SenseAnywhere Compliance FDA 21 CFR Part 11

Version 2.2

SenseAnywhere B.V.

Bergrand 218
4707 AT Roosendaal
The Netherlands

+31 165 796 210

info@senseanywhere.com

www.senseanywhere.com

SenseAnywhere Compliance FDA 21 CFR Part 11

Document Status

- Document title: SenseAnywhere Compliance FDA 21 CFR Part 11
- Authors: N. Segers
- Identifier: Documentation/FDA
- Version: 2.2

Revision History

Version	Date	By	Reason
1.0	20180201	N. Segers	Initial version.
2.0	20190415	N. Segers	Document in new template.
2.1	20190828	N. Segers	Textual changes.
2.2	20200824	N. Segers	The document has been updated (IQ, OQ, Data Export, and minor textual changes).

Definitions and abbreviations

Table 1 Definitions and abbreviations

Definition / Abbreviation	Explanation
DQ	Design Qualification
IQ	Installation Qualification
MSV	Manufacturer Software Validation
OQ	Operational Qualification
SA	SenseAnywhere
SAClient	SAClient Portal

Introduction

This document serves to evaluate the SenseAnywhere software (SAClient) compliancy with FDA 21 CFR Part 11 regulation. As part of this document the FDA 21 CFR Part 11 requirements are listed and provided with a description of how the SenseAnywhere software satisfies each requirement, contributing to a compliant system. At the moment of writing, the FDA 21 CFR Part 11 regulations are current as of April 1, 2015.

bsi. ISO 9001 Quality Management FM 698025 ISO/IEC 27001 Information Security Management IS 727158

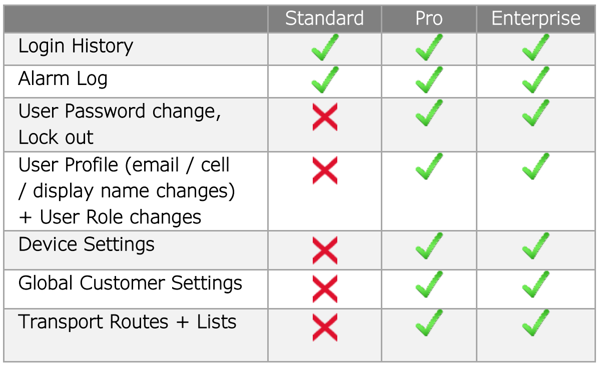
FDA 21 CFR Part 11 Requirements and Checklist

What follows now is a listing of all requirements and how SenseAnywhere satisfies them.

Subpart B – Electronic Records

Table 2 Section 11.10 – Controls for closed systems

Requirements	Comments
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:	The insertion of measurements requires absolutely no human interaction. AccessPoints communicate via a secure protocol with the SenseAnywhere back end, which takes care of the insertion of new measurements. It is impossible for any service to modify or delete measurements, therefore maintaining data integrity.
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	SenseAnywhere keeps track of all changes made to critical configuration. SenseAnywhere has performed a full validation of the system. As a result, SenseAnywhere has a completed Manufacturer Software Validation (MSV). Installation of hardware and configuration of SenseAnywhere portal can also be validated by the customer. This is possible with an Installation Qualification (IQ) and Operational Qualification (OQ).
(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.	In the SenseAnywhere portal it is possible to export all data provided in tables, including measurements, to Excel (XLSX) format. Customers can use the Data Export feature to create files that contain device measurements or events (PDF, CSV, Excel). Reports are provided in PDF format. Graphical data can be exported to several image formats.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	All our electronic records are stored in Azure storage facilities. Backups are made automatically by Microsoft of all our data. Customers do not have direct access to our storage facilities.

