The Impact of 21 CFR Part 11 on Product Development

Product development has become an increasingly critical factor in highly-regulated life sciences industries. Biotechnology, medical device, and pharmaceutical companies all rely heavily on validated and traceable product development systems, especially for high risk and complex products. For companies that choose to develop their own management and control of development assets are still subject to provisions of 21 CFR Part 11 from the Food and Drug Administration (FDA), which require extensive validation efforts and internal support costs. Streamlining processes and automating hand-offs during development and testing is not a trivial task, even with a document or quality control system.

FDA ruling 21 CFR Part 11 specifies how electronic records and electronic signatures can be used as a substitute for paper records and handwritten signatures. It is broadly applicable to electronic records that are central to the process of developing and manufacturing biotechnology, drugs, and medical devices. The goal of this paper is to educate product developers so they can understand the impact of this ruling and learn how to achieve compliance through the intelligent use of tools and good process.

What are electronic records?

According to the FDA, an "electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system." Not all electronic records are subject to 21 CFR Part 11, only those that are maintained in accordance with FDA published predicate rules.

These rulings, such as the Good Laboratory Practice (GLP) and Current Good Manufacturing Practice (CGMP), mandate what records must be maintained, what needs to be contained in the record, whether signatures are required and how long records must be maintained.

What is an electronic signature?

Electronic signatures are intended to be binding digital equivalents of handwritten signatures. The FDA states that an "electronic signature is a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature." It is important to note the FDA does not equate an electronic signature with a digital signature, such as those provided by commercial entities Verisign, Entrust, etc. FDA predicate rules specify which electronic records require signatures, electronic or otherwise. If signatures are necessary, and they are collected electronically, then compliance with 21 CFR Part 11 is mandatory.

How does the ruling impact product development?

To meet the requirements of 21 CFR Part 11, a product development project must follow repeatable processes with change tracking and sign off procedures. The intent of this ruling is to ensure there is a clear and irrefutable record of each and every change made during the product lifecycle. This otherwise cumbersome task can be made simpler using product development tools that are built with compliance in mind. When selecting these tools, you should look for the following:

- Access is limited to authorized users
- Records can only be updated by users with security access
- Timestamps are recorded for each and every change
- Changes are authenticated using electronic signatures
- Accurate change histories are maintained for all records
- Meets audit trail requirements
- Provides a configurable workflow for good repeatable processes
- Strong objective evidence is captured during testing
- Traceability throughout the entire lifecycle.
- Reporting capabilities

Fulfilling these requirements is straightforward with TestTrack, Seapine Software's product development management and change control tool. TestTrack is built for the task and offers an array of features that ease regulatory compliance and promote better decision making.

TestTrack helps organizations meet FDA requirements with a seamlessly integrated requirements, risk, test, and issue tracking system that supports robust electronic signature handling, traceability, and comprehensive audit trails.

21 CFR Part 11 Compliance Matrix

The following matrix provides an assessment of how TestTrack facilitates compliance with 21 CFR Part 11.

The term "Acknowledged" is used to answer portions where there is no notable action required on part of the software. This indicates the recommendation has been read and understood in the context presented. In some instances, a more defined response is also provided.

Any software that is used to comply with 21 CFR Part 11 is only an element of the solution. Compliance cannot be achieved by the tools alone. It is how the tools are configured, maintained, and used that determines whether an organization reaches its compliance goals. A well-defined process with strong rules for enforcing accountability greatly facilitates this end.

TestTrack can be implemented for management of electronic development records in lieu of traditional paper records and fully supports additional electronic signature verification during the change process. TestTrack supports electronic signatures by positively identifying the user through a unique username and password combination. This information is controlled and centrally managed via a license server. LDAP and Active Directory integration allows the administrator to use these technologies to replace/supplement the built-in user management.

