telemedicine technologies

Trusted information systems for health professionals

CleanWeb™

Integrated solution for the electronic management of clinical trials
From eCRF design to database lock

FDA 21 CFR part 11
Compliance analysis

Reference	*CW2-FDA10/2010*
Version	*1*
Revision	*0*
Date	*November 2012*

Telemedicine Technologies S.A.S.
102-104, avenue Edouard Vaillant – 92100 Boulogne-Billancourt - France
Tel.: (33) 1 55 20 08 00 - Fax.: (33) 1 49 10 06 52 - E-mail : contact@tentelemed.com - WEB : http ://www.tentelemed.com
Société par actions simplifiée au capital de 829 528 Euros - R.C.S. Nanterre 429 849 318 - TVA : FR90429849318
Société Générale - Banque 30003 - Guichet 03392 - Compte 00020262063 / 19

Table of content

Foreword

This document has been produced by TELEMEDICINE TECHNOLOGIES acting in its capacity as the editor of CleanWEB™, an integrated solution for the electronic management of clinical trials.

The purpose is to present an analysis of the compliance of the CleanWEB™ software solution with U.S. Food and Drug Administration regulation 21 CFR Part 11.

This regulation is in effect since 1997 and requires that computerized systems include automated technical controls to assure that electronic records maintain security and data integrity and can be subject to audits and inspection as well as paper records, and to ensure that electronic signatures meet standards that allow them to have the same legal bearing as traditional handwritten signatures

This document features the following presentation conventions: each section begins by quoting the corresponding 21 CRF Part 11 regulation section (italicized text on a grey background) followed by a description of the manner in which this is addressed by CleanWEB™ (in blue).

This document is designed to help customers achieve risk based, GAMP-5 compliant system validation. TELEMEDICINE TECHNOLOGIES also proposes support services aimed to lower the cost of validation and reduce the time that said validation takes.

Applicable and reference documents

- FDA 21 CFR Part 11. Electronic Records; Electronic Signatures; Final Rule Electronic Submissions; Establishment of Public Docket; Notice. (March 1997)
- Guidance for Industry Part 11, Electronic Records; Electronic Signatures — Scope and Application (August 2003)
- Guidance for Industry Computerized Systems Used in Clinical Investigations (May 2007)

These documents can be downloaded from the web site of the FDA at:

http://www.fda.gov/RegulatoryInformation/default.htm

Partie B - Electronic Records

Section 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 confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine.

CleanWEB™ implements all processes to automatically ensure that electronic records are properly identified, secured, versioned and that all changes are tracked.

CleanWEB™ protects the confidentiality, integrity, authenticity, availability, and non-repudiation of electronic records and actions undertaken through a number of means. Authentication is used to uniquely identify users and to indicate the user(s) responsible for the creation, modification, deletion and signature of electronic records.

CleanWEB™ provides powerful tools to enable mandated administrators to grant users with appropriate access rights specific to each accessible study and befitting their role (investigator, clinical research nurse or assistant, data manager, etc…). Administrators can thus grant or deny users the ability to view, print, create, modify, or delete records. Access control is granular, enabling the configuration of the aforementioned access controls at all levels, from the individual records, to entire forms or the complete eCRF, as well as investigation centres.

When a record is stored by the system, a secure hashing algorithm creates a unique signature key by means of an electronic certificate. Any subsequent change to the record will trigger a comparison with the stored signature key. The failure of this comparison for a given record indicates a lack of integrity.

The system's audit trail module further protects records by logging all change-inducing activities, and protects against repudiation by logging all system activities and identifying the users who executed them.

Section 11.10(a) - Validation

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

As the editor of the CleanWEB™ software solution, TELEMEDICINE TECHNOLOGIES ensures that all associated activities, including software design, development and testing, are performed according to methodologies which ensure compliance with all applicable regulations including 21 CFR Part 11. This is achieved on one hand by utilizing industry-standard system development lifecycle methodologies, software engineering and quality assurance practices, configuration management practices, standardized methodologies for development testing, formal acceptance testing, and release management, and on the other hand by incorporating the technical security and Part 11 checks required for successful validation into our software.

