telemedicine technologies

Trusted information systems for health professionals

CleanWeb

The integrated solution for the electronic management of clinical trials
From the design of the electronic Case Report Forms to database lock

Security and Patient Privacy Handling
Key features & responsibilities

Reference	*CW-202-COM*
Version	*1*
Revision	*0*
Date	*July 2015*

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 871 596.24 Euros - R.C.S. Nanterre 429 849 318 - TVA : FR90429849318
Société Générale - Banque 30003 - Guichet 03392 - Compte 00020262063 / 19

Table of content

Purpose

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 outline how patient privacy is protected when nominative patient data are used in the eCRF as well as to describe the conditions under which security, continuity of service, contractual and legal responsibilities, data ownership and long term archiving are handled.

Quality Management & Certifications

21 CFR Part 11 compliance

CleanWEB™ is compliant with the US Food and Drug Administration regulation 21 CFR Part 11 on electronic records. For additional information on this compliance, please refer to the following document released by TELEMEDICINE:

FDA 21 CFR Part 1 – Compliance analysis, (Ref.: CW_compliance_21CRF11_V7 - UK.pdf)

ISO 9001:2008 Certification

All activities related to

Development and provision of collaborative software for clinical research and epidemiology

Have been audited and are certified as complying with the requirements of standard ISO 9001:2008 by Bureau Veritas Certification (certificate n°FR020752-1 dated February 2015).

Information System Validation, audits

CleanWEB is a subject to a Validation Process based on state-of-the-art GAMP 5 methodology[1]. Information System Validation is key for the management of security, as it ensures that the software effectively does what it has been designed to do.

This process is documented and ruled by dedicated Standard Operating Procedures (SOPs).

Audits

Customers are entitled to audit on site, all quality management and information system validation documentation at any time with prior 2 weeks' notice.

Please contact our ***Quality Assurance & Production Manager***.

Key security features

Security is the result of a whole set of processes and technical features covering all of the production chain, including software validation and compliance features as outlined in the previous sections.

Key security features can be outlined as follows:

- Except if explicitly otherwise specified in the Service Contract, the server is hosted in a dedicated virtualized environment (Virtual Datacenter) provided by TELEMEDICINE and dedicated to the exclusive usage of the Customer.
- The General Hosting Conditions are detailed in Appendix 1 hereto.
- Transmissions over Internet are HTTPS encrypted using a dedicated SSL certificate duly authorized and registered for the server of the Customer.
- The data center services are purchased from a specialized provider subject to ISO 27001 certification for security management:

[1] Good Automated Manufacturing Practice

- Physical access to the data center is restricted and controlled. Protection against attempts of intrusion by non-authorized personnel is ensured by a number of systems and processes: access protected by armor-plated doors, electronic badges, digital fingerprint analyzers and human verifications.
- All infrastructure is redounded with very high level of continuity of service.
- TELEMEDICINE is the sole and exclusive administrator of the Virtual Datacenter[2]. The data center provider only intervenes for the maintenance of the Infrastructure. Physical access to the site hosting the Infrastructure is authorized only to mandated staff of the service provider.

- The Service is based on an Infrastructure including a Primary Site and a Secondary Site located on different geographical areas. All servers are located in a private area.
- Daily automatic data (files, databases) backups are performed both on the Primary Site and the distant Secondary Site. These backups are incremental and cover the last 5 months of activity.
- A Firewall system managed by mandated TELEMEDICINE staff ensures protection from non-authorized remote access.
- Routine maintenance operations are performed remotely from the authorized workstations located in the TELEMEDICINE premises and a continuous monitoring of security conditions is performed by TELEMEDICINE's staff in charge of Service Management.

Continuity of Service

TELEMEDICINE is committed to make its best efforts to minimize Service downtime: Continuity of Service ratio is higher than 99.5%.

For details, please refer to the Appendix 1 hereto entitled General Hosting Conditions.

Handling Personal Patient Data

The name and first name of a patient, his home address, personal telephone number or email address are "Personal Patient Data" subject to special protection regulations.

It is the responsibility of the owner of the collected data to justify why such identifying data need to be collected and they shall only be collected for the usage that requires their collection. Whatever such requirements, CleanWEB provides the necessary features to ensure the adequate management of such data.

