business process it supports? Are these arrangements adequately documented and tested?	Sparta	The customer is responsible for system uptime and redundancy and availability of back-ups.