ANNEXURE 01

FDA 21 CFR Part 11
Compliance Checklist
Electronic Records, Electronic Signatures
Validation
For

HT16u (Humidity-Temperature)

Logger Software

Masibus Automation And Instrumentation Pvt. Ltd.

B/30, GIDC Electronics Estate,
Sector-25, Gandhinagar-382044, Gujarat, India
☎+91 79 23287275-79 ⌨+91 79 23287281-82
Email: support@masibus.com
Web: www.masibus.com

Contents

1. Introduction

Effective August 20, 1997, the U.S. Food and Drug Administration (FDA) released and published a new rule to enable companies to approve their results with electronic signatures and to transfer paper-trail documentation into electronic records. This rule is known as 21 Code of Federal Regulations, Part 11 (referred to as 21 CFR Part 11) and applies to all industry segments regulated by the FDA. 21 CFR Part 11 (in short: Part 11) defines the FDA acceptance criteria for the use of electronic records and electronic signatures in place of records in paper form and handwritten signatures on paper. In this regard, electronic records and signatures must be as trustworthy, reliable and effective as conventional records. The impact of this rule on current work practices and data handling in various industries has been much higher than expected. The FDA regulations are also applied beyond the pharmaceutical industry in other life sciences, such as the food and beverage industry, cosmetics, consumer care, etc.

The requirements on electronic records of 21 CFR Part 11 is not new to the industry as they only summarize several predicate rules. However, 21 CFR Part 11 places high emphasis on the implementation of all measures to protect and secure electronic records. Besides all uncertainties and changes that 21 CFR Part 11 requires in the behavior of the vendors of reporting and analysis software, it is well worth implementing in today's laboratories because it can help the industry with one of the most important issues in pharmaceutical research—bringing new drugs faster to market. The major benefits of this shift towards electronic data management are in the potential productivity increase for the industry. The industry can decrease its data output on paper, speed up the data review and approval process, and benefit from new automation technology based on computerized system control.

The main requirements of 21 CFR Part 11 are data security, data integrity, traceability/audit trails and electronic signatures. Data security and data integrity are maintained by requiring users to login with a valid user name and password. There are then permission tables that delineate what a user has access to and what that user has the ability to do. Anything that is done with the data is logged to the audit trail, thus maintaining the integrity of the data. Capturing the - who, what, when and why of data modifications is the requirement of the traceability/audit trails requirement. This data is captured automatically and includes the user name, the date and time, and what was modified. The data that is not captured is why the data was modified. This data cannot be modified. It is all permanent and readily available in human readable format.

SMART-HT meets the functional requirements for the use of electronic records and electronic signatures.

The Masibus recommendations for the software architecture, conception, and configuration will assist users in achieving compliance. This document is divided into two parts: The first part provides a brief overview of the requirements of Part 11, the second introduces the functionality of SMART-HT under the aspect of those requirements.

2. Purpose

This document describes the SMART-HT software compliance with the US Food and Drugs Administration's Code of Federal Regulations, chapter 21, part 11 (aka FDA 21 CFR Part 11).

FDA 21 CFR Part 11 compliance embraces complete systems including hardware, software, documentation, file & user management, user rules of conduct, company security standards, etc. Taken that into consideration SMART-HT software is only one element in this system chain. Despite that fact, Masibus guarantees that, providing the SMART-HT software will not in itself create any breaches of FDA 21 CFR Part 11 compliance.

3. About SMART-HT

SMART-HT is a windows based software, which supports Masibus HT16u device products. It provides true data collection and monitoring function; such collected data will be view in tabular, graph, zoom observation, and dynamic transfer to file without any need for annoying programming.

Its unique concept combines three key functions (Configuration, Downloading Data and Reporting), which position SMART-HT as the most convenient solution. Software is design to streamline the process of downloading data and reviewing it in a user-friendly, time efficient manner. The software offers many customizable features and options, software includes many types of reports, and it includes displays like tabular and trend.

Thank you for choosing SMART-HT.

4. FDA 21 CFR 11 - SUBPART A

General Provisions

4.1 Sec. 11.1 Scope

(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.

(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.

(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.

(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.

(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.

(f.) This part does not apply to records required to be established or maintained by Sec. 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

4.2 Sec. 11.2 Implementation

(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.

(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:

(1.) The requirements of this part are met; and

(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.

4.3 Sec. 11.3 Definitions

(a.) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b.) The following definitions of terms also apply to this part:

(1.) Act means the Federal Food, Drug, and Cosmetic Act (section. 201-903 (21 U.S.C. 321-393)).

(2.) Agency means the Food and Drug Administration.

(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.

(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.

(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.

(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.

(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.

(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 writing in a permanent form. The act of signing with a writing or marking instruments 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.

(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.