TELEMEDICINE TECHNOLOGIES implements a validation policy documented in standard operating procedures which apply to the whole field of its activities in clinical research. This includes software development, secure hosting services and technical support, as well as eCRF design and management services. The title “Clinical Research” refers to all activities involved in biomedical research, epidemiology, post marketing studies or patient registries.

All applicable regulations (US, EU, international) are taken into account: ICH E6-E9, ICH Q9-Q10, 21 CFR part 11, GCP, European Commission Directive 2001/20/EC / Directive 2005/28/EC, Annex 11, cGMP.

GAMP-5 methodology is applied.

Customers who use CleanWEB™ must verify this compliance and TELEMEDICINE TECHNOLOGIES provides said customers with the tools required to perform and document their verification, either by means of audits and inspection, or by providing an appropriate verification environment.

Additionally, Customers who run CleanWEB™ within their own technical and operational environment must ensure compliance of their particular set-up with 21 CFR Part 11 requirements.

To this end, the Customer shall perform activities that result in documented specifications and evidence showing, at a minimum:

- How the system will be used
- How it will be configured
- How it will be deployed
- That it was installed successfully
- That, within this particular environment, it functions correctly and properly automates the regulated processes and records.

TELEMEDICINE TECHNOLOGIES delivers support services to help customers achieve risk based, GAMP-5 compliant system validation, to lower the cost of validation and reduce the time said validation takes.

Section 11.10(b) - Copies of Records

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.

If it is desired by the customer, mandated system administrators can grant inspectors / auditors with view-only access to system records. The customer also has the capacity to make copies of records in both native and PDF formats. Native formats can be exploited by most off-the-shelf software (EXCEL, SPSS, SAS, etc…). Such copies may or may not include the complete audit trail attached to the exported records.

Section 11.10(c) - Protection of Records

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

The protection of records is described in section 11.10 above. In addition, record metadata contains timestamps that are included in all copies of reports generated by the system and from which the expiration date of the record can easily be derived.

CleanWEB™ also provides an automated function to alert the mandated administrators that a given record has expired and that manual action is required.

Section 11.10(d) – System Access

Limiting system access to authorized individuals.

This point is also introduced in section 11.10 above.

CleanWEB™ limits system access to authorized individuals through user authentication (via access codes: Identification Code and Password), and limits authorized users to only the approved activities and record access granted to their respective roles.

Section 11.10(e) – Audit Trails

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.

CleanWEB™ is protected by a secure, computer-generated audit trail that records all user actions and all changes to records so that the record content prior to the change can be reconstructed if need be.

Audit trail data cannot be modified or deleted. The audit trail can be viewed online at the level of each data record, visit or eCRF. It also can be included in the overall data extraction (copy of all records).

Each entry in the audit trail includes the identification of the user responsible for the action or change, a timestamp, as well as all metadata necessary to reconstruct previous record state. Timestamps are delivered by the server clock, regardless of the time zone of the user in question. The server is synchronized with an online time delivery service.

Section 11.10(f) – Sequencing of Events

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

CleanWEB™ implements a series of sequenced workflows for instance for data monitoring and data validation processes. Users are constrained to execute such workflows within the permitted sequence.

Section 11.10(g) – Authority Checks

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

CleanWEB™ implements a highly granular access rights system, as discussed in section 11.10 above. Access to the system is controlled by an authentication process based on access codes (Identification code and password). Identification codes are unique within the system and are associated with profiles (composed of a set of access rights). This enables CleanWEB™ to control with extreme precision the authorizations assigned to each user or group of users.

This access rights management system enables one to (a) control access to records according to the type of operation performed (read, write, delete and administer), (b) define the records upon which the user can intervene, and (c) grant or deny access to the activities for which users possess the appropriate permissions. These permissions can be granted via user roles in a role-based security mode and can be further customized at the user account level.

