Scite line

Scite line Virtual Clinical Trials (VCT) 21 CFR Part 11 Compliance Whitepaper

Introduction

Research organizations are increasingly benefitting from the advantages of decentralized solutions. These companies must adhere to the regulatory requirements of United States (U.S.) Federal Regulation Title 21, Chapter 1, Part 11 (21 CFR Part 11) if using electronic records and electronic signatures in place of paper-based records to comply with FDA rules.

Many organizations are choosing Sciteline's Virtual Clinical Trial (VCT) product to digitize patient informed consent, patient reported outcomes and clinical assessment outcome processes. 21 CFR Part 11 requirements can be satisfied using VCT when it's properly configured to execute electronic signatures.

This paper presents an assessment of the technical features and the procedural controls that allow for the application of 21 CFR Part 11 compliant signatures using Sciteline's VCT product. The assessment focuses on how Sciteline's Virtual Clinical Trial (VCT) product and the research organization using VCT share responsibilities for achieving compliance.

Background

System Overview

Sciteline's Virtual Clinical Trial solution includes a cloud-based electronic signature service offered in a Software-as-a-Service (SaaS) model. The configuration of the service, with settings needed for an organizations business process, is managed by Sciteline's onboarding team in working with the Client.

Licensed users are added to a Virtual Clinical Trial site for the study. The users will receive an automated email requesting the users to activate their account. Active users are authorized to use the electronic signature functionality based on the privileges assigned to them during trial set up. An authorized user (i.e. individual in research team) may also assign a document in VCT to a study participant for review and signature. Authorized users can access and sign the document from desktop web and mobile native apps (i.e. Android and iOS). Valid credentials are required to authenticate the signing user, allowing for the individual's signature to be applied to the document. Once all requested signatures have been applied to a document, the research team and participant can access the signed document via VCT. The signed documents are available in PDF format and can be retrieved by the Client to manage their electronic record retention policies. The audit trail for the electronic signature records can also be exported from the platform.

Transactional data (including original documents, audit trial and final signed PDF document) are securely stored within the data layer managed by Sciteline. The infrastructure resides in data centre managed by cloud service providers.

21 CFR Part 11 Overview

21 CFR Part 11 specifies the requirements for electronic document and signature submissions to the U.S. Food and Drug Administration (FDA). The law defines the criteria for which the FDA 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*."

Under 21 CFR Part 11, a system is described as either an open or closed system. Sciteline's CFR Part 11 module has been designed to support an "open system", meaning that it is an environment in which system access is not controlled by the individuals/organization who are responsible for the content of the electronic records in the system. In comparison, a closed system is one which the system access is controlled by the individuals who are responsible for the content of the electronic records in the system.

The system has implemented controls and procedures to ensure the authenticity, integrity and confidentiality of the electronic records, as part of meeting the requirements under 21 CFR Part 11. The client is responsible for validating that the system meets the needs for their intended use and applicable regulatory requirements. In addition, the client has a shared responsibility for achieving compliance.

Conformance with 21 CFR Part 11 Regulations

In this section, the compliance requirements of 21 CFR Part 11 are assessed to determine how Sciteline's Virtual Clinical Trial product conforms with the regulations. In addition to Sciteline's technical controls, the Client is responsible for defining and implementing processes to ensure that VCT is used in a controlled manner that meets the requirement of 21 CFR Part 11. During trial set up, the Client is responsible for selecting the appropriate signature functionality to meet their business process requirements, for coordinating with Sciteline to configure the product to the trial workflow, and for ensuring the supporting processes are in place to govern the use of VCT in a controlled manner.

21 CFR 11 Subpart B

Section 11.10 Controls for closed systems
What the law requires
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:

Section 11.10(a)
What the law requires
Validation of systems to ensure accuracy, reliability, consistent intended performance and ability to discern invalid or altered records.

How VCT Complies

Sciteline can audit all data and server related events, inclusive of the operating system and database.

Sciteline employs a number of controls during the software development lifecycle such as peer code reviews and multiple layers testing including functional, integration and unit to ensure issues are identified before being deployed into production. All deployments go through our Change Control Procedures and must be formally approved before it is deployed into our production environment.

Client's responsibilities

A client organization is responsible for:

- Validating their computer systems used to support the regulated activities.
- Identifying authorized end users who would have access to the system.
- Validating the installation of the system.

Section 11.10(b)

What the law requires

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.

How VCT Complies

The signed electronic records and its audit record can be generated or exported and can be retrieved by the client within the application.

Client's responsibilities

A client organization is responsible for documenting and defining the process for retaining signed records.

Section 11.10(c)

What the law requires

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

How VCT Complies

All data is encrypted and is stored securely. Throughout the duration of the agreement with the client, each signed electronic document and its audit record can be retrieved by the client within the application.

Client's responsibilities

A client organization is responsible to ensure the record retention period outlined in the contract is sufficient for the purposes of the trial.

Section 11.10(d)

What the law requires

Limiting system access to authorized individuals.