5. FDA 21 CFR 11 - SUBPART B

Electronic Records

5.1 Sec. 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, 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.

Software compliance: SMART-HT supports access control. It registers changes to electronic records as audit trail events. Software provides built in functionality for easy to use data acquisition, and automatic data logging to RDMS database, measurement analysis, and data presentation and reports. The data record itself can no longer be altered and therefore does not required an audit trail. Unauthorized changes are prevented by the system through access control. Additionally the SMART-HT databases are password protected, the password of any database by use of SMART-HT software as well as the verification of its compliance with the FDA requirements, Standard Operating Procedures-SOPs, and its final validation remain the sole responsibility of the systems integrator and of the end customer.

(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.

Software compliance: SMART-HT writes all its records to an SQL-complaint RDMS database. Data records and audit trails can be exported or archived. The information is available on-line to the authorized operator in either standard or customized displays, or can be printed or exported.

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

Software compliance: Device data are stored in password protected relational database and supports long-term archiving. Data is read only through SMART-HT software and may be accessed in any other way, to avoid alteration and falsification it remains the sole responsibility of the systems integrator and of the end customer to protect those databases from being deleted, moved, and renamed or from any other actions, which could harm the stored data. Each action to delete, print, and export data, is further controlled by the entry of an approver's credentials. The approver must have sufficient privileges to perform the selected action. The systems integrator or end customer should specify retention periods and define procedures for backup and retrieval of electronics records. In addition, to prevent data loss, you must ensure that the file directory in which the database resides is kept intact by using a variety of security software, including the native security available with most windows operating systems.

(d.) Limiting system access to authorized individuals.

Software compliance: Standard procedures to limit physical access are the sole responsibility of the systems integrator and of the end customer. The end customer should ensure that only persons who have a legitimate reason to use the system should be granted access to the system. As this requirement is virtually equivalent to 11.10(g), it is interpreted to refer to both physical access and logical access. SMART-HT provides an advanced user management defining access rights to the software. As required by FDA21 CFR11.200.1, SMART-HT employs two distinct identification components such as a unique combination of user name and password. Also, a user with administrator access must log in to be able to access the User Accounts, which controls the access of

all users and grant access to chosen users only, and assign usage privileges to each. Additionally, the software supports a number of schemes to prevent the compromising of a user's password including minimum password length, complexity, password aging, and preventing the re-use of recent passwords.

(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.

Software compliance: The audit trail is secure within the software and cannot be changed by a user. When using SMART-HT there is no way to overwritten or alter, falsify or delete a record of the data while the database is password protected. However, it remains the sole responsibility of the systems integrator and of the end customer to protect those files from being corrupted, damaged, deleted, moved or renamed, or from any other actions which could harm the stored data. It is the sole responsibility of the end customer to manage this Database. We strongly recommends activating the MS SQL Audit Trail feature in order to trace any manual changes to the records. Audit trial events can be viewed, printed and archived. All user operations in the SMART-HT such as report generation on demand, login/logout or any other assigned action, are tracked by SMART-HT's audit trail mechanism which contains time stamp, user name, and events.

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

Software compliance: SMART-HT supports interlocks and sequential function flow. Software is designed to ensure that the user is limited to performing one function at a time, and in the correct order. Operator actions are designed to require confirmation.

(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.

Software compliance: SMART-HT advanced user management provides definition of access rights to the features of the application. As required by FDA 21 CFR 11.200.1, SMART-HT runs two distinct identification components such as a unique combination of user name and password. The software restricts access to the user and user role configuration. When the rights are changed, the software automatically generates an audit trail event. In addition, the systems integrator and the end customer should define how access is limited to authorized individuals (e.g. who has access to specific objects or functions), excluding the special rights for administrators.

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

Software compliance: Not applicable to SMART-HT software. It remains the sole responsibility of the systems integrator and of the end customer to choose, configure, manage and maintain these checks to determine, as appropriate, the validity of the source of data input or operational instruction.

(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.

Software compliance: SMART-HT is supplied with a user guide and a thorough help file is included within the software. It remains the sole responsibility of the systems integrator and of the end customer to verify that the users configured as being members of a User Group will have the education, training, and experience that corresponds to the tasks assigned to this User Group. The customer is responsible for ensuring that personnel working with the software are qualified.

(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.

Software compliance: It is the sole responsibility of the systems integrator and of the end customer to defining, establish and maintain the adherence to such written policies. User need to have their own Standard Operating Procedures-SOPs.

(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.

Software compliance: The systems integrator / end customer who has developed or deployed a project using SMART-HT software is responsible for writing its own project documentation and maintaining it. SMART-HT provides software audit trails to record changes and actions carried out. In house procedures are the user's responsibility. SMART-HT software documentation is fully version controlled in accordance with our quality procedure. User guide are included on the distribution media. The software documentation is delivered in PDF files.