For instance, workflow steps can be configured so that only individuals with certain roles or permissions can execute the steps in question.

Section 11.10(h) – Device Checks

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

This is not applicable for this compliance analysis. Any type of terminal can be used to access CleanWEB™, provided that the user has been provided with access codes and can successfully complete the authentication process.

Section 11.10(i) – Training

Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

This is not applicable for this compliance analysis. This issue involves technical and procedural controls that must be implemented by the customer.

However, and depending on the roles of the targeted users, TELEMEDICINE TECHNOLOGIES proposes training programs tailored to these roles such as eCRF design, CTMS functionalities, EDC, data management, monitoring, etc. Training documentation and certificates are delivered to participants.

CleanWEB™ software is delivered along with all the available user guides as well as a training program for the customer's personnel in charge of eCRF design, data entry or records validation. Such training can also be performed by trainers within the customer's organisation following an initial training course delivered by TELEMEDICINE TECHNOLOGIES.

The qualifications of the staff members of TELEMEDICINE TECHNOLOGIES who contribute to the various services provided by the company in the field of clinical research are fully documented. Curriculum Vitae and pertinent training certificates are included in the audit file of the company.

Section 11.10(j) – Electronic Signature Accountability

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.

This issue is not applicable for this compliance analysis as it involves technical and procedural controls that must be implemented by the customer.

Section 11.10(k) – Control of System Documentation

Use of appropriate controls over systems documentation including:
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

This issue is not applicable for this compliance analysis as it involves technical and procedural controls that must be implemented by the customer.

Section 11.30 – Controls for Open Systems

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

CleanWEB™ is based on «Client/Server» architecture. Secure HTTP (HTTPS) and Secure Socket Layer (SSL) protocols are used to encrypt communications between the client workstation and the server. User sessions and records are therefore protected from unauthorized access.

CleanWEB™ can also be accessed via encrypted virtual private network (VPN) tunnels.

Partie C – Electronic Signatures

Section 11.50(a) – Content of Signature Manifestation

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.

The signature as implemented by CleanWEB™ contains the user name, the date and time of the signature, and the basis or motive of the signature.

Because this is an electronic signature, any changes made to a given electronic record after it has been signed can be detected.

Section 11.50(b) – Control and Display of Signature Manifestation

The items identified in 11.50(a) 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).

Users can display the signature information in the user interface of CleanWEB™. Signed records can be rendered by CleanWEB™ as secure PDF versions of the original document. The signature information appears on both electronic and printed versions of the signed rendered PDF document.

Section 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.

Within CleanWEB™, an electronic signature is linked to its associated electronic records as follows:

- Record metadata contains the signature status. When the record in question is signed, this metadata also contains the unique identifier of the attached signature record.
- CleanWEB™ enables publishing of a rendered PDF version of the record which contains the manifestation of the electronic signature, which in turn allows signed records used outside of the system to maintain the signature/record link.
- CleanWEB™ maintains an audit trail which indicates whether a given record has been signed and, in the case where a signature has occurred, contains the ID of the user responsible for the signature and the date and time at which said signature was applied to the electronic record.

Section 11.100 – General Requirements

Section 11.100(a) – Uniqueness of Signatures

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

Activation of the signature is controlled by the access codes that have been allocated individually to each user of the system.

CleanWEB™ ensures uniqueness of Identification codes in the system: 2 different user accounts cannot have the same Identification Code. This control is implemented both at the database and application levels.

Deletion of user account data is not allowed to avoid that Identification Codes be reallocated.

Section 11.100(b) – Identification of Signers

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.

This is not applicable for this compliance analysis as it involves technical and procedural controls that must be implemented by the customer.

Section 11.100(c) – Equivalence to Handwritten Signatures

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.

This is not applicable for this compliance analysis as it involves technical and procedural controls that must be implemented by the customer.

Section 11.200 – Electronic Signature Components and Controls

Section 11.200(a) – Non-Biometric Signatures

Electronic signatures that are not based upon biometrics shall employ at least two distinct identification components such as an identification code and password, shall be used only by their genuine owners; and shall 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.