CleanWEB is compliant with the most demanding requirements as specified by the French CNIL (Commission Nationale Informatique et Libertés):

- In the database where they are persisted and stored, Personal Data are encrypted.
- This database is separate from the CRF database.
- The access rights management system of CleanWEB based on User Authentication with access codes, enables to fully control the access to the Patient Data and allow such access only to relevant personnel.
- Except if otherwise specifically required and documented by the Customer, such access is only granted to personnel of the investigational site where the patient is enrolled and CleanWEB provides all features to ensure this requirement.
- For other personnel such as CRA, Data Manager, Project Manager, Principal Investigator etc…, the corresponding data fields may be displayed in the user interface but their value will be set to *****. The term "User Interface" shall also include all dashboards and all printable material that may be generated using CleanWEB.
- Personal Patient Data cannot be included in the extraction files.
- CleanWEB provides features to fully delete such data is the patient so wishes.

[2] Refer to General Hosting Conditions in appendix for more details on virtualized environments

Liability

TELEMEDICINE implements all required processes and technical means to ensure that the provided Service based on the usage of its CleanWEB software is effectively delivered according to specifications and contractual conditions.

TELEMEDICINE shall only be liable for all issues in direct relation with the delivery of the Contracted Service.

It is reminded that the Usage of the Service delivered by TELEMEDICINE remains under the exclusive Responsibility of the Customer and therefore the Customer is the only liable entity in case of misuse.

TELEMEDICINE can in no way be prosecuted or held liable for any breach on the good clinical practice that fall under the Responsibility of the Customer.

It is reminded that overall Security is the result of the whole chain of measures at operational and technical levels. As examples, TELEMEDICINE cannot bear any liability in case the informed consent of a patient is not obtained, or if an investigator discloses his access codes or Personal Patient Data to a non-authorized third party, or in cases where the Customer may have provided inappropriate specifications to TELEMEDICINE.

Ownership of data & related capacities

The data collected by means of CleanWEB remain the exclusive ownership of the Customer. In no way, TELEMEDICINE will and may claim any ownership on such data, including in cases of unilateral Contract interruption, disagreement with the Customer or for any other reason whatsoever.

CleanWEB provides an online user interface that enables the mandated representatives of the Customer download online all of the data (except the Patient Personal Data) in the form of CDISC/ODM compliant archive (snapshot mode, both for metadata and clinical data) that can be re-imported in another software supporting the standard.

This feature also enables to automatically generate XML based electronic records suitable for long term archiving of the data and metadata, including management data and the full audit trail as required by the standard.

This feature is available since release 164.0.0 of CleanWEB.

TELEMEDICINE is CDISC Gold Member (http://www.cdisc.org/our-members) and has engaged the CDISC certification for the following use cases:

<table>
<tr><th colspan="3">ODM Data Import</th><th colspan="3">ODM Data Export</th></tr>
<tr><td rowspan="2">Metadata</td><td colspan="2">Clinical Data</td><td rowspan="2">Metadata</td><td colspan="2">Clinical Data</td></tr>
<tr><td>Snapshot</td><td>Transactional</td><td>Snapshot</td><td>Transactional</td></tr>
<tr><td>✓</td><td>✓</td><td>--</td><td>✓</td><td>✓</td><td>--</td></tr>
<tr><td colspan="3">ODM Metadata Interoperability</td><td colspan="3">--</td></tr>
</table>

This certification process is expected to be completed before the end of year 2015.

For more details, please refer to the following available documentation:

- **CDISC-ODM Import/Export Module, Technical Specifications**, *Ref. CW-189-TEC, Version 2 dated 22 June 2015*
- **CDISC-ODM Import/Export Module, User Manual**, *Ref.: CW-190-USM, June 2015*.

Appendix 1 – General Hosting Conditions

1. Definitions

Virtualization	technology that enables several Virtual Servers to run on a physical Infrastructure
Infrastructure	a series of physical resources including those of one or several Virtual Datacenters the local area network (LAN), bandwidth for internet connectivity and Virtualization
Virtual Datacenter:	dematerialized Datacenter including Hosting Servers, Storage Space, Virtual Machines and a private network, as well as a user interface to manage all these resources.
Storage Space:	allocated hard disk space enabling the storage of the data of the Hosting Servers in a centralized and secured way.
Hosting Server:	physical server computer machine with adequate memory and processing capacity, designed to host one or several Virtual Machines.
Virtual Machine:	logical server utilizing the resources of the Virtual Datacenter. Within a Datacenter, Virtual Machines are managed independently one from the other.
Service:	hosting service delivered by TELEMEDICINE TECHNOLOGIES to its Customers
Primary Site:	physical site where the production Infrastructure is located
Secondary Site:	physical site dedicated to the remote backup (files and databases) of the Primary Site.