How VCT Complies

Access to the system is strictly governed by role-based permissions assigned within the system by authorized administrators. Individuals are required to change their account passwords on a regular basis, and unsuccessful login attempts will result in account lockout.

Client's responsibilities

The client organization is responsible for documenting user access procedures that outline who may be added as a signer for the purposes of their study.

Section 11.10(e)

What the law requires

Use of secure, computer-generated, timestamped 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.

How VCT Complies

Audit logs are maintained for all activity within the application, inclusive of date and timestamps, identity of a user. User Audit logs are kept in a database and stored in accordance with Sciteline's data retention policy. The database is backed up regularly and are kept in object storage with write ahead logs to ensure point-in-time recovery. Admin activity and system event audit logs are securely kept in our cloud hosting provider's platform.

Client's responsibilities

The client organization is responsible for defining and document the process for retaining and archiving signed records and audit trails.

Section 11.10(f)

What the law requires

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

How VCT Complies

Client's responsibilities

System logic is embedded into user interfaces and process flows to enforce sequence-based workflows, where signatures are applied in a predefined order. Users cannot create, delete or modify records in a particular step that is out of order in the overall sequence and after submission.

The client organization is responsible for documenting the process for using the Sciteline signing module which should consideration for mandatory signature sequences.

Section 11.10(g)

What the law requires

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.

How VCT Complies

Users are authenticated by a unique username and password before they are able to access any system features. The product uses role-based access controls (RBAC) to assign abilities to specific features and functionality (such as the ability to create or modify assessment schedules). Sciteline utilizes segregation of duties for operational job responsibilities. Identity and access management (IAM) permissions are utilized to ensure individuals only have access to what they need to perform their job.

Client's responsibilities

The client organization is responsible for defining and document the process for:

- Defining the process for user access management, include specifying the criteria for providing and revoking user access.
- Defining the processes that deter record and signature falsification.

Section 11.10(h)

What the law requires

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

How VCT Complies

The source of records can only be a terminal device that is executing Sciteline software and operated by a user that has provided authenticated credentials to an authorized user account.

Client's responsibilities

If a device check is deemed necessary, a client organization is responsible for:

- Determining whether implementing device checks are required based

---

A device check is necessary when only certain devices have been designated as a legitimate source of data inputs or commands. In these circumstances the checks would be

implemented to determine if the data or command source was authorized.

on regulatory requirements and assessment of risk.

- Establishing the process that defines which devices are authorized to provide data or operational instructions.

Section 11.10(i)

What the law requires

Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training and experience to perform their assigned tasks

---

How VCT Complies

Sciteline staff must complete privacy and security training upon onboarding and on an annual basis. Staff that may be required to have access to data as part of their job responsibilities must have successfully passed a criminal background check, and receive approval from Sciteline's designated Privacy Officer

Client's responsibilities

The client organization is responsible for:

- Defining the process for their end user training.
- Ensure that proper training is provided to the end user prior to using the system.
- Establishing the process for employing the use of electronic signatures, including implementing provisions to ensure that signers understand that their electronic signature is legally binding.

Section 11.10(j)

What the law requires

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.

How VCT Complies

Client's responsibilities

N/A	The client organization is responsible for establishing the process governing the use of electronic signatures. This includes implementing procedures to hold individuals accountable and responsible for actions originating under or authorized by their electronic signatures.

Section 11.10(k)(1)

What the law requires

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.

How VCT Complies	Client's responsibilities
Sciteline has procedures in place to ensure control for systems documentation can only be accessed, changed or distributed by Sciteline staff. Standard Operating Procedures are accessible to relevant users.	The client organization using the system as part of a regulated process is responsible for establishing the process governing the controlled documentation management to ensure that they have correct and updated versions of standard operating and maintenance procedures.

Section 11.10(k)(2)

What the law requires

Use of appropriate controls over systems documentation including:

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

How VCT Complies	Client's responsibilities
Standard Operating Procedures for change control exist throughout the software development lifecycle. All code is developed with full source control and code revisioning. All issue management is documented in an organizational tracking system. Any major system upgrades are fully documented, and clients are notified in advance.	The client organization using the system as part of a regulated process is responsible for establishing the process governing the controlled documentation management to ensure that the have correct and updated versions of standard operating and maintenance procedures.

21 CFR 11

Section 11.3

What the law requires

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.

How VCT Complies

VCT encrypts all electronic records on our servers at rest and in transit. Security certificates and ciphers are periodically reviewed by the security team and any issues identified are corrected in a timely manner to protect the confidentiality and integrity of the data.

Client's responsibilities

The client organization is responsible for implementation of the security controls/measures and procedures applied to the computer systems or terminals in which end users are using to access the VCT system

Section 11.50

What the law requires

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.

(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).

How VCT Complies

When electronic records are signed, the system records the following items as part of the electronic signing process:

- Date and time stamp
- User ID and full name of the signer(s)
- Meaning associated with the signature (e.g. end user has signed consent form)

The electronic record includes the signature component, which is stored in the same database. The system allows the display of the electronic signature as described in 11.50 (a) either on the screen or in a report.