<table>
<tr><td>(d) Limiting system access to authorized individuals.</td><td>Only registered users can use the SenseAnywhere system. All users need to authenticate with their unique username and password, in combination with authorization roles. A Super Admin is able to set and edit the Access Rights of a user at the Global Customer Settings page.</td></tr>
<tr><td>(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.</td><td>All changes to records are tracked with audit trails within the system. It is impossible to modify audit trails. Measurements and alarm history cannot be changed either. The customer is able to review audit trails within the system for reviewing purposes. Depending on the type of subscription, different audit trails can be reviewed:

<table>
<tr><th></th><th>Standard</th><th>Pro</th><th>Enterprise</th></tr>
<tr><td>Login History</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>Alarm Log</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td>User Password change, Lock out</td><td>✗</td><td>✓</td><td>✓</td></tr>
<tr><td>User Profile (email / cell / display name changes) + User Role changes</td><td>✗</td><td>✓</td><td>✓</td></tr>
<tr><td>Device Settings</td><td>✗</td><td>✓</td><td>✓</td></tr>
<tr><td>Global Customer Settings</td><td>✗</td><td>✓</td><td>✓</td></tr>
<tr><td>Transport Routes + Lists</td><td>✗</td><td>✓</td><td>✓</td></tr>
</table>
</td></tr>
<tr><td>(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.</td><td>Whenever a sequencing of events is required, the SenseAnywhere system enforces this.</td></tr>
<tr><td>(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.</td><td>Only registered users can use the SenseAnywhere system. All users need to authenticate with their unique username and password, in combination with authorization roles (which are managed by SenseAnywhere).</td></tr>
<tr><td>(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.</td><td>Communication to the SenseAnywhere back end cannot be manipulated by users. The protocol used by the devices and back end makes sure that the data is valid.</td></tr>
</table>

(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.	Records of the employment and educational history of SenseAnywhere employees are verified. It is the customer's responsibility to make sure only qualified people make use of the SenseAnywhere system. SenseAnywhere makes sure the distributors have sufficient system knowledge and understanding. The distributors should provide customers with education and training to use the SenseAnywhere system.
(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.	N/A. It is the customer's responsibility to develop written policies related to responsibility.
(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. (2) Revision and change control procedures to maintain an audit trail that documents time- sequenced development and modification of systems documentation.	(1) Responsibility of the organization that makes use of the SenseAnywhere system. (2) All SenseAnywhere documents include a revision history, which is forced by the SenseAnywhere documentation policies.

Table 3 Section 11.30 – Controls for open systems

Requirements	Comments
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.	N/A. The SenseAnywhere system is a closed system.

Table 4 Section 11.50 – Signature manifestations

Requirements	Comments
(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.	When a signature is created, the following data is included: • User ID, this uniquely identifies the user with all his credentials. • Date and time the signature was created. • Meaning of 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).	Where a signature is visually represented in the SenseAnywhere system, it is presented in human readable form.

Table 5 Section 11.70 – Signature/record linking

Requirements	Comments
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.	All signatures are stored inside Azure storage facilities. The signatures cannot be modified afterwards. A signed electronic record is linked to only one signature, which cannot be removed or altered.

Subpart C – Electronic Signatures

Table 6 Section 11.100 – General requirements

Requirements	Comments
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Every user makes use of its unique username and password combination. Usernames cannot be reused or reassigned to another individual.
(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.	N/A. This is the responsibility of the customer.

(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. (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.	N/A. This is the responsibility of the customer.

Table 7 Section 11.200 – Electronic signature components and controls

Requirements	Comments
(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. (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.	The SenseAnywhere system makes use of two distinct identification components: the unique username and password. The first time a user logs in into the portal, both identification components are required. When signing, the user needs to provide the password only. When a user logs out, or is timed out, the user needs to log in again, requiring both the username and password.

(2) Be used only by their genuine owners; and	Customer's responsibility.
(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.	N/A.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	N/A. The SenseAnywhere system does not support biometric signatures.

Table 8 Section 11.300 – Controls for identification code/passwords

Requirements	Comments
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.	Every username within the SenseAnywhere system is unique.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	N/A. Customer's responsibility.
(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.	User accounts can be deleted by customers (super admin) if access rights of the user are permitting the action. If not possible, resellers can delete these user accounts on request for customer. Password can be reset by the user or by SenseAnywhere. Password recovery is not possible.

(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.	All login attempts are logged within the SenseAnywhere system. User accounts are temporarily locked after consecutive failed attempts, which also logged.
(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.	N/A.

Supporting tools for validation

1. Design Qualification (DQ)
2. Manufacturer Software Validation (MSV)
3. Customer Qualification Documents
    a. Installation Qualification (IQ)
    b. Operational Qualification (OQ)

   The IQ and OQ can be bought by the customer as a package and the documents can be filled in digitally.

bsi. ISO 9001 Quality Management FM 698025 ISO/IEC 27001 Information Security Management IS 727158