2. General Service Features

The Service is based on an Infrastructure including a Primary Site and a Secondary Site located on different geographical areas.

This Infrastructure is delivered by specialized companies selected by TELEMEDICINE for the excellence of their Services. These Services are subject to service contracts which are distinct for the Primary Site and the Secondary Site.

These contracts define the conditions according to which a series of Virtual Datacenters are dedicated to TELEMEDICINE. TELEMEDICINE is the sole and exclusive administrator of the Virtual Datacenters subject of the aforementioned contracts. The contracted service companies can only intervene for the maintenance of the Infrastructure and are responsible for the power supply as well as the connectivity to the Internet backbone.

Except if otherwise specifically specified in the particular contractual conditions, TELEMEDICINE delivers to the Customer one Virtual Machine dedicated to the purchased Service.

The Infrastructure includes a state of the art fire protection system.

It will be of TELEMEDICINE responsibility to ensure that the selected company complies with these conditions, as specified in the Agreement.

The connectivity of the Primary Site of TELEMEDICINE to the Internet backbone is 300 Mb/sec at a minimum.

3. Power supply at rack level

Redounded induction

Data center powered by two distinct high voltage circuits (20 000 volts), through 2 distinct EDF lines. In case of complete interruption of the power network, generators guaranty normal operation of the infrastructure without service interruption.

Redounded power supply

Every server machine is powered by two power units functioning simultaneously, each of which being supplied by two different circuits.

Redounded inverters

Two inverters deliver a regulated power supply to every server. These systems are equipped with a set of batteries to deliver instantaneous protection from input power interruptions until the activation of the standby generators.

4. Data Confidentiality

Physical access to the site hosting the Infrastructure is authorized only to mandated staff of the service providers ensuring the maintenance of the Infrastructure as specified in the Agreement.

Protection against attempts of intrusion by non-authorized personnel is ensured by a number of systems and processes: access protected by armor-plated doors, electronic badges, digital fingerprint analyzers and human verifications.

A Firewall system managed by mandated and trained TELEMEDICINE staff ensures protection from non-authorized remote access.

All servers are located in a private area.

Logical security and confidentiality counter-measures implemented by hosted software are not in the scope of these present general conditions and shall be detailed in the appropriate contractual documents.

Most of the hosted software applications are based on a client / server architecture implementing the HTTP communication protocol. Except if otherwise specified in the particular contract, a dedicated SSL certificate is associated to the server module to ensure HTTPS encryption.

5. Backups

To comply with current regulations, daily automatic data (files, databases) backups are performed both on the Primary Site and the distant Secondary Site and in dedicated Virtual Machines.

These backups are incremental and cover the last 5 months of activity.

6. Remote maintenance, anti-virus surveillance

Routine maintenance operations are performed remotely from the authorized workstations located in the offices of the TELEMEDICINE.

Authorized workstations are identified by a fix IP address. The Firewall authorizes such maintenance operations only from the specified IP addresses and on an encrypted channel. Authorized users must authenticate (user ID and password). They must also know the access codes to the session of the Operating System of the targeted machine.

All workstations at TELEMEDICINE are equipped with an anti-virus with adequate upgrades. A continuous monitoring of security conditions is performed by TELEMEDICINE's staff in charge of Service Management

7. Continuity of service

TELEMEDICINE is committed to deliver the best quality of service to its Customers.

The whole Infrastructure to access software applications is redounded:

- Firewall ("fail over" system)
- Network connections at the level of every Hosting Server
- Switches: every connection of the Server is routed towards different equipment
- Routers: two routers ensure routing redundancy (HSRP protocol)
- Redounded Hosting Servers: automatic restart of the service within minutes in case of equipment outage / failure
- Storage Space is implemented on a RAID 1 disk array

The following conditions apply in case of service interruption:

- Service interruptions relating to maintenance operations and which duration does not exceed 5 minutes can be performed by TELEMEDICINE without preliminary notice
- In case of maintenance operations requiring service interruption for more than 5 minutes, the Service Manager as well as all users of the Service will be notified by email at least 48 hours before the maintenance. Such interruptions shall not last for more than 4 hours.
- In case of unexpected Service interruption, a call number is accessible at office hours (9am – 6pm). TELEMEDICINE is committed to restore the Service within a maximum delay of 4 hours following reception of the first call or of detection of the interruption.
- In all cases, TELEMEDICINE will make its best efforts to inform users appropriately and minimize Service downtime.

Contact information:

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 - 09 – Email: clinicaltrials@tentelemed.com
http://www.tentelemed.com