Client's responsibilities

The client organization is responsible for establishing the process governing the application of electronic signatures, including the required purposes for each signature.

Section 11.70

What the law requires

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.

How VCT Complies

The electronic signature is stored in the same data file or document that is signed thus directly linking the electronic signatures to the electronic record.

Client's responsibilities

N/A

---

21 CFR 11 Subpart C

Section 11.100(a)

What the law requires

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

---

How VCT Complies
All user identification and password combinations are unique. The system does not permit these combinations to be reused or reassigned by anyone else.

Client's responsibilities
The client organization is responsible for establishing a processing for:

- Identifying authorized end users and assigning access rights prior to provisioning access into the system.
- Ensuring no two end users are associated to the same email address.

Section 11.100(b)

What the law requires

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.

How VCT Complies
N/A

Client's responsibilities
The client organization is responsible in identifying authorized end users and assigning access rights prior to provisioning access into the system.

Section 11.100(c)

What the law requires

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.

How VCT Complies
N/A

Client's responsibilities
The client organization is responsible for submitting a certification to the FDA that the use of electronic signatures in their system is intended to be the legally

binding equivalent of traditional handwritten signatures.

Section 11.200(a)

What the law requires

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.

How VCT Complies

The system requires two components for authorization and electronic signatures, the user identification and password. The system distinguishes between an electronic signature assigned and linked to an electronic record, and an authorization for controlled system access.

All signing in the software requires the end user to enter the person of the individual who is logged in to the session at the time of system use.

Each signer must identify themselves with a unique user ID and password, irrespective of the type of signature requested. A series of signings during a single, continuous session will require the user to enter their two components for authorization.

Client's responsibilities

N/A

Section 11.200(a)

What the law requires

Electronic signatures that are not based upon biometrics shall:

(2) Be used only by their genuine owners; and

How VCT Complies

N/A

Client's responsibilities

The client organizations are responsible for:

- Identifying authorized end users that will be using the system and providing detaisl to Sciteline for account creation.
- Ensuring that no two end users are associated to one email address.
- Implement appropriate procedures and policies to prohibit the sharing of end user credentials.

Section 11.200(a)

What the law requires

Electronic signatures that are not based upon biometrics shall:

(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.

How VCT Complies

N/A

Client's responsibilities

The client organizations are responsible for implementing appropriate procedures and policies to prohibit the sharing of end user credentials.

Section 11.200(b)

What the law requires

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

How VCT Complies

Not applicable – the system does not currently support signatures based on biometrics.

Client's responsibilities

N/A

Section 11.300(a)

What the law requires

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: Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

How VCT Complies

Every combination of user identification and password is unique.

The system does not permit reusing or reassigning user names.

Client's responsibilities

The client organization is responsible for:

- Ensuring that no two end users are associated to one email address.
- Implement appropriate procedures and policies to prohibit the sharing of end user credentials.

Section 11.300(b)

What the law requires

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

How VCT Complies

The software supports password aging and minimum password length and prevents the

Client's responsibilities

The client organization is responsible to setup and maintain password settings in alignment with compliance needs.

---

reuse of a configurable number of prior passwords.

Section 11.300(c)

What the law requires

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.

How VCT Complies

If an end user loses or forgets a password, end users are instructed to call our technical support services to deactivate and/or reset the password.

Client's responsibilities

The client organization is responsible for documenting and defining policies for handling lost, stolen, missing or compromised passwords of their end users.

Section 11.300(d)

What the law requires

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.

How VCT Complies

Sciteline has transaction safeguards to prevent the unauthorized use of passwords. Sciteline also has rate limits and account lockout policies to prevent third party attempts to brute force credentials.

Client's responsibilities

N/A

Section 11.300(e)

What the law requires

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.

How VCT Complies

Not applicable -Sciteline's system does not employ the use of codes generated by tokens or devices in our application.

Client's responsibilities

The client organization is responsible for informing Sciteline of any specific requirements they need to comply with their regulatory purposes.

About Sciteline

Sciteline combines creative thinking, innovation and cross industry leadership experience to develop decentralized trial solutions to help solve some of Canada's most challenging issues in clinical research. Our mission is to accelerate the generation of new knowledge by enabling researchers to achieve their best work while connecting them with a diverse population of patients. We believe that by reducing the patient burden by changing the status quo, we can lower the cost of delivering new drugs and medical devices to patients.

Connect

To learn more about Sciteline's products and services, please visit **www.Sciteline.com**

Subscribe

To receive upcoming thought leadership publications and articles please follow our Linkedin. To subscribe to our blog, please visit **www.Sciteline.com**

Disclaimer:

This document was created based on Sciteline's interpretation of the regulation. This document does not constitute legal or professional advice. The software along with the electronic signature capabilities can be used together with appropriate controls and procedures implemented by our clients, in accordance with FDA-compliant processes. Each client is responsible to perform their own due diligence based on internal processes.

Information about 21 CFR Part 11

For further information about the requirements of 21 CFR Part 11, please see www.fda.gov.