Both a user's identification code and password are required in order for said user to be authenticated at the system login and when carrying out electronic signatures. Passwords are protected so that anyone other than the genuine owner would need to collaborate with either the original owner or the application administrator.

CleanWEB™ protects against “brute force” attempts at unauthorized password use by disabling accounts for several minutes following 3 consecutive unsuccessful attempts and reporting these to the system administrator.

Section 11.200(a)(1) – Series of Non-Biometric Signings

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.
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.

Access to the electronic signature is only possible for authenticated users, having entered their access codes (Identification code + password).

CleanWEB™ authorizes authenticated users to perform series of signatures during a single user session. Upon each signature, the user must enter his/her password to ensure that the individual performing the signature is indeed the individual associated with the user account and thus the signature. CleanWEB™ also reminds the user the purpose of signature and good practice rules.

Section 11.200(b) – Biometric Signatures

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

This is not applicable for this compliance analysis as this issue involves technical and procedural controls that must be implemented by the customer.

Section 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.

Identification codes and passwords must contain a minimum of 8 characters.

Passwords must include uppercase and lowercase letters as well as numbers and the following special characters : ! ? $ % ( ) _ + - [ ] { } : ; @ § # < > / . Passwords cannot be identical to the Identification code to which they are associated.

To ensure complete access code integrity, the Customer shall also implement procedural controls: for instance to ensure that two users do not share the same access code.

When appropriate, for instance upon delivering access codes to a new user or during the signature of an electronic record, the CleanWEB™ user interface reminds the user of his/her responsibilities regarding access codes and their obligation not to share these with other users.

Section 11.300(a) – Uniqueness of Identification Code / Password

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

CleanWEB™ does not authorize the creation of two or more users with the same Identification code. This check is implemented both at the database and application levels. When attempting to create a user account with an Identification code which is already allocated to a previously registered account, an error message is displayed. The administrator is then prompted to enter a different Identification code to complete user account registration.

Section 11.300(b) – Password Management

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

The first password allocated to a user account is generated automatically by CleanWEB™ at the point of account activation. CleanWEB™ uses a secure hashing algorithm to create a non-reversible encrypted password key. Only this key is stored in the database and therefore the actual user password is never displayed in the user interface. Upon receiving their access codes, users are reminded of their responsibilities and of their obligation not to share these access codes with others. Upon logging in for the first time, the user is prompted to change this initial password. This step is obligatory and thus cannot be skipped.

Additionally, CleanWEB™ makes it mandatory to regularly change passwords. The frequency of these changes is configured at the level of the server. The most commonly used frequency is 3 months.

The last 3 passwords associated with a user account cannot be reused and, as previously mentioned passwords cannot be identical to the Identification Code. Passwords have to be compliant with previously mentioned strength criteria which exclude the use of common words.

For perfect compliance with this requirement, the Customer shall also implement appropriate standard operating procedures.

Section 11.300(c) – Device Loss Management

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 r permanent replacements using suitable, rigorous controls.

This issue is not applicable for this compliance analysis as it involves technical and procedural controls that must be implemented by the customer.

Section 11.300(d) – Transaction Safeguards

Use of transactions 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 of the system security unit, as appropriate, to organizational management.

CleanWEB™ detects unauthorized login attempts with brute force protection as previously mentioned in this document.

This also requires a procedural control that must be implemented by the customer.

Section 11.300(e) – Device Testing

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.

This issue is not applicable for this compliance analysis as it involves technical and procedural controls that must be implemented by the customer.

Requests for information shall be addressed at:

TELEMEDICINE TECHNOLOGIES S.A.S., 102-104 avenue Edouard Vaillant - 92 100 Boulogne-Billancourt – France
Clinical Trials Department – Telephone: +33 1 55 20 08 00 - 07 – Email: clinicaltrials@tentelemed.com
http://www.tentelemed.com