21 CFR 11.1 – Scope	TestTrack Compliance
(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.	Acknowledged
(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.	Acknowledged
(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.	Acknowledged
(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with Sec. 11.2, unless paper records are specifically required.	Acknowledged
(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.	Acknowledged

21 CFR 11.2 – Implementation	TestTrack Compliance
(a) For records required to be maintained, but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.	Acknowledged
(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:	Acknowledged

21 CFR 11.2 – Implementation	TestTrack Compliance
(1) The requirements of this part are met; and	Acknowledged
(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.	Acknowledged

21 CFR 11.3 – Definitions	TestTrack Compliance
(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.	Acknowledged
(b) The following definitions of terms also apply to this part:	Acknowledged
(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).	Acknowledged
(2) Agency means the Food and Drug Administration.	Acknowledged
(3) Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.	Acknowledged
(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.	Acknowledged
(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified	Acknowledged
(6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.	Acknowledged
(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.	Acknowledged

21 CFR 11.3 – Definitions	TestTrack Compliance
(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate in writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.	Acknowledged
(9) Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.	Acknowledged

Subpart B – Electronic Records

The FDA distinguishes between open and closed systems. Closed systems are those where access is controlled by persons who are responsible for the content of electronic records on the system. Open systems are accessible by those who are not directly responsible for the electronic records on the system.

21 CFR 11.10 – Controls for Closed Systems	TestTrack Compliance
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.	TestTrack can be configured as a closed system with an audit trail. The organization can use the audit trail to discern between valid and invalid records. TestTrack maintains a distinct audit trail for this purpose and has the ability to verify theses records against any tampering. TestTrack also includes reports that greatly reduce the documentation for system validation.
(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.	TestTrack reports include who made changes, when they made them, and the type of change. Changes are date/timestamped. These reports, including full audit logs, can be distributed in paper or electronic form.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	The security within TestTrack gives complete control over which users can complete specified actions. The organization is ultimately responsible for backing up and protecting the records for their retention period.
(d) Limiting system access to authorized individuals.	TestTrack uses a set of rules based on security group settings that uniquely identifies each user from their username and password combination. The internal security settings determine the access and privileges of the logged in user.

21 CFR 11.10 – Controls for Closed Systems	TestTrack Compliance
(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.	TestTrack can be enabled to capture the full detail and history of all changes to records. Enhanced compliance rules and options can also be enabled during testing to help enforce stronger processes and data capture in testing. TestTrack maintains a distinct comprehensive audit trail that can be retained indefinitely and explicitly searched by date range, users, items, and modification sources and types.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	The ability to complete any given action is controlled at the security group level and is under the control of the administrator(s) to set what permissions are allowed to what users to make what changes at any given point in the process. The configurable workflow facilitates the process workflow that is appropriate for the record being managed. The history of actions completed within TestTrack contains timestamp information for when the action was completed and by what user, showing the sequence in which actions occurred. The organization is ultimately responsible for enforcing proper sequencing of steps and events. Additionally, enhanced compliance rules and options can be enabled during testing to help enforce stronger processes and data capture during test execution, even at the step level.
(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.	TestTrack uses a set of rules based on security group settings that uniquely identifies each user from their username and password combination. The internal security settings determine the access and privileges of the logged in user.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Within TestTrack no historical record is made until an action is completed (e.g., "Assign defect").
(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.	Access is controlled via security groups to those individuals deemed appropriate. The organization is ultimately responsible for this requirement, but Seapine offers both online and on-site training options.
(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.	The organization is ultimately responsible for this requirement, but TestTrack can be configured to use and present the exact organizational vernacular through a certification and testimony message whenever an electronic signature is used. You can also set the maximum attempts before logging out a user attempting to falsify a record without proper login and password information.
(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.	There is online help and documentation. Printed copies of documents and guides are available. The organization is ultimately responsible for this requirement.
(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	TestTrack maintains a distinct audit trail for this purpose, including an optional verbose log.

21 CFR 11.30 – Controls for Open Systems	TestTrack Compliance
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 Sec. 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.	TestTrack can be used as an open system or a closed system depending on the access to the server via an IP address and port. Through the use of the username and password combination and internal security groups the administrator can secure the system as required for compliance. Use of SoloSubmit, SoloBug, email import or any import method implicitly defines usage as an open system. This would mandate controls for open systems be applied.

21 CFR 11.50 – Signature Manifestations	TestTrack Compliance
(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;	The name of the signer is displayed and can be reported against.
(2) The date and time when the signature was executed; and	A date and timestamp are contained in the history and audit log.
(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	The completed action and process flow information is logged with who modified the record and when it was modified. Information about the change, as entered by the signer, is also captured and can be set as a required field.
(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.	TestTrack provides this record information identified in this section through the user interface (electronic display), as well as through a report (printout).
(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).	Acknowledged

21 CFR 11.70 – Signatures /Record Linking	TestTrack Compliance
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.	The history of any action performed in TestTrack is not modifiable and contains the details of the action taken as well as a timestamp and the user who performed the action. Each electronic signature is linked to the respective electronic record. Electronic signatures cannot be removed, copied, or compromised by ordinary means..