5.2 Sec. 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 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.

Software compliance: SMART-HT is designed for collection and representation of electronic records in a document format. Modification, maintenance and transmission of such records are not part of the scope of SMART-HT software. The establishment of written procedures and controls 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 remains the sole responsibility of the end customer. SMART-HT does not provide any functionality for digital (encrypted) signatures.

5.3 Sec. 11.50 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).

Software compliance: SMART-HT is designed for collection and representation of electronic records in a document human readable format. The SMART-HT Report provides electronic signing of the exported documents. When electronics records are signed, the system records the following items as part of the electronics signing process:
Name of the signer
Title of the signer
The meaning associated with the signature
The date and time when the signature was executed
Optional comments.

5.4 Sec. 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.

Software compliance: SMART-HT is designed for collection and representation of electronic records in a document format. Signing of such records is not part of the scope of SMART-HT software. The establishment of linking electronic signatures to their respective electronic records remains the sole responsibility of the end customer.

6. FDA 21 CFR 11 - SUBPART C

Electronic Signatures

6.1 Sec. 11.100 General requirements

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

Software compliance: SMART-HT user management system provides assigning a unique electronic signature to a unique set of user name and password of a user. It is the sole responsibility of the systems integrator;s and of the end customer's not to give an already used set of user name and password to another or different users.

(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.

Software compliance: The verification of the operator's identity before establishment, assignment or certification of an electronic signature (user name/password), which allow them to use software is the sole responsibility of the end 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.

Software compliance: The certification to the agency by the person using electronic signature that this signature (user name/password) are intended to be a legally binding equivalent to traditional handwritten signatures remains under the direct responsibility of the end customer.

(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.

Software compliance: The submission in paper form of the certification to the Office of Regional Operations remains under the direct responsibility of the end customer.

(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.

Software compliance: Providing additional certification or testimony upon agency request remains under the direct responsibility of the end customer.

6.2 Sec. 11.200 Electronic signature components and controls

(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.

Software compliance: SMART-HT provides an implementation of two distinct identification components such as a unique combination of user name and password for users with assigned electronic signature.

(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.

Software compliance: In SMART-HT, the first signings are always performed by the two identification components (user name/password) and all subsequent signings are performed using one identification component (pincode).

(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.

Software compliance: In SMART-HT, the first and all subsequent signings are always performed by the two identification components (user name/password).

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

Software compliance: Verification and certification that a unique combination of identification components is not used by different individuals is the sole responsibility of the customer.

(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.

Software compliance: It is strongly recommended that the end customer shall prohibit the use of an individual's electronic signature by anyone other than its genuine owner. Password data cannot be retrieved from the software. Along with unique user names, the software includes a feature to block a user account after a specified number of consecutive failed login attempts. The administrator can specify how many consecutive failed login attempts will block out a user account. Once the account is blocked, user cannot use that account to access the software until an administrator unblocked the account again.

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

Software compliance: SMART-HT software does not support biometric signatures. Standard tools of third party manufacturers can be used to create and add an electronic signature by features available in PDF file, but it is the sole responsibility of the systems integrator and of the end customer to design, develop and validate such system.

6.3 Sec. 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. 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.

Software compliance: SMART-HT User Management mechanism prohibits the coexistence of identical sets of signature identification components. For more details, please see Sec. 11.100 (a.).

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

Software compliance: SMART-HT has an option to be configured password aging and minimum password complexity and prevents the reuse of a 10 number of prior passwords.

(c.) 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 or permanent replacements using suitable, rigorous controls.

Software compliance: The implementation of such controls as to remove from the system or republish a combination of signature components that has become compromised remains the sole

responsibility of the end customer. The blocking out of user account that fail consecutive logins can help to identify a compromised user name. Unauthorized logon attempts are logged to the audit trails event log. Also, the administrator can deactivate any user account and can add a new temporary user account and password if necessary. Customer is responsible for defining procedures for handling forgotten or lost passwords.

(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.

Software compliance: The user block feature after a specified number of consecutive failed logins is a safeguard against unauthorized access to the software. SMART-HT generates an audit trail log and message upon the every failed login attempt and locks the software. The configuration of an urgent reporting linked to such an event remains the sole responsibility of the systems integrator and of the end customer.

(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.

Software compliance: Such tokens, cards, and devices are not part of the SMART-HT software. Initial and periodic testing plan for these components remains the sole responsibility of the systems integrator and of the end customer.

7. Contact Information

For further information described in this compliance checklist, please contact at Masibus Automation And Instrumentation Pvt. Ltd. by phone or email:

B-30, G.I.D.C Electronic Estate, Sector - 25, Gandhinagar - 382044. Gujarat - India.
Phone: +91 79 23287275-79
Fax: +91 79 23287281
E-mail: **support@masibus.com**