Subpart C – Electronic Signatures

21 CFR 11.100 – General Requirements	TestTrack Compliance
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	The unique username and password combination required by TestTrack ensures the user is authenticated when logging in. All records created by a user are permanently linked to the creator's unique username. The administrator can configure the system so that passwords cannot be reused.

21 CFR 11.100 – General Requirements	TestTrack Compliance
(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.	The administrator is responsible for verifying that each user entered into the system is properly identified before entering a unique username and password combination for said user. Administrators can set strong passwords rules in the Seapine License Server that are applied universally, including the ability to enforce a minimum password length, minimum number of letter characters, numeric characters, and minimum number of non-alphanumeric characters in a password. Passwords can be restricted so they cannot be set to the user's username, first name, or last name. Passwords can optionally expire in 'x' days. LDAP or Active Directory can be used instead of these features to centrally manage users. All records created by a user are permanently linked to the creator's unique username. The organization is ultimately responsible for this requirement.
(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.	The organization is ultimately responsible for this requirement. TestTrack provides and supports an additional certification and testimony message any time an electronic signature is required of a user, which is controlled and established by the administrator. As an added benefit, TestTrack can also require a signature of meaning or reason to be required.
(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.	The organization is ultimately responsible for this requirement.
(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.	The organization is ultimately responsible for this requirement. TestTrack provides and supports an additional certification and testimony message any time an electronic signature is required of a user, which is controlled and established by the administrator. As an added benefit, TestTrack can also require a signature of meaning or reason to be required

21 CFR 11.200 – Electronic Signature Components and Controls	TestTrack Compliance
(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.	TestTrack uses a username and password combination to identify the logged in User.
(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.	TestTrack requires the user to initiate a continuous period of controlled system access with a username and password combination. Each action the user performs within this period creates a historical record that contains information about the action and user. The username and password used at login identifies the user. The administrator can specify whether the password alone is sufficient for electronic signatures or if both the username and password are required.
(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.	TestTrack requires the user to initiate a continuous period of controlled system access with a username and password combination. Each action the user performs within this period creates a historical record that contains information about the action and user.
(2) Be used only by their genuine owners; and	The organization is ultimately responsible for this requirement.

21 CFR 11.200 – Electronic Signature Components and Controls	TestTrack Compliance
(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.	This is a procedural issue because the "Administrator" user has the ability to manage and maintain all users and passwords. The "Administrator" user can change any user's password if necessary. Unusual activity notifications, such as for failed log ins and direct connection attempts, can also be sent to the administrator or other organizational members through the License Server.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	The use of biometrics is not currently supported.

21 CFR 11.300 – Controls for Identification Codes/Passwords	TestTrack Compliance
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.	TestTrack uses a username and password to uniquely identify the person logged into the system. The password is not required by default but can be enforced. Usernames must be unique and are not case sensitive. All records created by a user are permanently linked to the user's unique username.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Administrators can set password rules, such as password aging, in the Seapine License Server that are applied universally. LDAP or Active Directory can also be used to centrally manage users.
(c) Following loss management procedures to electronically de-authorize 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.	TestTrack does not use tokens, cards, or other devices at this time.
(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.	TestTrack can be installed as a client/server application that is accessed through an IP address and port for additional security. Intruders would first have to have access to the network then to the specific server, IP address, and port. Security is further enhanced as users are validated with a unique username and password combination. In addition, before the user is logged in they must receive authorization from the license server. Failed login attempts are recorded. Administrators can set strong password rules in the Seapine License Server that are applied universally. LDAP or Active Directory can also be used to centrally manage users. Unusual activity notifications, such as for failed log ins and direct connection attempts, can also be sent to administrator or other organizational members through the License Server.
(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.	TestTrack does not use tokens, cards, or other devices at this time.

About Seapine for Life Sciences

Founded in 1995, Seapine Software is based in Mason, Ohio, with sales and support offices located in Europe, Asia-Pacific, and Africa. Hundreds of leading medical device, pharmaceutical, biotechnology, and clinical research organizations rely on Seapine to streamline their core development processes, drive innovation, and gain a competitive edge.

Learn more at life-sciences.seapine.com.